MASTERARBEIT / MASTER’S THESIS

Titel der Masterarbeit / Title of the Master‘s Thesis

„Incorporating data protective behaviour“

verfasst von / submitted by

Roger Ferdinand François von Laufenberg, BA

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Arts (MA)

Wien, 2016 / Vienna 2016

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 066 905
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Soziologie
Betreut von / Supervisor:	Dr. Reinhard Kreissl

Acknowledgements

The months and months spent writing this thesis could not have been done without the help, support and inspiration of several people which deserve to be mentioned here.

First of all, I would like to thank Reinhard Kreissl, who not only provided great support by supervising my thesis and helping me to concretise my ideas but also gave me the possibility of gaining a lot of research experience in a range of fields across the discipline. In general, the whole team at the Vienna Centre for Societal Security (VICESSE), with which I had the opportunity to work with in the last couple of years is a great source for exchanging ideas and discussing the broad range of topics in our field.

I would also like to thank my friends and colleagues who I have met during my great experience here in Vienna. In particular, this includes Vera, who made the last semesters of my studies bearable and with whom it was always a pleasure to exchange my thoughts on different research topics, as well as Chris who always showed great interest and was ready to listen and discuss about my problems and ideas. And of course to all my other friends with whom I hope to spent a lot more years to come.

Also my family who has supported me throughout my search for the right studies in their best possible ways and have helped me through some more difficult phases as well.

And finally I would like to thank Verena, who not only was patient during the whole summer as I was finishing my studies, but also was probably my greatest source of inspiration, willing to help wherever she could and being supportive in every possible way. You make also the upcoming challenges look manageable, thank you!

Table of content

Contents

List of Figures

1. Introduction

In our modern techno-societies, our personal data – covering our names and dates of birth, our shopping and consumer habits to our biometric features like fingerprints – has not only become open to a widespread group of people and institutions, but has also become a fiercely contested economic good (Fuchs 2012). Everyone's personal data is being passed through the hands of public and private organisations, some of them making a large amount of money with it – or are at least trying to, while others are using the personal data for in-depth analysis of the behaviour of citizens, consumers and users in order to implement manipulation or controlling measures in further consequence (Bauman et al. 2015). Regarding these practices of data collection and data processing, big concerns are raised – while on the one hand, more and more of our habits and behaviour of our past and present actions and thoughts are stored, processed and made available to a large range of organisations and institutions due to the technification and "datafication" (van Dijk 2014) of our daily lives, on the other hand the property rights of the personal data are not clearly delimited and established (Schwartz 2005; Purtova 2015).

Personal data can have multiple ownerships depending on the extent it has been shared and depending on who has been able to gain access to the data (Al-Khouri 2012) – often personal data is passed on voluntarily to organisations by consumers and citizens, however, personal data is also often captured by organisations (e.g. through internet browsing collections or the collection of location data) and in further consequence also derived from available data through extensive analysis (see for example the research by Kosinski et al (2013) who derived private traits and attributes through the Facebook Likes of users). Clearly delimiting who has what kind of rights on the data is thus a difficult task. Similarly, it is difficult to keep track of where (traces of) personal data are stored, for how long the collection is intended to last and who will have access to it. Individuals have become leaking data containers (Kreissl, 2014, p. 15f.) and in many instances the traceability of the personal data has become almost impossible.

A result of this phenomenon is a raise in popularity of disciplines like surveillance studies, researching the mechanisms behind surveillance and the effects of surveillance on societies, and in further consequence an increase in debates about data protection and privacy rights. For example, in their 2014 report, Human Rights Watch criticises the practices of mass surveillance of national governments and states that '[w]e must (…) recognize that the duty to protect rights in a world of globalized communication cannot stop at territorial borders' (PoKempner 2014, p.50). Legally, aims to regulate data protection have been in place already for a few decades. On a European level, a data protection Directive has been introduced in 1995, trying to harmonize the different national laws handling data protection in Europe. With regard to the fast progress of the technological development and the outdated Directive from 1995, the European Commission proposed a reform of the Directive in January 2012 (European Commission, 2012). After long negotiations and several drafts, an agreement on the new directive and a new regulation have been reached by the European Commission, Council and Parliament in December 2015 (European Commission, 2015a).

One of the main changes with which the EC promoted the new regulation and directive was that they "will give people **more control** over their personal data and make it easier to access it" (European Commission, 2015b; emphasis in original). A strong emphasis on the rights of the citizens in regard to data protection is to be welcomed and is a continuity of what has been the general practice regarding data protection within the last decades. For example, in the Directive of 1995, one possibility for citizens to control and access their personal data is the Art. 12 – *'The right of access'* (cf. section V of the directive 95/46/EC 1995, p.12) which is regarded as an active tool for data protection by knowing exactly what personal data is processed by different organisations. This right grants citizens the possibility, upon request, to obtain their data processed by an organisation. Different cases have already shown that problems arise when data is stored by multinational organisations, like e.g. in the case of Max Schrems vs. Facebook, where an Austrian law-student has not only tried for years to simply access his data stored by Facebook, but also to assert this right by taking Facebook to court (cf. http://europe-v-facebook.org/EN/Objectives/objectives.html).

A recent European research project, the IRISS[1] project, has examined the likelihood of ensuring this right of access in private and public organisations and institutions across Europe. The outcome of the project showed that it was not only difficult to identify the person or the legal entity responsible for the processing of the personal data, but also that 43% of all the requests for access did not result in a disclosure of personal data (L'Hoiry & Norris 2014). The project showed how the organisations deal with the requests, where they fail to comply with legal frameworks and what effects this could have on the citizens and their privacy rights. It also establishes serious doubts if a new regulation and directive will really provide citizens with

[1] Increasing Resilience in Surveillance Societies

more control of their personal data if under the current legal settings, a simple request to access to personal data fails in many cases.

While these findings are crucial, they lack in critical questions in regard to why these requests failed in so many instances and why these difficulties occurred. They also do not consider the possibilities and difficulties that occur on the side of the organisation regarding these requests. This is however an important aspect to consider, when almost half of the data controllers do not operate according to the data protection directive (and their national implementation). Is this done on purpose, or is this due to uninformed employees? Or is the legal framework outdated in such a way that data processors cannot conform to it as initially intended by the Directive due to technological developments – and thus standing in opposition of a technology neutrality of legal norms (Greenberg 2016, p. 1495). Or is it maybe an outcome of the lack of interest from the citizens' side, who rarely address concerns or the request to access to personal data to the data processors?

These questions have fuelled the research interest in my master thesis, and thus why I will focus on the operating of data protection in organisations by researching how the procedure of granting those rights is treated from the controller's point of view. Primarily with a focus on how employees operating data collection and data protection have been appointed to their role within the organisation and how they have obtained their knowledge on data protection principles – and how this knowledge influences their work and their contact with "lay" data subjects and their contact with the technology behind the data collection and the process. The study also has an interest in researching how the data controller and the related organisation treat data collection in general, giving further insight into the motivation and purpose of the way of operating.

Thesis Structure

My thesis can roughly be divided in two parts. The first part will broadly introduce the field of research by presenting the state of the art of similar studies (**chapter 2**), followed by the research question I aim at addressing with my thesis (**chapter 3**). **Chapter 4** will continue with the theoretical concept behind my thesis, drawing from two broad disciplines – *surveillance studies*, which is utilised for describing the motivations as well as the implications behind surveillance practices; and *science and technology studies*, which helps to understand how the technology which is at the basis of many surveillance practices is shaped by many societal, political and cultural factors while being equally able to shape its surroundings. Finally, in **chapter 5**, I will give insight into the methodological approach of my research.

The second part of my thesis largely consists of the analysis of my collected data. First by analysing the relevant data protection laws (**chapter 6**), starting with a short historical overview of the development of relevant legal provisions regarding data protection and the current European data protection Directive from 1995, before I continue with highlighting the important changes brought forth by the new General Data Protection Regulation. Lastly, I will shortly show how the legal state of the art in Austria deals with data protection. The main analysis of my empirical results will be shown in **chapter 7**, which will highlight how data collections, data processing and data protection are negotiated in organisations and thus handled differently depending on a range of internal and external influences. The breakdown of the influences will demonstrate how a certain behaviour with a focus on data protection – or data protective behaviour, as I call it – is tried to be implemented by certain individuals within organisations and handled by other employees and employers. **Chapter 8** will provide a discussion on the results and the possible implications for organisations as well as individuals outside of organisations or citizens, before I will conclude with some final thoughts in **chapter 9**.

2. State of the Art

This chapter provides an overview of empirical studies in the field of research of surveillance studies. These studies are insofar of importance as the idea for the present study was based on some of them. Several of these researches show how surveillance practices are performed in different situations, some focussing on manual surveillance operators and thus trying to unveil the opaque haze of surveillance from an operating point of view. Others focus more on the outcome of surveillance of people, or on how ordinary citizens are able to contest surveillance practices by utilising the available legal rights. Finally, some of the studies focus on the surveillance workers, the people operating the surveillance practices. There might be a lot of other research studies not included here which are also relevant. A comprehensive list of the state of research is beyond the scope if this analysis. However, in my opinion, the ones presented in this thesis give a good overview of what has been done and how my research fits in the current discussion and how it might help in closing one or two gaps in the field. A more general overview of (also theoretical) surveillance studies will be presented in Chapter 4.

*****

My study will not be the first to examine how personal data is handled in different settings. Norris and Armstrong (1999a, 1999b) have probably provided the most ground-breaking empirical research of surveillance practices of CCTV operators, due to it being the first of its kind. While previous studies on video surveillance systems have focused on the impact of CCTV on crime rates, Norris and Armstrong have directed their attention to how CCTV operates in practice. Their two-year study was carried out by performing participant observations of the operations in CCTV control rooms on three different sites with installed CCTV systems (Norris & Armstrong 1999a, p.160). Norris and Armstrong describe video surveillance systems beyond crime fighting as "the power to watch and potentially intervene in a variety situations, whether or not they be criminal" (ibid., p.158), which is why they focused their research on who and what gets watched, as well as the criteria by which the 'targets' of surveillance are chosen. The researchers collected data on the persons or groups (sex, age, ethnicity and appearance) being targeted by surveillance and why they were being treated as 'suspicious' (crime related, public order, no obvious research[2] or other) (ibid., p.162f.).

[2] No obvious reason was chosen when the 'scrutinised showed no specific suspicious signs in terms of behaviour or wasn't a known offender for the operators, but still targeted by the operators.

The incoming information for CCTV operators is enormous: for a CCTV system with 20 cameras with 25 frames per second a total of 43.2 million frames need to be processed by the operators – per day (ibid., p.158f.). A selection of information thus needs to be done by the operators. Although their position – remotely in the operating room – serves as an 'advantage' since the watched behave normally as if they weren't watched, the disadvantage for the operators is the lack of other sensory input and information and thus they have to rely solely on the visual information. Based on this, it can be assumed that the operators have to apply some sort of filters in order to process the amount of incoming data.

On the one hand, the study shows that from a demographic point of view men, teenagers and black people were way more likely to be targeted by the surveillance operators. In comparison to their presence in the general population, they were between one and a half and two and a half times more probable to be selected by the operators (ibid., p.162f.). On the other hand, the study also shows that many of those who are more likely to be targeted, are also targeted for no obvious reason by the operators (ibid., p.163). Instead, CCTV operators often make assumptions based on prejudices: youths are referred to as "toe-rags" and "scumbags" and aimed at by surveillance "because they are up to no good". Selection of close observation is done based on their attire, posture and clothing. Having supposedly a "scrote walk" – meaning that they look too confident and hard, either with their head up and back straight, or their chin down and shuffling along – in combination with a "scrote haircut" – either being too short, too long or with hair gel – were reasons for youths being targeted by surveillance, in anticipation of any possible criminal behaviour (ibid., p.164f.). Similar for black people and ethnic minorities, who are targeted on the basis of prevalent stereotypes and are even more exposed if being young, male, wearing headgear – and thus trying to cover up something – or having a car (ibid., p.169f.). If women are targeted by surveillance, it is often for voyeuristic reasons (ibid., p.174).

Norris and Armstrong thus show to a large extent how discriminatory concepts, prejudice and voyeurism determine the reasons why individuals and groups are selected for surveillance and observed while they are walking through the city centre, are shopping in the city mall, or just hanging out and talking. While not all observation by the operators were based on these criteria – roughly half of the observations were crime or public order related – the decision for targeting individuals based on intuition and interpretation creates a *suspect* population, where one is a suspect due to belonging to a specific group (ibid., p.175). Although individuals belonging to these categories are statistically not involved more often in criminal activities, they are still treated as suspects when caught on tape – whether they are innocent or not – and in turn painting a rather negative image towards the 'suspect population' about their own position in society, of which the majority is law-abiding (ibid., p.176).

In a similar approach, Hempel and Töpfer (2004) have studied the increase in CCTV practices in seven European countries (including Austria) in their URBANEYE project. Beside short- and long-term participant observation in CCTV control rooms and expert interviews with the managers and operators, they also analysed news articles on video surveillance systems, the extent of video surveillance systems of public places in cities by visiting sites and mapping the systems, surveying and interviewing citizens on their knowledge about and attitude towards CCTV, and organised expert workshops on the policy implications of CCTV (Hempel & Töpfer 2004, p.3f.).

The study has mainly shown the wide variations and differences of video surveillance practices between the researched countries. Not surprisingly the diffusion of CCTV systems was the highest in Great Britain, as was the acceptance in public. Also the installed systems were more likely to be in line with the legislation. In Germany and Austria, however, video surveillance systems were not developed and present as much and also more likely to be contested by the public and the media, but also often operated in secrecy in (semi-)private places, lacking signage and thus constituted a violation of data protection regulations.

The symbolic character of CCTV systems was often predominant, hoping to prevent deviant behaviour as a result of the visibility of the cameras and not so much to 'catch' deviant behaviour on tape or by the gaze of the operators. As with the study by Norris and Armstrong, the URBANEYE study also showed the discriminatory targeting patterns of CCTV operators, aiming at the surveillance of whole 'suspect populations' in order to cope with the amount of incoming information. This is also noticed by the 'suspect populations' as it were also mainly youth and teenagers who showed opposing attitudes towards video surveillance and also subjectively felt to be targeted more often by surveillance practices. Finally, although many respondents were in favour of video surveillance, the majority doubted that surveillance had a positive impact on crime rates – instead of preventing crime, many respondents assumed a displacement of crime as a result of the video surveillance systems (ibid., p.4f.).

The following years saw a range of further studies, empirically researching different aspects of surveillance, and involving a range of different methods – often however relying on interviews with different stakeholders involved in certain parts of video surveillance. Galdon Clavell et al. (2012) have for example analysed the deployment of CCTV surveillance systems in Spain, conducting semi-structured interviews with actors involved in the deployment at regional levels which supported legal and media analysis on video surveillance in Spain (Galdon Clavell et al. 2012, p.58f.). The authors draw the picture of a highly fragmented deployment of CCTV systems, with a surveillance practice which is influenced by legal grey areas, hampering the original restrictive effect of CCTV regulation (ibid., p.67). A more ethnographical approach was chosen by Stuart Waiton (2010) in trying to understand the reasons for the implementation of a CCTV system in a calm residential area in the outskirts of Glasgow. While also driven by a personal agenda of opposing the installation of the system, Waiton nonetheless gives an interesting analysis of the driving forces behind such projects – through participant observations at public meetings informing on the project as well as informal talks with residents and shopkeepers. Even though from a methodological point of view the empirical research appears to lack the standardised approach of data collection (see e.g. Gläser and Laudel 2009, p. 29), Waiton identified how a political dynamic of governmental agencies and local MPs, but also a 'silent majority', opposing parties like residents and activists shape the discourse around the implementation of the CCTV system.

Liisa Mäkinen (2016) has provided some interesting insight into domestic CCTV surveillance usage by conducting interviews with people having installed video surveillance systems at their homes in Finland. She investigates the reasons behind residents having installed systems at their homes, how these are used, but also how the residents think about their installed systems and what their feelings towards the system are (Mäkinen 2016, p.60). Drawing on the results of the interviews, she describes five types of domestic surveillance: *controlling surveillance* aiming at keeping the house in order; *caring surveillance* which should ensure that the residents are safe at home; *recreational surveillance*, a more playful type of surveillance of the weather or the surroundings of the house; *communicational surveillance* using the video surveillance system for communicating from a distance with residents of the house; and finally *sincere surveillance* – responding to the question of how surveillance is performed instead of why – in which the "residents as watchers aspire to separate themselves from voyeuristic watchers and spies" (ibid., p.75). For further examples of (empirical) research of CCTV surveillance systems, see Germain et al. (2013) who provide an extensive analysis of surveillance studies contributions aiming at identifying the reasons surveillance studies scholars use to describe the success of video surveillance technology.

Others have focused their research on how different scrutinized react to surveillance practices in general – thus on the one hand changing the subject of research to the citizens and on the other hand opening the field of surveillance from specific CCTV practices to wider surveillance practices. Krasmann and Kühne (2014) for example analysed the social acceptance of digital fingerprints on IDs in Germany, and draw the interplay between trust and mistrust in technology, as well as fact and fiction in discourses and narratives on surveillance and security used by ordinary people. The researchers interviewed citizens applying for the renewal of their ID or Passport who seldom follow the dichotomy of dystopian visions of control when deciding whether or not to submit digital fingerprints to governmental authorities, but instead reduce "the impermeable world of automated control technologies", making it "imaginable and thus accessible" (Krasmann & Kühne 2014, p.11). Rachel Finn (2011) uses a combination of surveillance and post-colonial studies, focusing her research on how brown people in the USA – specifically young college women of South Asian descent – experience new forms of 'othering' and racism as an outcome of the increased post-September-11th surveillance and anti-terrorism campaign. While especially state surveillance can often target ethnic minorities as a result of being part of a 'suspect population', Finn focused on surveillance practices by ordinary white Americans, Neighbourhood Watches, etc., creating a subjective feeling of being stared at as a result of being South-Asian amongst the interviewees, and produce a 'terrorist' identity.

Research on surveillance practices in combination with control within residential care homes for young people (McIntosh et al. 2010), or respectively towards low-income fathers (Myers & Wilson 2014) shows how 'the controlled upon' react to and resist such form of surveillance. While in a system of governmental institutions like residential care homes for young people, control might appear necessary in some contexts, the research shows that the line between care and surveillance is thin and is often an ambivalent experience for the caretakers and children alike (McIntosh et al. 2010, p. 300). Myers and Wilson specifically show how low-income fathers subjectively feel surveilled by different governmental institutions – Child Support Enforcement, the criminal justice system, and Child Protective Services, how this form of surveillance impacts their privacy and how fathers justify their reaction to surveillance, which often consists of disappearing from the public eye.

An analysis of cultural notions and possible different understandings of surveillance and privacy were researched by Luther and Radovic (2012). The authors have shown how notions and concepts like privacy as well as workplace and public monitoring are perceived by Japanese citizens. A notion of privacy, which is rather understood on a personal level of keeping secrets from others who are close to them, without any societal meaning, also shapes the attitude towards surveillance practices. While state surveillance practices were considered necessary for the respondents, workplace surveillance was rejected. The rejection however relied not so much on an intrusion of privacy but rather on a feeling of distrust from the company towards its employees, as in Japan "companies are often thought to be an extension of a worker's family […] with a hierarchy in place where those in positions of power were assumed to take on paternalistic characteristics" (Luther & Radovic 2012, p.272).

A different methodological approach was taken by the European research project IRISS[3], which has examined the likelihood of ensuring this right of access by trying to submit subject access requests to different private and public organisations which partake in data collection practices. The project brought forth multiple important findings, as already the first steps of identifying the person or the legal entity responsible for the processing of the personal data proved to be difficult in many cases – even though the Data Protection Directive requires a clear identification of the data controller. Upon submitting the subject access requests only 57% of all the requests for access resulted in a disclosure of personal data. Additional information, like the sharing with a third-party or the instalment of automated decision making was often even more difficult to obtain (L'Hoiry & Norris, 2014). Also the qualitative results of the project showed some interesting findings – starting with the lack of information on data collection practices organisations pro-actively provide, over the suspiciousness the researchers as data subjects were confronted with, to the obvious evasive measures some organisations undertook to not have to comply with the regulations, going straight to ignoring the request.

Thus, the IRISS project can show how data controllers deal with subject access requests, where they fail to comply with legal frameworks and what effects this could have on the citizens and their privacy rights. It also creates doubts if a new data protection regulation will really provide citizens with more control of their personal data if under the current legal settings a simple request to access to personal data fails in many cases. While the researchers nicely demonstrate the difficulties encountered with subject access requests, they missed the opportunity to inquire possible reasons for the discrepancy between the law in the books and the law in praxis.

Compared to the studies of Norris & Armstrong (1999) and Hempel & Töpfler (2004), the other studies focus on many different aspects of surveillance, but leave out the surveillance work(ers),

[3] Increasing Resilience in Surveillance Societies

those being “responsible for the daily operation of surveillance” (Smith 2012, p.107). Surveillance work in state-related and private organisations is often neglected in surveillance studies (ibid., p.109), despite surveillance work(ers) being increasingly required by modern bureaucratic organisations – with the increase in occupations needing employees processing, collecting and analysing personal data. Thus, there seems to be a gap in research:

> “[F]ew studies have examined how this labor is situationally enacted, performed, managed, regulated, experienced and understood. Indeed, while the organizational objectives, protocols and logics underpinning surveillance have received significant analytical attention, surveillance workers – with some notable exceptions – are noticeably invisible, their role and significance either presupposed or overlooked by a scholarly collective more concerned with excavating the power relations and socio-political implications associated with new envisioning technologies” (ibid.).

While some of the “notable exceptions” have already been presented above, I will conclude this chapter with some noteworthy studies on the surveillance work(ers), which also influenced my research interest and to which I hope to be able to connect my research. Despite some methodological restrictions and difficulties, mainly that many organisational surveillance practices are preferred to be kept in secret and organisations often having a monopoly over information collections and the access to that information (Smith 2012, p.109), researchers have been able to gain access to surveillance work(ers). Smith (2007) has, similar to Norris and Armstrong, researched CCTV operation rooms through ethnographic observation, examining the surveillance workers’ “interpretations of the various incidents, individuals and social realities observed” (Smith 2007, p.280). Smith shows that operators use a social construction of reality in order to make sense of what is in most instances an ordinary urban image, but also in order to ‘escape’ from the occupational routine and monotony found in CCTV operation rooms. In such instances, CCTV systems can be used as a social medium, where the ‘watcher’ can interact with the ‘watched’ by physically moving the camera for example (ibid., p.292f.). This research further shows how video surveillance operations are largely shaped by the person(nel) sitting in the control room, but also create “a range of measures to counter and negate the predominantly controlling (strategical) gaze of the cameras” by using blind spots of the system or trying to merge with the surrounding people (ibid., p.305f.).

Kirstie Ball (2003) with her analysis of electronic workplace surveillance through computer-based performance monitoring (CBPM) in call centres can also be included into the broader picture of studies focussing on surveillance work(ers). Ball demonstrated in her study the social ordering and value systems in organisations, which are influenced by electronic workplace surveillance:

> "Vertical (by management) and horizontal (through staff competitions) electronic surveillance practices in Norco were situated in a complex network of non-electronic surveillance (appraisal), and longstanding social relations, which […] also performed a crucial categorizing role" (Ball 2003, p.213)

In this context, Ball also indicated that even though the organisation seemed to be practising electronic workplace surveillance in a non-discriminatory way, younger male employees appeared to be favoured nonetheless as a result of the social relations of the department (ibid., p.218).

Finally, a new and interesting empirical contribution to the field of surveillance studies is provided by McQuade (2016), who uses Pfaffenberger's concept of "technological drama" as a framework in order to analyse the effects of (surveillance) technologies in policing through participant observation of meetings and interviews with people who work in intelligence. McQuade aims at capturing the political dimensions of technology and how different police officers from various agencies deal with the conflicting positions which emerge through the introduction of new (surveillance) technologies (McQuade 2016, p.14).

These studies aiming at the surveillance work(ers) thus try to shed some light on how surveillance is performed focusing on organisational, cultural aspects, but also on how they are influenced by political decisions, which are often implied on the surveillance workers. As such, contributions focusing on the surveillance work(ers) can also provide insight in why different surveillance practices are the way they are and why in certain instances resisting strategies of the scrutinised might work or not. Taking the case of the IRISS project, which researched how (un-)successful subject access requests are, a research of the surveillance work(ers) can give insight in why these requests failed in so many instances and why these difficulties occurred. Is it a practice which is done on purpose or is this due to uninformed data controllers? Is the legal framework out-dated in such a way that data controllers cannot conform to it as initially intended by the directive, also in relation to the technological developments? Or is it maybe an outcome of the lack of interest from the citizens' side, who rarely address concerns or request access to personal data? Further research of surveillance work(ers) thus can create a better understanding of

> “how biography, memory and organisational positioning influence surveillance worker decision making; [of] the intricate and multi-dimensional social relations in which surveillance workers are situated; [of] the social realities that surveillance workers produce, consume and inhabit, and the embodied consequences associated with human-technology interactivity in general, and the “labour” of watching in particular” (Smith 2012, p.114).

3. Research Question

In the field of Surveillance Studies, there are more or less two shortcomings. I have already presented the first in the previous chapter: surveillance studies scholars have often neglected the empirical analysis of the so-called ‘surveillance work(ers)’, the personnel operating the surveillance technology or performing the surveillance practice. The second shortcoming is more general in the sense that surveillance studies “is heavy on theorizing and light on empirical research” (Zureik 2007, p.114). Although the previous chapter might suggest otherwise and existing empirical research brings forth excellent contributions to the field, “an abundance of nominal (if rarely operationalized) concepts” is lasting, in which “[t]erms such as surveillance, social control, privacy, anonymity, secrecy, and confidentiality tend to be used without precise (or any) definition and are generally, not logically, linked” (Marx 2007, p.125f.).

These two points need to be addressed by new research in the field of Surveillance Studies – providing empirical research with the specific focus on surveillance work(ers). But the relevance of this research is not only based on a lack of such research in the discipline of sociological surveillance studies. My focus on the work of data protection in organisations has also relevance from other points of view. From a general public’s point of view, knowing to what extent your right – in this case in combination with data protection regulations – is really granted and to what extent measures are (not) established by organisation in order to guarantee a functioning data protection is important and enables one to cope with such practices. And also from a political point of view, knowing possible ‘flaws’ between the law in the book and the law in practice is necessary, especially with regard to the new general data protection regulation entering into force in 2018.

This is why this master thesis will focus on the operating of data collection, data management and the protection of such data in organisations, by researching how these procedures are dealt with from a data controller’s point of view and giving insight into the motivation and purpose of the way of operating. As the data controller is generally only the legal entity of the organisation having the authorisation for collecting data in some way (see chapter 6), the research will focus on how organisations handle this legal requirement – either by installing data protection officers, by delegating data processing principles to the IT department, or maybe by not considering specific possibilities of handling data collection and protection. Furthermore, the role of the data collection technology and technology in general will be researched with regard to the management of personal data in organisations. Finally, the relation between the 'surveillance workers' and the data subjects as well as the wider societal implication of data collection practices are important to be analysed. This leads us to the following research question:

How are data collection and data protection practices managed and negotiated within organisations, facing an entanglement of these practices with legal, technological and societal implications?

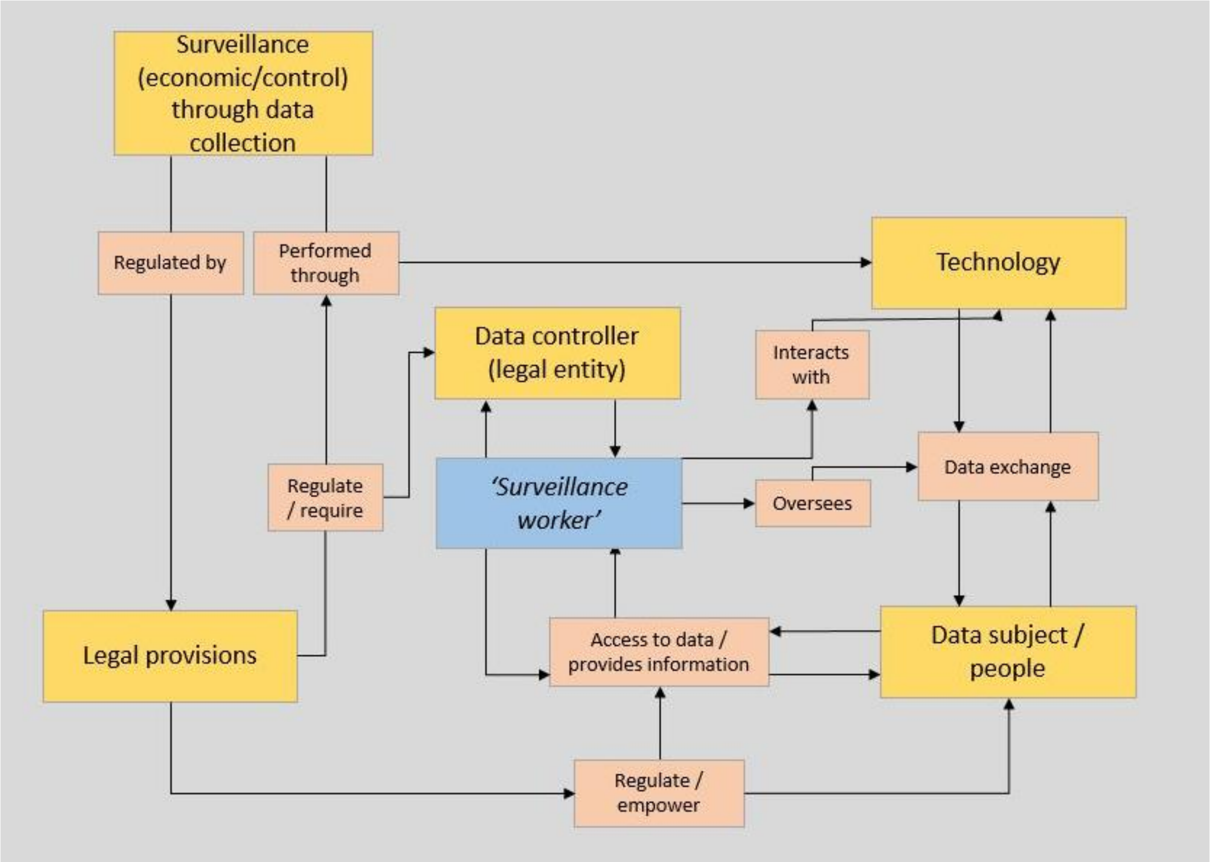

Figure 1: The surveillance worker in data collection practices

Figure 1 gives a first abstract idea of the – complex – process behind data collection. This sketch is a theoretical assumption which forms the basis of the research question presented above and the sub-questions presented below. Surveillance is in this case performed through the different data collection practices in the organisations. The yellow boxes represent the different individuals, regulations and technologies involved in the surveillance practice – thus the factors shaping surveillance. The smaller rose coloured boxes represent the different processes, acting between the individuals, regulations and technologies of the data collection.

Generally, these data collections are within certain legal limitations, demarking the allowed and not allowed practices. These legal provisions for example authorise the data collection through a so-called data controller, who is legally responsible for the collection in question – often the CEO of the organisation. But also the rights of the data subject/people in relation to the data collection are regulated, or the technical means by which the collections are performed (including e.g. relevant technical standards etc.). The focus of the research here is on the data controller and the other 'surveillance workers' included in the data collection practice – highlighted in 'blue' in Figure 1. Supposing the data controller delegates the data collection processes to different parts of the organisation, 'surveillance workers' determine and shape how personal data is collected, treated and protected – "overseeing" the data exchange between the data subject and the data collection technology, interacting with the technology, but also serving as access point for the data subjects in cases of concerns, subject access requests or necessity for information in general.

There is thus a range of further sub-questions which relate to how data collection practices are managed and negotiated within organisations:

- How is knowledge on data collection and protection produced and managed by 'surveillance workers' in private as well as public organisations and within the organisation institutionalised?

Since data collection practices are regulated by legal provisions, the knowledge on how to deal with these provisions needs to be managed in some way – it needs to be acquired and constantly updated. Specific knowledge can be institutionalised within the organisation – employees with experience and knowledge are a valuable asset for every organisation in which the transfer of this information to other employees needs to be guaranteed. An advantage in knowledge can be crucial when competing with other organisations, or when trying to manipulate lay-people. Gaps in knowledge, however, can be problematic, especially when challenged by others. 'Expert' lay-people for example – informed citizens who are aware of their rights and know how to execute them – but also the technology itself can challenge missing knowledge. This research will thus try to analyse how experience and knowledge in regard to data collection and data protection are managed in private and public organisations.

- How do 'surveillance workers' handle problems – dilemmas, conflicts, or crises – encountered in their day-to-day operations?

This sub-question indirectly relates to the previous question, as dilemmas can be a result of lack of expertise. However, it doesn't specifically need to be related, which is why the conflict resolution is considered specifically. Conflicts can be manifold – resulting from internal or external input, technical nature or psychological nature, conflicting with legal requirements or with ethical and normative concerns and resource problems– and thus should also be analysed in their broadness. This also does not only involve the management of actual crisis, but also means to prevent and circumvent such events, or cope with the outcome and implications.

These are the main questions I bring forth to the research subject and they are expected to be answered throughout the empirical research in my thesis. In order to address these questions, I envision conducting expert interviews with 'surveillance workers' – people involved in data collection and/or data protection in organisations. Even though the empirical part of the research is a qualitative approach, the strict inductive approach – leading from specific cases to a specific theory – is not aimed at here. Though entering a field of research without theoretical pre-knowledge and as objectively as possible is – in theory – ideal for researching the field in its integrity, it is an approach which is not feasible in practice, which is why I rather call for the pragmatic approach of *abduction*, "the complementary and constant dialectic between inductive and deductive theoretical development" in which we constantly move from theory (re)construction to empirical data collection and analysis and back (Pearce 2012, p.832f.). While the pragmatic approach initially serves as a validation for mixed methods researches, it is not limited to it. Instead it suffices to acknowledge that every research method has its advantages depending on the requirements and research questions and the strength can lie in a variety of methods – or using the words of Bourdieu:

> "The division between "theory" and "methodology" establishes an epistemological opposition an opposition that is in fact constitutive of the social division of scientific labor at a certain time (…) [and] I believe that this division into two separate instances must be completely rejected", in which also a combination of methodological approaches "will be hailed as a breakthrough and a daring challenge to methodological monotheism!" (Bourdieu 1992, p.223f.).

And although I will not be able to choose a mixed methods approach here – mainly due to pragmatic reasons of a lack of capacities – the general idea and the paradigmatic approach serve as guidelines for my research here.

4. STS – Surveillance, Technology and Society

This chapter presents the theoretical background of the study upon which the empirical data collection and analysis will rely. The work of data collection and protection in organisations cannot be analysed from a surveillance studies perspective alone, since there are many different components influencing these processes. An STS approach – in the sense of bringing together Surveillance, Technology and Society – will thus be more suitable. Although the theoretical framework should be understood as a melting pot of the three aspects, each of them will be introduced separately. Starting with the location of surveillance in ***sub-chapter 4.1****, I will not only introduce the main trends in the field of surveillance studies but also specify which of these appear more suitable for this study and why. In* ***sub-chapter 4.2*** *the surveillance aspect will be complemented by a technological aspect, introducing a more STS (in this case Science and Technology Studies) and Actor-Network Theory (ANT) focus on surveillance, which will be completed by the societal reactions to surveillance and technology in* ***sub-chapter 4.3****.*

*****

Surveillance, technology and society are strongly interconnected, as we will see throughout this chapter. Surveillance heavily relies on technology in order to be able to perform (Marx 2002) and society nowadays is also deeply focused on technology in almost all aspects of functioning. Vice-versa technology is also not only a mere product or system based on different components like modules, sensors, processors or, in its simpler form, screws and cogs, but technology is also the result of different inscriptions by designers, producers, users, and historical and cultural developments – all in all a socio-technical assemblage. In order to concretise this initial thought, I will work through the three different aspects, trying to locate each of the components within their interconnection.

4.1. Locating Surveillance – Who, where and how?

The meaning of 'locating' surveillance is essentially to address the following aspects when analysing surveillance here: What exactly is surveillance – how do different scholars understand surveillance and with which understanding can I work? Also the question of who is involved in surveillance should be concretised here, limiting the field of the surveillance worker. During the theoretical research for my thesis, I worked through a lot of definitions and definition-attempts of surveillance, some of which I deem suitable for my research, while other definitions don't appear to fit my concept of surveillance, without wanting to negate their importance and validity in the surveillance discourse. Thus, while in the next chapters the focus will mostly lie on trying to draft a concept of surveillance which fits the purposes of this research, digressions to other definitions will be provided in order to clearly delimit the conceptual framework of surveillance. Furthermore, in regard to the research questions above and the focus on the role of data collection and data protection practices, the concept of dataveillance as coined by Roger Clarke (1988, 1997, 2012) and the relationship between surveillance/dataveillance, privacy and data protection will also be introduced.

While surveillance as a research field is not entirely new, the changing technological developments and the emergence of the term "risk society" which tries to find a balance between trust and risk (Beck 2015; Giddens 1999) have not only created the idea of a "surveillance society" (Lyon 2001) but also an increased interest in this research field within the last decades. Technology has had many impacts on surveillance, not only in the methods of surveillance, but also in the relations between the surveillance performer and the ones which surveillance is aimed at, the power-balance between the two as well as the societal and cultural reactions towards surveillance. Surveillance has also gained in popularity in political discussions and is here often perceived in a twofold way – either as an absolute necessity for providing security against external threats, or as a danger for modern societies eroding the citizens' privacy.

Studying surveillance from a social sciences point of view has the aim of conceiving the relationship between the ones ordering surveillance and the ones who are under surveillance, conceiving the effects and consequences of surveillance. Also here surveillance can be perceived in multiple ways – as a coercive praxis delimiting the freedoms of individuals vs. legitimate means of care (for example watching the activities of your neighbours in order to see if something unusual happens). It thus can be argued that watching over/surveilling someone is a normal practice (Tschohl et al. 2016, p.32) and when considering the historical and cultural background this is also observable. In rural towns or within close family ties, the practice and in further instance also the consequence of surveillant activities is different as opposed to the same activities in an anonymous setting of modern societies – like a large city. While in the former, the practice is a horizontal one in which generally everyone can watch everyone, in the latter case surveillance is strictly hierarchical in which only a few (governmental as well as private) actors actually have the means of performing surveillance (ibid., p. 33). Each of these have different implications and thus require a closer scrutiny.

Considering this it is not surprisingly, that different concepts of surveillance have emerged within the field of surveillance studies (Allmer 2012a, 2012b). On the one hand definitions on the basis of Foucault's panopticism of surveillance stress the repressive disciplinary notion of surveillance as a result of power-inequalities (e.g. Zuboff 1988; Poster 1990; Elmer 2003, 2004, 2012; Bigo 2006, 2008; Bogard 2012). This can be complemented by a political economic approach, which can be found within the critical surveillance studies, framing surveillance as an important factor in the accumulation and production of surplus value and profit (see e.g. Allmer 2012a, 2012b; Fuchs 2008, 2010; Sandoval 2012, Heyes 2012). On the other hand, a general understanding of surveillance stresses the technical process of surveillance as forms of data collection, with flexible roles and not solely as means of exercising power (however without refuting the possible negativity of the character of surveillance) (e.g. Giddens 1985, 1995; Marx 2002, 2008; Clarke 2012; Lyon 1994, 2001, 2003a; Norris and Armstrong 1999a).

It is along this division of panoptic surveillance and the broader understanding of surveillance where I will present the theoretical analysis of surveillance. But first I will start with a working-definition of the term of surveillance.

4.1.1. A working-definition of surveillance

Especially for new readers in the field of surveillance studies, the definitions introduced by Roger Clarke (2012) are suitable for getting a first grasp of the concept of surveillance, as he opts for a rather simplistic, almost schematic approach when defining surveillance. Clarke defines the general meaning of surveillance as the "systematic investigation or monitoring of the actions or communications of one or more persons", and then goes further by graduating between *personal surveillance* aimed at specific persons, *mass surveillance* aimed at (large) groups of people and *Überveillance* as the "[s]urveillance of a feature of a person, or of an artefact that is very closely associated with a person included embedded within the person's body" (ibid.). Finally, the term *Sousveillance* – initially coined by Mann et al. (2003) as "inverse surveillance" – means the usage of surveillance as a countermeasure.

Continuing with this systematic approach of defining surveillance, Clarke also lists different forms of surveillance, ranging from *physical* surveillance by the means of sensations like "vision and aural", through *communications* (monitoring messages) and *data* (using personal data systems) surveillance, to *locating/tracking* surveillance which focuses on data revealing spatial information and *body* surveillance in forms of measurements of bodily aspects of a person (as a form of Überveillance). Another form of Überveillance is the *omnipresent/omniscient* surveillance as the "integrated application of multiple forms of surveillance" (ibid.).

Although this method of surveillance definitions might be useful for obtaining a first understanding of the matter, it is worth to be extended a bit further. A more comprehensive definition of surveillance can be obtained by using an etymological approach. The origin of the word surveillance lies in the Latin word *vigilare*, meaning to keep watch, which in further consequence can be found in the French word *surveiller* (Marx 2011, p.85). Keeping watch as a translation of surveillance shows a more historical understanding of the word surveillance than it might be the case nowadays. Considering the instinctual awareness which is generally attributed to keeping watch, we see that the act of 'surveilling' is not (or not entirely) done consciously. This is what Gary T. Marx also calls *non-strategic surveillance.* Within *strategic surveillance,* however, the act of surveillance underlies a certain self-consciousness in which the intention and effort are much more deliberate than in the non-strategic surveillance (ibid, p.86). It is this connotation of the word surveillance which is also closer to the French meaning of *surveiller* as in *observer avec attention*, *examiner* or *contrôler* (Centre Nationale de Ressource Textuelles et Lexicales) – meaning to observe with attention, to examine/investigate, to control.

It is within this strategic surveillance in which Marx also situates the *new social surveillance*, which not only includes the conscious act of surveillance, but also involves the usage of tools which increase senses and perception in order to enhance the range of surveillance. Or, to use Marx's words, new social surveillance is "the scrutiny of individuals and contexts through the use of technical means to extract or create information" (Marx 2011, p.89). This modern definition of surveillance implies the usage of technological tools in order to effectively perform surveillance. Particularly in the wake of technologies of data collection, which accumulate ever more personal data, in greater detail but also less noticeable, this emphasis on technology in surveillance definitions is important (Marx 2002, p.9). Furthermore, the definition introduced by Marx suggests that surveillance doesn't have to specifically address individuals known beforehand, but can also be intended at contexts – different settings, patterns of relationships, places and spaces, time periods, networks and settings (Marx 2011, p.88f.).

Clarke's more general definition of surveillance primarily understands the act as a systematic monitoring of actions and communications of a person, which then starts to specify by adding technical means enhancing the monitoring techniques and also not solely aiming at persons anymore. It is only the latter aspects of Clarke's definition of surveillance which are included in Marx's definition of new social surveillance which inherently requires specific tools for monitoring and aims at humans and contexts alike. It is also on the basis of the senses where both definitions come together. Although Clarke (2012) mainly introduces the requirement of sensation – especially visual and aural – in surveillance only at the level of physical surveillance, Marx further adds senses as touching and smelling, even though he also specifies that the vision remains the most important sense in the context of new social surveillance (Marx 2008, p.88f.).

Within the next chapters a profounder analysis of the act of surveillance – *as the monitoring or scrutiny of individuals and groups of people, their actions and communications, as well as their different contexts by technological means in order to extract specific information* – will enhance the understanding of the broader subject of research in this matter. Having defined the key words and the basic concept of surveillance mainly serves to further allow the analysis of what surveillance is, how it is performed and who is involved in the surveillance practices, but also the implications of surveillance.

4.1.2. Typologies of surveillance

The heading of this sub-chapter already suggests that surveillance can be classified based on different characteristics which one assumes to be prevalent. As I mentioned in the introduction of this chapter, three main concepts or typologies of surveillance can be observed upon reading the different theoretical approaches in the surveillance studies. Although they don't differ that much, it is one specific trait which bears the main point of divergence between the positions: the connotation of surveillance, i.e. if surveillance is intrinsically a negative practice or if there are also neutral/positive aspects of surveillance.

Panopticism and Critical Surveillance Studies

Probably the most discussed and best-known historical contribution to the field of surveillance studies is the theory of modern panoptic surveillance by the French philosopher Michel Foucault. Mainly in his work *discipline & punishment*[4] (1977), Foucault describes the disciplinary power exerted through surveillance practices. The metaphor used by Foucault as a reference for surveillance is the Panopticon which relies on the interpretation of the architectural concepts and political project of prisons/closed institutions of the English social reformer Jeremy Bentham (1748-1832). The Panopticon by Bentham is the concept of a prison with a panoptic tower at the centre, from which, in theory, every corner of the prison can be watched without the watcher being seen by the inmates. As such, the prisoners (or inhabitants, students, patients, if converted to other 'closed' institutions) can be under constant observation by the supervisor without exactly knowing if and when they are observed. It is this "*apparent omnipresence* of the inspector (…), combined with the extreme facility of his *real presence*" (Bentham 1995, p.12) which constitute the powerful surveillance character of the Panopticon and as such require no real form of coercion, especially within the practise of institutional violence (Elmer 2012, p.24).

While the Panopticon by Bentham mainly focused on the *watcher*, Foucault laid his conceptual perspective on the ubiquitous surveillance as a result of power mechanism for which the Panopticon serves as an ideal-form (Foucault 1977, p.205), having its main function in establishing discipline. Discipline requires a mechanism of hierarchical observation, in the form of "techniques that make it possible to see induced effects of power, and in which (…) the means of

[4] Interestingly, the French original title of the work is *surveiller et punir* (1975). Instead of using the verb *surveiller*, for which the English version of 'to surveill' finds no mention in the dictionaries (Marx 2011, p.85), the translated version of *surveiller et punir* replaces the act of surveillance by the outcome of surveillance in the Foucauldian sense, which can be described as obedience or *discipline*.

coercion make those on whom they are applied clearly visible" (ibid., p.170f.). It is this form of disciplinary power which is surveillance for Foucault (Fuchs 2011, p.115). The analysis of Foucault is of historical nature, which is what needs to be kept in mind when trying to transfer the Foucauldian concept of the Panopticon on the surveillance concepts of today.

It is also against the background of this historical perspective that the concept of disciplinary power has been further developed, with a short but important contribution by Gilles Deleuze which sees a replacement of the disciplinary character of surveillance. In Deleuze's *Postscript on the Societies of Control* (1992) it is the concept of *control* which he sees as the main point when expanding Foucault's Panopticon to the digitalised, data-driven surveillance (Elmer 2012, p.26). For the pre-modern discipline societies, spaces of enclosure facilitated the amassing of power and knowledge. Foucault already recognised a change within discipline societies due to the transience of spaces of enclosure (Deleuze 1992, p.3). As Deleuze brilliantly puts it, "enclosures are *molds*" (ibid., p.4; emphasis in original), strict and rigid forms, which were challenged by the ever-changing environment of globalisation – especially of the capital – and technological development (Bogard 2012, p.31). However, "controls are a *modulation*, like a self-deforming cast that will continuously change from one moment to the other" (Deleuze 1992, p.4; emphasis in original). It is the modular which is needed in order to adapt to changing environments. These mechanisms of control, according to Deleuze – electronic monitoring of prisoners, perpetual training and corporations in schools, as well as the corporate system – are at the "substitution for the disciplinary sites of enclosure" (ibid., p.7).

Many other authors have found use in the critical notion of power inequalities, discipline but also control of Foucault's notion of panopticism and the development of the concept by Deleuze, when characterising surveillance, but also more generally for characterising contemporary societies. Examples are the panoptic character of information technology at workplaces in corporations, enhancing the surveilling effect of control and authority at workplaces by Shoshana Zuboff (1988), Mark Poster's notion of the superpanopticon (1990) in the wake of the endlessness of panoptic possibilities due to the technological development and consumer surveillance, or more recently Bigo (2006) coining the term of the ban-opticon in order to describe the global state of insecurity as a result of the events of 9/11 and the propagated 'war against terrorism' which in turn require a state of global policing and an increase in secret services and surveillance.

Opting for a similar approach, Foucault's Panopticon is used in the field of critical surveillance studies, which combines the panoptic idea of domination and control, as well as the asymmetrical power relations with economic surveillance in the form of resource control and exploitation. Critical surveillance studies see "the connection of surveillance with the modern state, media and technology, ideologies, hegemony, class struggles, and alternatives to surveillance society", or, to put it 'simple', the combination of surveillance studies with Karl Marx's critical theory (Fuchs 2015, p.6). A critical, Marxist analysis of surveillance integrates important concepts into the field of surveillance studies, especially the economic nature of many private/corporate surveillance practices – which can also be applied to state/governmental surveillance practices.

One of the main concepts of critical surveillance studies is the assumption of an inherently negative aspect of surveillance as a result of fundamental power asymmetries and in relation to the repressive power of capitalism and the state (ibid. p.7). According to Fuchs (2011, p.128), surveillance has the function to benefit certain groups at the expense of others through coercive means. It follows the reason of competition and aims at the prevention or influence of certain behaviours amongst groups or individuals by those with more power and capital. From a more repressive point of view, this is done by "gathering, storing, processing, diffusing, assessing, and using data about humans so that potential or actual physical, ideological, or structural violence can be directed against humans" (ibid.). From a more economic point of view, surveillance and monitoring of individuals and groups is solely based on financial means, assigning value to objects/information which then can be exploited (Elmer 2012, p.28) and is thus an important aspect for ensuring the creation of surplus value and accumulating profit (Allmer 2012, p.47). This form of economic surveillance has especially seen an important increase with the development of new information and communication technologies, particularly with the internet (Allmer 2011, p.581).

It is the panoptic concept of surveillance which is considered to be predominant. Even though surveillance technologies are not centralised anymore – as it was described by Foucault – the dominant actors of surveillance technologies in the form of states and corporations accumulate centralised power, creating disciplinary economic and political behaviour (Fuchs 2011, p.120f.).

Hand in hand with the critical analysis of surveillance also goes a critique on a more general – or as Fuchs (2011, p.111; 2015) calls it – neutral concept of surveillance. Due to the assumption of all surveillance being fundamentally negative, a neutral concept of surveillance is not possible, as it always involves power inequalities. According to Fuchs (2011, p.130) it is not the level of technology which determines the surveillance character (as e.g. Gary T. Marx puts it (2011, p.88f.)), but rather the social structures behind the surveillance operation: Is the outcome of the surveillance technology beneficiary to all, or does it cause domination and exploitation? According to Fuchs (2011, p.126; 2015, p.7), the analysis of repressive forms of surveillance is not possible if we accept a normalisation of surveillance, thus if every form of data collection is considered to be surveillance.

Although a critical analysis of surveillance studies practices and the inclusion of Marxists' theory in combination with surveillance has to be welcomed as it can contribute importantly to the field of surveillance studies, I however see only limited applicability. While the contribution prominently shows the dangers in relation to surveillance, especially in situations where power inequalities are predominant and surveillance is (solely) used to dominate and repress certain groups or individuals, I would not consider this to be the main analytical aspect of surveillance. I also do not agree with some of the critique on the 'neutral' concepts of surveillance. Especially since many differentiations also exist in the general concept of surveillance, which do not automatically reject a negative reading of surveillance – as Fuchs hints in his more presumptuous criticism when questioning "the existence of something called "surveillance studies" as opposed to a critical theory of society" (Fuchs 2015). Before we go deeper into this critique on the general surveillance studies, I will first proceed with what is meant by this and how surveillance is perceived here.

General Surveillance Studies

Taking into consideration the definition I suggested in the first sub-chapter, the *extraction of specific information* is a key aspect of surveillance practices. If we now use a more general analytical focus on the concept of 'surveillance as information extraction', the twofold tendency of negativity and neutrality is apparent.

Surveillance, Democracy and the State

The relationship between surveillance and democracy, as Ball and Spiller (2014), but also Haggerty and Samatas (2010) have established, can serve as a good example of why surveillance is not necessarily negative, while bearing severe tendencies towards negativism. Democracy is not only a governmental system which "involves a system of open procedures for making decisions in which all members have an equal right to speak and have their opinions count", but "it is also an idea, a doctrine, a set of institutional arrangements, and a way to rely to others" (ibid. 2010, p.1f.). Within this, democracy can be influenced by surveillance in a twofold way. Surveillance can facilitate democracy, "it runs through the information infrastructures which, for example, help to target welfare at the most needy, facilitate democratic participation through voting and distribute public resources efficiently" (Ball & Spiller 2014, p.11). Surveillance in these instances – through its information extracting and processing – serves a bureaucratic, administrative and controlling purpose.

This form of surveillance as part of bureaucratic procedures in public and private administration can already be found in Max Weber's (1980; first issue 1922) analysis of bureaucracies as legitimate forms of domination. Although not specifically mentioning the surveillance character, Weber describes the power constellations existing in bureaucracies. According to Max Weber, power means "the probability that one actor within a social relationship will be in a position to carry out his own will despite resistance, regardless of the basis on which this probability rests" (Weber 1968, p.53, English version), which can either be authoritative but legitimate – or coercive through force. Adding the term of 'domination' (Herrschaft) as "the probability that a command with a given specific content will be obeyed by a given group of persons" (ibid.), Weber describes the purest form of legitimate domination as the one exerted through the modern bureaucratic administration (Weber 1980, p.124), with clear principles of hierarchies and official channels (ibid., p.551) commanding the technical most advanced instrument of power (ibid., p.572). However, according to Weber, this does not imply if and how bureaucracy can emphasise a specific perception on the social construct they concern (ibid.). While this relates to the ideal-typical forms of bureaucracy, Weber also recognises the difficulties and problems of strong bureaucracies, related to secrecy and non-existing transparency, as well as the strong retention of power of bureaucratic administrations against others like parliaments and even monarchies (ibid., p.572ff.).

If we contrast Weber's notion of bureaucracy with the panoptic surveillance of Foucault (and later readings of panoptic or critical surveillance studies), we also find a certain divide between the concept of power and domination. While no one denies the existence of power inequalities and forms of domination, they are not considered inherently negative in Weber's description of bureaucracies, but rather as a necessity for a functioning administration in its ideal form, but with certain constraints in real situations.[5] It is in this approach that bureaucracy is seen as an effective and durable state of surveillance – alternating from neutral, necessary administrative practices to specifically negative practices of surveillance: processes of tax collection, defence, policing, welfare, intelligence (Lyon 2003b, p.167).

Furthermore, it is interesting that Orwell saw surveillance partially as a result of bureaucratic procedures (Lyon 2015, p.141), too, which thus, recalling Orwell's most famous novel 1984, can show how democracy on the other hand can also be challenged by surveillance practices. Monitoring techniques can trigger fears of expressing opinions, hinder certain activities or movements, altering the way of participating in public and political debates, which can especially occur in authoritarian, but also in democratic societies (Ball & Spiller 2014, p.11). The sheer reach and possibilities of such monitoring techniques were disclosed three years ago by Edward Snowden, who clearly revealed *how* governments engage in such large-scale population-monitoring practices (Lyon 2014, p.2). The Snowden revelations have heavily influenced the discourse in the field of surveillance studies, but also advanced the discussion on surveillance practices in a more public arena.[6]

[5] Weber also did not consider bureaucracies as inherently positive. Wolfgang Mommsen (2004, p.180ff.) has provided a comprehensive analysis of Weber's critique on bureaucracy as compared to his ideal-form of bureaucracies as the technically perfect form of domination.

[6] It needs to be noted however that already previous surveillance-related events have influenced the discourse amongst surveillance studies scholars, be it through revelations on state surveillance or workplace surveillance (Lyon 2015, p.142). The mass-surveillance of the ECHELON program by the so called "Five-eyes" – an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States – was e.g. subject of a European Parliament investigation in 2000 and 2001, which considered the existence of such large-scale communication interception systems as given (European Parliament 2001, p.11). Also the terrorist attacks in the 2000s as a justification for national security related surveillance (Lyon 2001) as well as the increase in Big Data analytics (Lyon 2014) have found analysis amongst surveillance scholars. The Snowden revelations however brought forth surveillance "on the radar of most ordinary citizens" (Lyon 2015, p.142).

Surveillance technologies can also challenge democracy by how they are developed, implemented and governed (Haggerty and Samatas 2010). The configuration of (new) surveillance technologies is mainly located in commercial surroundings, isolated from public influence and only partly subject of the political debate. The development rather responds to a strict economic demand with the aim of creating profit through the research and development of new techniques (Ball & Spiller 2014, p.12; Haggerty and Samatas 2010, p.10). Implementation of surveillance techniques and thus heavily influencing the demand side of technology development are – particularly in recent times – policy responses to different crisis. Surveillance mechanisms for security reasons have seen an increase in instalments ever since the 9/11 terrorist attacks in the United States (Lyon 2001) and they haven't diminished but rather gained more competences and a broader reach in response to each new crisis. More recent examples are the terrorist attacks in Europe which happened in the last two years. These were followed by an increase in secret-service competencies, even more surveillance technology instalments at critical places (e.g. airports, subway stations), but also more draconian legal regulations – not to mention the on-going state of emergency in France granting special powers to the executive forces which have not only seen implementation against potential terrorist threats, but also e.g. against individuals and political groups protesting against the proposed work legislations (Zaretsky 2016). This form of surveillance development, implementation and governing can thus only seldom be critically challenged by the public, since the practices are not accountable and transparent, they cannot (or only partly) be negotiated and they are often implemented as a long-term solution for short-term crises – providing a rather negative example for the concept of integration by crisis (see e.g. Vobruba 2014, p.14f.).[7]

Again in this context, the Snowden revelations contribute important insights into the surveillance operations and form the basis of a re-thinking of surveillance in the technological 21st century (Lyon 2015, p.140). The practices of the NSA and other agencies like the GCHQ have brought forth evidence of three important aspects of surveillance. First the mass surveillance of governments on their own citizens; second the "public-private-surveillance-partnership"

[7] The concept of integration by crisis can mainly be found in political European Studies which assumes that as a result of crisis – e.g. financial crisis – the (institutional) integration of the European Union is strengthened. Since situations of crisis require rapid interventions, also unpopular decisions are seldom challenged by the public, often due to missing transparency. These interventions tend to outlive the crisis. Examples can be an increase in competencies of European institutions in order to be able to cope with the crisis which aren't revoked afterwards. Similar tendencies can be observed regarding surveillance practices and technologies as a result of security crisis.

(PPSP), where, among others, large internet companies share their ‘customer-data’ with governments; and third is a participation of citizens in their own monitoring through the usage of the private companies and participating in (online) communication (ibid., p.141).

The revelations of the NSA documents show a form of surveillance which is best to be described as mass surveillance in terms of general and large-scale information or data collections, including meta-data such as IP addresses, call durations, etc., on the basis of which targeted surveillance is performed in order to being able to identify and locate suspects (ibid., p.140). These practices have some important implications, which need to be addressed in order to further understand the concept of surveillance, as well as their reach. Collecting and sharing these mass amounts of data blur several lines and by this complicate the mundane understanding of data collection and surveillance.

Mass surveillance and the ‘cooperation’ of intelligence agencies blur the line of what is national and what is not, and this also in several ways (Bauman et al. 2014, p.125). Although this problem has already arisen with the digitalisation of communication through the internet, not knowing what kind of data is gathered and where it is processed, it is intensified if personal data is furthermore shared with intelligence agencies in different countries (or amongst the Five Eyes). Especially relating to national and international security it creates the paradoxical effect of data gathering and analysis for the national security, but which is no longer exclusively limited to the national. As has for example been documented by the NSA-leaks, intelligence cooperation from a US-point of view is categorised between Tier 1 countries (the Five Eyes) and Tier 2 respectively Tier 3 countries. This shows the ambiguity of intelligence and sharing: While the Tier 1 partners have agreed to share their data and in return do not spy on each other, the cooperation with Tier 2 countries includes data sharing and other surveillance projects, while continuing to spy on each other. This involves in further consequence a transformation of national sovereignty in what Didier Bigo (2001) calls the ‘Möbius ribbon’ or ‘strip’ (Bauman et. al. 2015, p.126) – “the merging of internal and external security” (Bigo 2001, p.5), in which national security is “inside out”, while there is an “outside in” mass surveillance of own citizens (Bauman et. al. 2015, p.126).

Closely tied to this point is a newly evolved geo-strategical power for countries with strong IT-infrastructures. This becomes apparent when considering the powerful position the United States have managed to obtain by accumulating almost all major (western) internet-corporations geographically on their territory, and thus being able to access a large part of the global internet traffic. The Snowden leaks document for example the voluntary or forced cooperation of the NSA and the British GCHQ with private internet and telecommunication providers such as Microsoft, Google, Facebook, Apple, Vodafone, BT, etc. (ibid., p.123f.). Countries with direct or indirect access to this kind of data have a strategic advantage over countries without access. The same goes for countries who have an important internet data hub on their territories, since national security agencies have been linked to accessing these data streams directly, for example GCHQ's Tempora program accessing and intercepting data streams from the UK to Western Europe; the French DGSE intercepting data of underwater cables from their military base in Djibouti; the German BND intercepting from the largest European data hub in Frankfurt, etc. (ibid., p.122).

Mass surveillance also blurs the line of public and private data collections, which in further consequence also has implications on legal understandings of privacy and data protection. The extent to which internet corporations share their data with national security agencies was probably the most surprising outcome of the revelations by Edward Snowden, which has led to important reflections in terms of data protection legislations. Especially within the European Union, considerations of keeping data streams out of reach of American companies and isolating data storage on European soil aim at creating digital borders as a reaction to this "public-private-surveillance-partnership" (ibid., p.130). The result of this is a form of digitised geopolitics in a global digital realm.

Regarding the legal implication of data protection, it is obvious that mass surveillance, which by its nature initially targets every data subject, contradicts the Human Right of respect for privacy (which has also been confirmed by the Human Rights Court) (ibid., p.132). However, it also seems as if the existing legal requirements have so far not been effective enough in guaranteeing the assertion of the right to privacy. It thus becomes clear that the current data protection laws are heavily challenged not only by the mass surveillance practices, but also by the technological aspects of the digitalised global. Furthermore, it becomes ostensible that the law – in this case data protection and privacy – can also only be as strong as its enforcement. Both for the public as well as for the private partner in the global surveillance practices, legal consequences have been minimal so far. As an example, although the Court of Justice of the European Union declared the European Commission's US Safe Harbour Decision – which considered the data protection principles to be the same in the US and the EU[8] – to be invalid as a

[8] This is mainly of importance for data transfer from the EU to the US by international corporations like Facebook and Google with subsidiaries located in the EU.

result of the NSA practices (Court of Justice of the European Union 2015), a new set of principles between the EU and the US called the EU-US Privacy Shield is currently being negotiated, improving the principles compared to the Safe Harbour but still being flawed on several levels (see Article 29 Working Party, 2016). Also the forthcoming General Data Protection Regulation, replacing the old 1995 Data Protection Directive, has to prove if it can really take on this strong challenge of global mass surveillance and 'loose' technology in terms of data collection.

Strictly commercial

Although the above analysed surveillance practices have shown the blurring line between state/governmental surveillance and consumer/customer surveillance, it is worth having a closer look at surveillance practices by private corporations as well. It should be noted however that the focus of analysis in this context is more on the surveillance practices of corporations with the purpose of profit increase, or as a sole business model, and not so much on the economic side of the "surveillance-industrial complex" as a reaction to the surveillance society (see Ball & Snider 2014).

Consumer surveillance is, similar to state surveillance, certainly not a new development and has already been discussed widely amongst surveillance studies scholars. The example of Customer Relationship Management (CRM) nicely reflects one of the main aspects of consumer surveillance in terms of how it's done and what the implications are. CRM is the analysis of consumer data, i.e. what is bought, how the products are used, etc., in order to be able to characterise consumer behaviour and in further consequence – ideally – being able to attract new customers while retaining the existing ones. In short, it involves the creation of "statistical consumer profiles" (Ball et al. 2010, p.113) and it can be observed in its simplest form with loyalty cards. The analysis of loyalty card data serves on the one hand to get an idea of general consumption trends, while on the other hand specific consumer-related surveillance is probably the more powerful tool of the produced data by these schemes.

The usage of loyalty cards and the participation in such consumer data providing schemes are often considered as a "bearable nuisance" by customers – knowing without exactly knowing that you share your personal consumer data globally but still being used in order to profit from bonuses or discounts (Fischer et al. 2014, p.41ff.). Other possible benefits for customers can include personalised and customised products and services, while companies have ways of enhancing profit through better business performance (Ball et al. 2010, p. 114; Zwick & Dholakia 2004, p. 5f.).

Consumers might not always be aware of the sheer amount of data that can be collected, processed and shared globally in such ways, as the act of providing data is situated locally and only in certain instances (Zurawski 2011, p. 509f.). While the practices of analysing market situations, general consumption and consumer specific patterns might at first seem mundane, it is the asymmetrical information flow (Manzerolle & Smeltzer 2008, p.327) which creates an inequality between the corporation and the consumer. This means that corporations obtain a powerful position of knowledge – "monopolies of knowledge" (ibid., p. 330) – through which they are able to exploit and manipulate consumers. This becomes even more ostensible when considering the increased possibilities resulting from Big Data analytics. Big Data analysis aims at converting the consumer data into actions in order to obtain growth and market expansion, and which also relies on consumer behavioural manipulation. This basically means the transformation of consumer data into "actionable insight" to influence the consumer's actions intentionally (Esposti 2014, p. 210ff.).[9] This relates to what Haggerty and Ericson have described more generally as a 'surveillant assemblage':

> "This assemblage operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct 'data doubles' which can be scrutinized and targeted for intervention" (Haggerty & Ericson 2000, p.606).

The detachment of the personal data from the human is dispersed into a "multiplicity of heterogeneous objects, whose unity comes solely from the fact that these items function together, that they "work" together as a functional entity" (Patton 1994, p. 158), resulting in a disembodiment of the person (Marx 2011, p.88) or a 'decorporalisation' of the body (Haggerty & Ericson 2000, p.611) as well as a detachment of its actions and in the creation of virtual data doubles. In order to know the body (sticking with the terminology of Haggerty & Ericson), it is necessary to have it "broken down into a series of discrete signifying flows" instead of approaching it as a single entity to control it (p.612). The "surveillant assemblage" is interested in "transforming the body into pure information," making it comparable and mobile (p.613) and in further consequence being able to make profit through it:

> "The monetary value of this surplus derives from how it can be used to construct data doubles which are then used to create consumer profiles, refine service delivery and

[9] The problem of Big Data, surveillance and in further consequence data protection will subsequently be addressed in the next section.

> target specific markets. There is a growing trade in the corporate sale of such information” (ibid., p. 616).

However, this does not only have to be reduced to specific customer-related practices like CRM or loyalty cards. This can even more be observed amongst presumably free services on the internet, mainly with social media sites and the like. Users of social media sites are equally seen as consumers, who trade off their personal data for the “free” usage of the sites. This is why internet users should always remember that they are paying for the free services of these sites with their personal data and that also on the internet, ‘there ain't no such thing as a free lunch.’

Privacy and Data protection in a world of dataveillance

It becomes thus more and more clear that surveillance and personal data or data in general are closely tied together. As already stated in the initial working definition of surveillance, the aim of surveillance is an *extraction of specific information* which is mainly available in form of data that can be collected and analysed in order to obtain the required information. Surveillance requires details of people’s records – personal data – for extracting the specific information needed (Rule, 2007). Roger Clarke has coined the term of dataveillance (Clarke 1988, 2003) to describe the surveillance practices that solely rely on personal data: “*Dataveillance* is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons.” Clarke differentiates between two forms of dataveillance: personal dataveillance, which aims at previously identified individual, and mass dataveillance aimed at groups of people of which a certain suspicion exists and certain members of the group are of interest to be identified (Clarke 1988).

While dataveillance may have some benefits, as for example threats detection and in further consequence an increase of physical security of citizens, or related to financial benefits in public and private sectors in terms of taxation or insurance, the dangers of dataveillance most likely prevail. As a result of the disembodiment of the data from the person creating so-called ‘data doubles’ as described above, it is in further consequence also the data double that is monitored and not the specific individual. With data quality not always being entirely accurate and also possibly being incomplete (as the person herself is in general way more complicated as the data double suggests), risks of wrong identification, discrimination and exclusion, but also an increased general suspicion amongst the society are highly possible (Clarke 1988).[10]

[10] The specific dangers of surveillance and dataveillance will be described in chapter 4.3 Locating society, p.48.

Additionally, as already mentioned previously, the emergence of big data has even increased the possibilities and dangers of dataveillance. Citizens as consumers have become used to the trade-off of providing data for ‘free’ services, thus using their personal data as currency (van Dijk 2014, p.198). They are transformed “into leaking data containers” of which data collecting corporations create sophisticated consumer profiles (Kreissl, 2014b, p. 15f.). But this has also created a “normalisation of *datafication*” – meaning the transformation of social behaviour into data – and which is seen as a legitimate way of analysing human behaviour, not only in an economic/profit orientated context, but also more and more in scientific contexts (van Dijk 2014, p.198ff.).[11] The possibilities with big data seem to be endless, the same data is more and more analysed for different purposes (Lyon 2014, p.5), while considerations about the implications often seem to be neglected by practitioners (Esposti, 2015).

Dataveillance in terms of data collection for information extraction however does not operate in a legal vacuum. Data protection legislations[12] provide a framework in which data collection, processing and analysis can be done. The same goes for privacy. Although many Privacy-Invasive Technologies (Clarke 2001) exist, the importance of privacy has not diminished. Privacy is recognised in many instances as a fundamental human right, obtaining strong legal legitimation from Art. 8 of the 1950 European Convention on Human Rights and an even stronger legitimation with the 2000 Charter of Fundamental Rights of the European Union, where also specifically the right to the protection of personal data is mentioned (Galetta & de Hert 2014).

It should be noted that although privacy and data protection target a similar topic, they cover slightly different principles: privacy is based on the “*opacity of the individual*” while data protection covers the “*transparency and accountability of the powerful*” (Bellanova 2014, p.112, emphasis in original). Thus, while privacy can be considered as a normative tool for opacity – drawing the line of where one can interfere with the private life of others – data protection should be considered as a transparency tool organising “the channelling, control and restraint of power” (De Hert & Gutwirth 2006, p.37).

Clarke (2006) more specifically relates to privacy as the “integrity of the individual” distinguishable into four categories: privacy of the person, also known as ‘bodily privacy’ protecting the integrity of the individual’s body; privacy of personal behaviour concerning the integrity of for example sexual preferences, political and religious activities but also of behaviour in private

[11] See also Ruppert et al., 2013 for a good analysis of how *datafication* also challenges contemporary Social Science Methods, without specifically judging the usage of digital data as a means of analysing the social.
[12] An overview of European data protection legislation will be given in Chapter 7, p.63.

spaces such as the home; privacy of personal communication concerning the integrity of a person's communication with others; privacy of personal data, meaning that personal data should not be automatically available to others and that the control over data should remain in the hand of the originating individual (Clarke 2006). It is especially the latter category, data privacy, which overlaps with data protection, also when considering other definitions of privacy like that of James Rule who defines (data) "privacy as the exercise of an authentic option to withhold information on one's self" (Rule 2007, p.3).[13]

Again from a legal perspective, while general privacy concerns are regulated mainly at the level of Human Rights, the data protection principles are codified more extensively and precisely, which is also why these data protection principles are heavily challenged through emerging new technologies and in theory would require a constant adaptation. As such, one can say that:

> "Data protection as it is used today, is the attempt of taming with *legal* means a, through the *economic* mechanisms of the market, propagating *technological* development with vast *social* implications" (Kreissl & Ostermeier 2011, p.281; own translation, emphasis in original).

Recapitulating I

Before continuing with locating the technological aspect of surveillance, I will provide a short summary of what is considered surveillance here. As already previously mentioned, I consider a more general understanding of surveillance more suitable for the empirical analysis in question. Even though a general understanding of surveillance considers some of its aspects as a necessity of social and administrative functioning, it nonetheless has a focus on the *potential* negative implications of surveillance. It is understandable that a general understanding of surveillance potentially bears some difficulties: Treating surveillance too positively may trivialise the truly repressive forms of surveillance, under which people around the world suffer (considering North Korea or The United Arab Emirates for instance). Also including data collection too widely into the understanding of surveillance can blur the line between information gathering and surveillance too much (Fuchs 2011, p.130). These are aspects which need to be kept in mind when using a general concept of surveillance. And although I personally would not go as far as considering the monitoring of a baby by parents as surveillance (Marx 2002, p. 12), I can understand that from a technical or etymological point of view, it is closely related to some

[13] It should however be noted that Rule does not really make a differentiation between privacy and data protection, but instead uses the term privacy and privacy protection exclusively.

concepts of surveillance. At least conceptually closer than with the comparison made by Fuchs (2015, p.7) when considering that the administrative concept of surveillance is having a “Nazi henchman monitoring Jews in Auschwitz who are sent to the gas chamber on the next day (…) on the same definitional level with a babyphone [sic] that monitors a sleeping baby.”

While critical surveillance considers the general surveillance studies theory to include everything into the surveillance concept and by this making it impossible to analyse surveillance at all (Fuchs 2011, p.127), this could also be turned around: considering surveillance as always inherently negative makes it impossible to analyse also necessary forms of surveillance – which do exist – and thus impossible to analyse all possible implications of surveillance no matter of their value. This is probably easiest to be shown with a recent example. The ‘missing map project’[14] is a cooperation between the Red Cross and Doctors Without Borders, with the objective of mapping remote areas in crisis regions using satellite image data. The project is a collaborative and open project, everyone can go to their website or download the MapSwipe App and participate in mapping regions, locating towns, roads and houses. In crisis situations this information helps first responders in knowing where to go, as these places then are not missing on their maps anymore. The project can have a big impact in remote and poor countries which struggle even more in crisis situations. A question which however arises: Is this a form of surveillance? A neutral or even positive form of surveillance? Or is it simply a form of data collection? If one would disregard the purpose of the project, then we have a form of intelligence gathering, of surveillance which is done in collaboration with ordinary citizens and the local communities. The purpose of the project mainly reduces the ethical concerns of the surveillance activity, but it should not be entirely shut out here, too: What happens if the collected data falls into the wrong hands, for example a despotic regime with the goal of eradicating a certain minority? This thus entails questions of data security and data protection, without reducing the potential behind this project and bringing forth a positive example of surveillance. Including such notions in the field of study makes it in my opinion not only more varied but also shows the many different connotations surveillance can have:

> “When this is done we are in a position to analyse variations and also to note factors that may cut cross kinds of surveillance, apart from whether control is *the* defining attribute” (Marx 2011, p.90).

[14] http://www.missingmaps.org/

Thus the previous chapter has shown that surveillance can be found in many areas of one’s life and involves the public/government as well as the private/corporations. I have also already made several connections between surveillance and technology – including in my working definition of surveillance. This is mainly as the technological development has importantly shaped what we consider surveillance nowadays. Particularly considering the dataveillance and big data characteristic, this becomes even more obvious.

4.2. Locating Technology

In comparison to the inclusion of technology for the analysis of surveillance in the previous sub-chapter, technology is the subject of analysis now. A common pattern, which can be observed amongst the classic surveillance studies approaches, is an inclusion of (surveillance-) technology as an agent in the analysis of surveillance, but seldom with a specific focus on how technology is shaped. Thus, while many scholars use a social-constructivism approach towards technology – implicitly or explicitly – these are often not further elaborated (Kreissl 2014b, p.14f; exceptions amongst others are Introna & Wood 2004; Lyon 2003b; Macnish 2012).

However, instead of simply including technology, I will aim at a systematic analysis of (surveillance) technology here, theoretically relying on contributions from the Science and Technology Studies, mainly the Actor-Network Theory. As such technology as a specific subject of analysis is not based on the fact that it is a product or system with different components like modules, sensors, processors or, in its simpler form, with screws and cogs. It is rather because technology is on the one hand socially constructed – socially defined norms and practices are inscribed into the design, embedded in different networks, influencing its functioning – and on the other hand shapes society – actions and communications are influenced by technological development.

4.2.1. Social Construction of Technology shaping the Social

Let’s first have a look at the social construction of technology in surveillance societies. Bruno Latour stated that “technology is society made durable” (Latour 1990, p.103). And according to Langdon Winner, technology should not only be judged by its contributions to productivity and efficiency, or regarding its impact on the environment, “but also for the ways in which they can embody specific forms of power and authority” (Winner 1980, p.121) and thus providing a strong statement regarding political inscriptions in technology. This means that political and in further consequence also social and personal beliefs can be, and are inscribed into the development of technological products and systems. The examples are manifold but in general seldom noticed: The broad boulevards in Paris were purposefully engineered in such a way by the orders of Louis Napoleon in order to prevent street fighting (ibid., p.124). Other examples of ‘technology having politics’ are not necessary implicitly engineered. It also doesn’t need to be a sole political inscription, as it is the case with Napoleon’s order of broad boulevards in Paris. Inscriptions can also be of social beliefs or ethical understanding, they can include prejudices, or they are of ideological nature. Boltanski and Chiapello for example describe ideology as "a set of shared beliefs, inscribed in institutions, bound up with actions, and hence anchored in reality" (Boltanski & Chiapello 2007, p.3) which can be extended to be inscribed in technology as well.

If we take for example surveillance technologies, we can see how social beliefs and ethical understandings can be designed into the technology, by this influencing how it functions and resulting in *socio-technical assemblages* (Haggerty & Ericson 2000). Let's take the specific example of a CCTV surveillance system, which can be operated in several ways. If the video surveillance system is operated by (trained-)personnel, it is considered as a manual operation. This generally has the big downside in terms of "processing power", where a large amount of CCTV cameras need to be observed by a handful of operators, who filter and prioritize information based on their own pre-judgements and beliefs with implications for both the CCTV system but also for the scrutinised (Macnish 2012, p.152ff.; Norris & Armstrong 1999). Taking the example of a CCTV system at the airport brought forth by Macnish, there are multiple steps in which the operator can make *wrong* judgements resulting in either a false positive (an innocent individual being questioned and maybe detained) or in a false negative (a targeted individual remaining unnoticed):

> "Stage 1 – CCTV operators look for suspicious individuals; Stage 2 – CCTV operators take a sustained look at individuals from Stage 1; Stage 3 – ground-based agents take a sustained look individuals passing Stage 2; Stage 4 – ground-based agents remove individuals passing Stage 3 for interview; Stage 5 – the arrest or release of any individuals from Stage 4." (Macnish 2012, p. 155).

In each of these stages, the operator or the ground-based agent can make one or more decisions resulting in a false positive or negative. This highly influences the efficiency of the surveillance technology. Further development of the technology aims at eliminating possible – human – errors. This can for example result in automated surveillance, in which processors filter information and act based on them (ibid., p.157f.). But while the automated processing of information might eliminate human errors, there are still other limitations which cannot be excluded from the technology: mainly that the automated processing is only as powerful as the *code* which tells it what to do. Since that code also needs to be written by someone or by a team, the code equally bears the risk of including the code-writer's prejudices and political beliefs – which in this case affects everyone caught by the CCTV operating system as opposed to only those who are noticed by the CCTV operator in manual surveillance systems (ibid., p.158; see also Lyon 2002, p.23ff.). Codes are developed relying on earlier codes, on models designed and created by others, require research and thus all happen in a broad social environment, creating a certain risk of institutionalising the author's and others' prejudices and political and social beliefs into the code (Macnish 2012, p.158).

Similar examples can also be found in non-state-related contexts. Especially in consumer-oriented technology development with a strong data collection focus (e.g. Facebook or Google), networks of engineers help to inscribe profit-oriented/capitalist ideology into the algorithms of their search engines or feeds. But also other actors, like website providers, users, competitors, mass media, policy and legal frameworks, shape for example search-engine technology (Mager, 2012). Mager shows in her analysis of search-engine development, that while engineers contribute a large share of how search-engines are designed, other actors are also largely involved. Website providers, often relying on search engine optimisation (SEO) techniques and adapting their search algorithms, want to be listed as highly as possible in order to reach a maximum of users to increase their profit, and also users shape search-engines by wanting to obtain the required information as conveniently as possible without further dealing with the implications of search engine algorithms and data collection practices (ibid., p.8f.).

As I already noted in the previous chapter, and Mager also stated, there are not only different actors involved in shaping the design and development of a certain technology, but it is also the wider environment – in the case of search engines the competitive environment, mass-media, policy and legal frameworks. In the case of state surveillance technologies, they can be seen as "a distinctive product of the modern world" (Lyon 2003b, p.161). First as a result of a systematic personal information collection for bureaucratic purposes, later with a strong law-enforcement link for limiting or preventing criminal and terrorist activities (ibid., p.163). It is thus the environmental setting, the network in which the technology is developed which equally shapes its orientation and purpose.

However, it is important when considering the social construction of technology to not focus on the designer, programmer, manufacturer or coder alone. Technology is also shaped by the imaginations of the users, the cultural and knowledge traditions and historical development: "the rapid expansion of surveillance technologies (…) illustrates some central aspects of modernity and a putative shift toward more postmodern conditions" (ibid.). Particularly regarding security-related surveillance technology, this can initiate a vicious cycle – which is observable in the current stream of events: “the more information is gathered, the more security problems are identified leading to more information gathering” (Kreissl 2014a, p.661). The increased eagerness to counter insecurity with technology solutions gives insight into the cultural meaning of technologies – at least in western spheres presented as the ‘Holy Grail’, the easy answer for difficult solutions and as such trusted by government agencies (Lyon 2003b, p.169).

The process of inscribing into technology however doesn’t stop there. Technology incorporates the inscriptions and in further consequence shapes the society. Social norms, political beliefs, knowledge is extended and consolidated through technology, acquiring power and getting more and more difficult to negotiate: Technology “both embeds and is embedded in social practices, identities, norms, conventions, discourses, instruments and institutions – in short, in all the building blocks of what we term the social” (Jasanoff 2004, p.3). Gilles Deleuze (1992, p.6) described the social and technical interplay in the way that it is “not that machines are determining” the social, but rather that machines “express those social forms capable of generating them and using them.”

As technology creeps deeper into modern life every day, the embeddedness of technology in social practices, in identities and norms becomes ever more present. The contrast between the natural (the human) and the artificial (the technology) gets narrower, and also heavily influences human agency – some previously natural events become part of human decisions with the help of technology (Kreissl 2014a, p.664f.). Technology helping to interfere with previously natural decisions can be found at large: from prenatal genetic screening to life-extending measures (ibid.). Also the surge in popularity of health enhancing “wearables”, thus body-borne technology can be neatly included into this list and also provides an insight into how social norms incorporated into technology are further extended and consolidated.

Health-enhancing wearables can measure a range of body functions and health data, from temperature and steps walked over blood pressure and heart rate to calories burnt over a certain period of time or tracking your sleep. The body-borne technology is filled with sensors being able to collect the necessary data, sometimes in combination with extra information input by the data subject. As an example, a fitness tracker is introduced on a website for wearables as follows:

> “Jawbone's latest wearable, the UP3 is *packed full* of some of the *most advanced sensors* in the space, which means it takes measuring your calorie burn each day seriously. It's

> easy to guestimate the impact 30 minutes of walking will have on your calorie deficit, but the UP3 tries to take out the guesswork, using data about your *height, weight, activity intensity* and *duration* from its huge range of sensors." (Caddy, 2016; emphasis added).

Incorporated into the technological system – the whole which combines the sensors with the program and the wearing device – are thus specific norms which are regarded as the ideal in terms of calories intake, blood pressure, activity, etc. These are included into the device and due to the popularity of these devices they influence peoples' activity, diet, sleep and so forth. In the terms of the Actor-Network Theory, the device functions as an opaque black-box (Latour 1999, p.304) in which for the device wearer / data subject, the input of the designer, of the programmer, etc., is not visible anymore. It is only the successful output of the device which is of interest. Only when the desired output is not guaranteed anymore, if unwanted outcomes are linked to the device, the device enters a more prominent role, requiring a dismantling of the black-box (ibid., p.183ff.).

This means that the role of the technology as an actant – "something that acts or to which activity is granted by others" (Latour 1996, p.7) – often comes to surface if a problem accompanies the technology. Or more generally speaking, if the embeddedness of technology in social life, if the incorporation of previously embedded social norms, political decisions or prejudices have an influence on the output of the device. If we take the example of an ATM machine (see Introna & Wood 2004, p.179f.), there is a long list of attributes which the machine considers to be *the norm*: assuming that everyone in front of the machine is able to see and read the screen, enter a code, etc., things of course not everyone is capable of and thus is excluded by the system. This becomes even more problematic when – as is more and more the case – (small) bank branches are closed and ATM machines in combination with home-banking are the only remaining possibility of accessing your account. The politics and norms inscribed into the technology thus have the possibility to decide on who to include and who to exclude. The technology requires that the individual is machine-readable (Kreissl 2014a, p.664) by which the individual mutates into a "human/technical hybrid" (Brown 2006, p.227) or a "techno-social hybrid" (Kreissl & Ostermeier 2011, p.292), "a node in an assemblage comprising technologies and artefacts, constitutively dependent on abstract systems for survival", a fusion of "biological and technical components in an organism" (Kreissl 2014a, p.664).

In surveillance societies, also the technological components and artefacts of the "techno-social hybrid" can become a target of surveillance. Technological products or systems which are closely linked to persons, be it their smartphone, laptop, but also their loyalty card or in some more extreme cases implanted RFID-chip, are targeted by surveillance practices. What Roger Clarke (2012) coins Überveillance, the "surveillance of a feature of a person, or of an artefact that is very closely associated with a person included embedded within the person's body" can also be seen as the surveillance of non-human actants from an ANT perspective. Due to the agency specific actants have on specific human actors, surveillance practices are not only aimed at the human, but also at these non-human actants.

(Surveillance) Technology as Gatekeeper

(Surveillance-) Technology evolves into a gatekeeper in such situations as the inclusion or exclusion of the techno-social hybrid solely depends on the technology. This can be observed in the case of the ATM by which non-machine-readable individuals are not compatible with the technology and thus excluded. But this can also be observed when considering the disembodiment of data and the creation of data doubles (Haggerty & Ericson 2000, p.606). Only a certain frame of the techno-social hybrid is captured in the data double, but certain forms of control and intervention are nonetheless inscribed into it (Hempel et al. 2011, p.16). Especially surveillance technologies have certain functions relying almost exclusively on the existence of a data double. Access control systems decide based on specific input: who is the individual wanting to access a certain site, is information available and is he or she identifiable and ultimately allowed to access or not? A range of categorisations helps the dichotomous decision of 'access: yes/no'. How those categories are defined, who sets the criteria and limits is seldom visible for anyone[15] and these settings are done beforehand through coding the system (see the examples by Macnish 2012, p.157ff.). It is not whether one is a man or a woman, or whether one is tall or small which is the basis of obtaining access, but rather if they "possess a valid ticket – which is possibly coded on the basis of those criteria" (Hempel et al. 2011, p.16, own translation). There is no room left for negotiations as the codes constitute the possibilities.

This can create an ambivalent situation. On the one hand the criteria of the technology can be based on categorisations which are different from the social divisions we know – and it thus does not matter what gender, race, age, wealth or attire one has, everyone is considered equally (Lianos and Douglas 2000, p.266). If we take again the example of the ATM machine, as long as you hold the right ticket/card and know the PIN number you are treated equally, no matter if

[15] This is however also the case for manual surveillance operations. The scrutinised individual is entirely relying on the willingness of the surveillance operator, without knowing on what basis his actions are performed (see for example Norris and Armstrong 1999).

you are a rich blonde female or a poor black male. Compared to the same constellation and the same transaction at the bank counter, one can suppose that the first person is warmly welcomed and the latter is confronted with suspicion at least. On the other hand however, if the technology rejects access for whatever reason, the individual has to adapt to the parameters of the technology as the error is on the side of the user. A negotiation with the system is impossible (ibid., p.264f.)

It shows that technology is more than just socially constructed and thus performing surveillance on behalf of others, on behalf of those with power. It is rather technology which functions "as nodes, or links, in a dynamic socio-technical network, or collective, kept in place by a multiplicity of artefacts, agreements, alliances, conventions, translations, procedures, threats, and so forth: in short by relationships of power and discipline" (Introna & Wood 2004, p.179). Surveillance technologies like cameras and the included algorithms are the locations in these networks in which norms, values, interests, or prejudices are negotiated and incorporated and thus also made durable (ibid., p.180; Latour 1991, p.103). But those networks are difficult to locate exactly, as is a certain distinction between specifically social and specifically technical components, "cause from effect, designer from user, winners from losers" (Introna & Wood 2004, p.180). It is also difficult to dismantle the networks and their participating actors and actants. The silent – hidden/embedded, passive, flexible and obscure (ibid., 183) – surveillance technology further increases this non-transparency, and thus also amplifies the black-boxing of its norms, values and interests. The opening of the black-box is what is, empirically and analytically, attempted here.

Digression – Surveillance regimes as anticipatory regimes

> "Dans un environnement international marqué par de grandes incertitudes et des préavis qui peuvent être très courts, les moyens de la connaissance et de l'anticipation constituent la première ligne de défense d'un pays." (Mallet et al. 2008, p.133).

The quote above is taken from the *livre blanc – défense et sécurité nationale* from 2008, commissioned by the former French president Nicolas Sarkozy on the state defence and national security. Loosely translated, the quote entails that in international settings, which are marked by great insecurities and short announcements, the defence of a country must primarily rely on intelligence and anticipation. This quote serves as an example for the way surveillance technologies are often seen – a means to anticipate future events. This is also the reason for this short digression within the theoretical analysis of (surveillance) technologies, the transformation of the surveillance regime into an anticipatory regime.

The anticipatory character was already addressed by Foucault (2007) in reference to "the general features of the apparatus of security" and "the art of governing and treatment of the uncertain." Foucault refers to the mechanisms of security, characterised by the management onto the future, which is "not exactly controllable, not precisely measured or measurable" (Foucault 2007, p.35). This uncertain, uncontrollable and not measurable is what is essentially responsible for the insecurity in the past as well as in modern times – and thus creates a new desire for more control. In modern societies, the future is perceived more and more as an open space ready for intervention, ready to be colonised by the *'us'* from the present (Luhmann 1976; Adams & Groves 2007).

With the surge of the "risk society" (Beck 2015), security can be defined by a balance between trust and risk. Giddens (1990, p.34) hereby defines trust "as confidence in the reliability of a person or system, regarding a given set of outcomes or events", while risk is defined as a probability of an unwanted outcome of events (Giddens 1999). There appears to be a strong requirement for a relentless pursuing of certainty which not only translates into a wide range of ubiquitous surveillance technologies, but also technologies "that seek to pre-dress the near-future – to redouble past relationships so as to predict future inefficiencies" (Elmer 2012, p.27). Beck ascertains an emergence of risks in regard to technological and scientific advances – however which can again only be opposed with further technological development. Luhmann however goes even further, as the raise of the societal importance cannot be ascribed only to the technological advances, but are also a result of the reliance of societal decisions which are persistently projected into the future (Luhmann 1990, p. 140; 1991, p.3). Risk thus emerges where decisions have to be made which are time-bound or future projected, while it is impossible of knowing the future (ibid., p.21). The notion of safety is often used as opposed to risk, however as Luhmann nicely shows, safety is a social fiction or an empty concept which, in terms of the none-occurrence of potential drawbacks, does not exist (Luhmann 1990, p.134).

Instead, the dichotomy of risk and danger proves more useful to describe the modern risk society. Uncertainty of damage in terms of time-bound choices can lead to this distinction between risk and danger. *Risk* then is contributed to the situation, if a damage occurs as the result of a specific decision that has been taken and to which the damage can be related. As opposed to *danger*, when the damage is the result of an external cause (ibid., p.148ff.). As a short example, for a smoker, cancer is considered a risk – as it can be the result of his or her decision to smoke, despite knowing the potential damage of cancer. For every none-smoker, cancer is considered as a danger. However with technological advancement the consideration of what is risk and what is danger changes. The technological nature of modern societies results in a controllability of processes and in further instance an increased predictability of resources and the possibility to attribute specific errors to their origin (Luhmann 1991, p.97ff.). Occurring damages require in such instances explanations – explanations which formerly could be related to something supernaturally. The dichotomy of risk and danger in modern societies thus require a persistent ‘intervening' into the future, with science's methods for prediction, for anticipation (Adams et al. 2009) as the tools for circumventing and explaining possible damages.

The emergence of ubiquitous surveillance is seen as an immediate reaction of risks like ‘terrorist' attacks like September 11 (Lyon 2001), resulting in "politics of temporality" in which the future requires to be anticipated (Adams et al. 2009, p.246f.). The anticipatory character creates a state in which the future determines the present, as the future appears to be *ever-present*, but without knowing if it is going to happen or not. The anticipation of the future is also a contest about *‘who'* is to shape the future, who can set the social setting in which the future is embedded and who determines the conditions under which the future is able to persist (Brown et al. 2000). This also entails questions of shared belief-systems – norms, beliefs and ideologies – which are desired to be persistent also in the future. Or, to use the words of Jasanoff, defining *sociotechnical imaginaries* as "collectively held, institutionally stabilized, and publicly performed vision[s] of desirable futures, animated by shared understandings of forms of social life and social order attainable through and supportive of, advances in science and technology" (Jasanoff 2015, p.6).

This however doesn't prevent a future from still being uncertain (Luhmann 1990, p.134) – something which will still happen and thus always demand an answer (Adams et al. 2009, p.248f.). While anticipatory practices can be found in many different sites, e.g. as a result of the techno-scientific integration in biomedicine (Clarke 2003), the emergence of the 'war against terrorism' has increasingly contributed to a "pre-emptive resistance" (Cooper 2006, p.129) or a "regime of anticipation" (Adams et al. 2009, p.247) in order to counter "incalculable" threats, "uncertain in time and place" (Cooper 2006, p.124).

Anticipatory regimes can be best characterised by the five dimensions introduced by Adams et al. (2009, p.254ff.), which can also be found in surveillance technologies:

- Injunction, meaning that there is a sort of obligation, moral imperative of being knowledgeable about possible futures. Especially in relation to security, the injunctive character is on the one hand kind of charged by the society, in order to be *safe*, on the other hand is seen by the familiarity surveillance has obtained in society, being part of everyday life (Bauman et al. 2014, p.142).
- The injunction of having a knowledge about the future inevitably leads to an abduction of the present by the future – something that can for example be observed in modern crime fighting methods which rely more and more on predictive policing practices or on "the new penology" as a result of "new technologies to identify and classify risk" (Feely & Simon 1992, p.457), thus in which the present is used to predict or prevent something in the future.
- Closely tied to the abduction is also the preparation for future incidents, thus not only aiming at and preventing an event from happening but also being prepared for certain events to happen and responding to them (which is strongly tied to crisis management practices).
- Anticipation is also very much driven by a thrive for optimisation, in which the aim is to shape the best possible future. Here the question emerges however for whom the future is optimised. In Big Data practices, the anticipatory character related to optimisation can be easily identified, as Big Data aims at a manipulation of the behaviour of the consumer through the tools of analytical intervention. Like for example identifying

a product's *optimal* price – the price consumers are still willing to pay but makes the highest profit for the company and thus is optimal for the company (Esposti 2014, p.216).

- Finally, and also related to the optimisation of the future is the creation of new possibilities through anticipatory regimes. The fight against terrorism has opened new possibilities for the economy of security and surveillance technologies; with Big Data analytics it has become possible of tailoring individual marketing strategies to the needs of the individual.

The anticipatory regime of surveillance (technology) has initiated a paradox status of the present – "not yet executed, but unwanted behaviour can be anticipated and thus becomes real" (Hempel et al. 2008, p.15). Surveillance technologies are not employed anymore in order to understand past events "but also to predict and intervene *before* behaviours, events and processes are set in train" (Lyon 2014, p.4). Since the boundaries between the state surveillance and consumer surveillance have blurred, the anticipatory character of surveillance, the management of future behaviour becomes contested between different stakeholders and shaped by the views and ideologies of each stakeholder group with technological surveillance systems "set up (…) with specific kinds of interests in control and influence" (Lyon 2003b, p.177). Shaping policing from post-crime to pre-crime and customised promotion of products by online stores like Amazon follow the same logic (Hempel et al. 2008, p.15) although with different aims of control and influence. But in all those cases, the citizen, the consumer, the individual has no telling in who shapes what and how, and neither has the possibility of partaking shaping or contesting the way his or her future is being manipulated.

Recapitulating II

What I have tried to demonstrate here is a theoretical perspective on surveillance technology, which departs from the strict distinction between social and technical, between human and non-human. Also (surveillance) technology is not only characterised by being shaped by the social, being technical assemblages of the social. I rather consider technology as an opaque black-box, which is embedded in and equally embeds the social – and which thus requires a deconstruction. Looking at the different actors and actants involved as well as the networks in which they are included makes us able to identify what interests, what knowledge and what ideology is translated into the technology and in further consequence tries to anticipate and manipulate the future of techno-social hybrids. Understanding the black-box technology – the codes and algorithms included in it making decisions on the basis of interests programmed into it – helps also to better understand surveillance practices. And this also leads us to “the core point” which “is to understand the “modern Human” as a technologically mediated and supported form of existence” (Kreissl, 2014b, p.15), whose role in this surveillant and technological world needs to be analysed.

4.3. Locating Society

The two previous sub-chapters have shown how surveillance is practiced – from a governmental side as well as from a profit-orientated level of corporations, and how technology shapes and is shaped by surveillance, how it is embedded by the political and the social and how it embeds the social and the political. The role of the society and the individual however have so far been left out – except here and there picturing a society delivered to surveillance practices. This is why I want to conclude this theoretical chapter about the role of the society in surveillance practices, on the one hand being at the mercy of, on the other hand reacting to surveillance.

4.3.1. Society at the mercy of surveillance

With the implementation of CCTV surveillance in specific areas, the expected impact of surveillance operations is generally falling crime rates. However, with governmental as well as commercial surveillance practices, the impacts are never unidirectional as in the gaze of surveillance everybody is scrutinized. Especially with mass-surveillance (Clarke 2012) everybody passing through a specific area, visiting a certain website or using a loyalty card scheme is targeted. Individuals are constantly profiled and classified into different categories – consumer and profit related in terms of commercial analysis, risk and dangerousness related in terms of policing and intelligence (Lyon 2001, p.2).

The effects of the categorisations of individuals can have an important impact on how they can act socially, as surveillance operations often go – intentionally or unintentionally – hand in hand with practices of discrimination and exclusion. Digital networks and Big Data collections have created a state of ubiquitous surveillance from which it becomes increasingly difficult to escape (Andrejevic 2012, p.92) and which focuses on influencing and managing individuals and populations, even manipulating behaviour (Lyon 2003a, p.3; Esposti 2014, p.220). As already shown in Chapter 2 (p.10ff.), Norris and Armstrong have shown in their empirical study on CCTV operators, how practices of social sorting and ethnic profiling dominate manual surveillance practices. If for example teenagers, black people, or male individuals are more likely to be targeted by surveillance without any obvious reason but just because they *look* suspicious (Norris & Armstrong 1999a, p.164), the discriminatory effect of surveillance is striking.

Surveillance data, whether this relates to numerical data, statistics or CCTV images, only show a frame of the actual. This data is also only partially viewed by analysts and operators reducing even more the frame of which the data wants to make a full picture and on which decisions are based. Which means that the reading of surveillance data is also “a process of intuition and interpretation that may vary considerably from one analyst to another” (Baumann et al., 2014, p.125). However, these decisions, based on intuition and interpretation, create a *suspect* population (Norris & Armstrong 1999a, p.175), in which individuals become suspects in general simply by belonging to a specific age group, having a certain gender or a different ethnical background. In the terms of Ian Hacking it is a making-up of people, changing the space of possibilities for the classified (Hacking 1986, p.165). Even if nothing hints at individuals belonging to these categories being involved in criminal activities more often, they are still treated as suspects when caught on tape – whether they are innocent or not. Furthermore, as shown in the previous chapter, with this discriminatory aspect the prejudice of ‘young, black, male = suspicious’ can also be embedded into the codes of surveillance technologies (Macnish 2012, p.158). As this in turn also reinforces the stereotype and further embeds the acceptance of the suspect population into society, this also diffuses a generally negative message to the scrutinised suspect population about their own position in society, of which the majority *is* law-abiding (Norris & Armstrong 1999a, p.176).

The discriminatory character of surveillance can also be related to consumer and commercial surveillance practices oriented at increasing profit in specific sectors. For example, medical companies have specified their operation on predictive genetic information analysis, bearing the potential of leading to mistakes and abuse, but also to discrimination (Poudrier 2003, p.111f.). Genetic discrimination means that individuals or groups are disadvantaged based on their genetic data (ibid.) – resulting in higher health insurance costs based on a certain genetic predisposition. The wider effect is similar to the CCTV case presented above: Individuals with a genetic predisposition of obtaining cancer are classified into a *suspect* category – in this case suspected to be more risk-prone to obtain some sort of cancer. Having a data double included into such a category can already be sufficient to fall into a different insurance scheme with higher rates.

The discriminative character of surveillance practices can be reinforced even further when considering the assemblage of different surveillance technologies, with the desire to combine and integrate different systems in order to obtain a more holistic picture (Haggerty & Ericson 2000, p.610). This is where the effect of discrimination can quickly turn into a form of exclusion. Data doubles are categorised in different databases, remotely accessible and making decisions on behalf of the individual – whether or not one has access to specific credits, or credit conditions depend on the data double in the credit scoring database, whether one might enter a country like the United States depends on the data double in the different security databases of the US.

The exclusionary effect of (surveillance) technology can also be a result of the technological design and their social norms embedded into it. As the example by Introna and Wood (2004) has shown, the way ATMs are designed certain people are excluded if they are not machine readable (Kreissl & Ostermayer 2011, p.281). This is one of the dangers of the evolution of the techno-social hybrid – the techno-dependence creates new forms of exclusion.

4.3.2. Society reacting to surveillance

While society might be largely at the mercy of surveillance practices, there are different societal reactions which are observable, ranging from *accepting* the surveillance practices over *adapting to*/*avoiding* the practice to *resisting* surveillance.

With the Snowden revelations, solid evidence on the global reach of public-private-surveillance-partnerships was provided, which not only reached people interested in the topic, but due to its sheer impact also the general public. And although many citizens consider (governmental) surveillance as unacceptable (Bauman et al. 2014, p.141), often citizens have simply learned to live with surveillance practices (Kreissl 2014c, p.173), *accepting* the surveillance society (Lyon 2001). Bauman et al. (2014, p.142) have identified three factors why surveillance is still widely accepted amongst citizens:

- Familiarity – ubiquitous surveillance has become a part of everyday life, with surveillance technologies being embedded everywhere around us. “Many people no longer notice them and certainly do not think about their surveillance capacities” (ibid.).
- Fear – 9/11 has not only led to a rise in surveillance but also to a rise of fear, which is even utilised specifically by governments, media and others for enforcing their own agendas. The fear of crime and terrorism and the medialisation of such events have created a constant state of fear in societies which make surveillance technologies more acceptable.
- Fun – many surveillance practices derive from data gained from technologies and services citizens use for fun. Social media as well as streaming music and movies, or online games are only some spots where individuals function as leaking data containers.

One additional factor can be found in the large empirical study by Kreissl et al. (2014b; 2014c), which could even be seen as a constituting factor for the other three factors:

- Not understanding surveillance due to “the peculiar nature of modern surveillance assemblages operating in most cases at an invisible, infrastructural level of data processing. Very often there is no tangible interface for citizens (as a police officer would be the interface of public order) and hence in a number of cases we found a lack of understanding about surveillance effects, sometimes producing extreme interpretations at both ends of the spectrum: trivialising and demonising” (Kreissl 2014c, p.173).

Not exactly understanding the surveillance assemblage has many reasons, of which I have tried to show some and which basically constitute the research behind surveillance studies: The black-box of surveillance (technology). Bauman and Lyon (2013) have coined the term *liquid surveillance*, demonstrating the difficulty of “situating surveillance developments in the fluid and unsettling modernity of today”, which is “in a liquid phase (…) [a]lways on the move, but often lacking certainty and lasting bonds” (ibid.).

Although surveillance might not be entirely understandable for citizens, active reactions are observable in societies in order to cope with surveillance: *adapting*/*avoiding* and *resisting*. Marx (2009, p.297) considers both techniques as neutralisation moves of citizens as a response to surveillance, which have the goal of defeating the use of surveillance. He introduces 12 prominent neutralisation moves which are a response to different surveillance practices, compromising avoiding, adapting as well as resisting surveillance:

Move	Action
Discovering	Find out if surveillance is in operation, and if it is, where, by whom and how
Avoiding	Choose locations, time periods and means not subject to surveillance
Piggy backing	Accompany or be attached to a qualifying object
Switching	Transferring an authentic result to someone or -thing it does not apply to
Distorting	Altering input such that a technically valid result appears but the inference drawn from it is invalid
Blocking	Eliminating or making data inaccessible
Masking	Involves blocking so that original information is shielded but goes beyond it to involve deception with respect to factors such as identity and location
Breaking	Rendering the surveillance device inoperable
Refusing	“Just say no” – ignore the surveillance and what it is meant to deter

Explaining and contesting	Accounting for an unfavourable result by reframing it in an acceptable way or offering alternative data and the claims of rival experts, making rights claims
Cooperating	Collusive moves with agents
Counter-surveillance	Role reversal as subjects apply the tactics to agents taking advantage of the double-edged potential of tools

Table 1: Twelve Neutralisation Moves (quoted from Marx 2009, p.298).

While most of the neutralisation moves described by Marx are clear, some might require an explanation or a specific example. The move *piggy backing* means that in order to pass an access control point for example, a person slips through while another person legitimately obtains access. *Switching* can be done by submitting health-test results from someone else to the insurance company in order to obtain better conditions (Marx 2003).

Counter-surveillance techniques, also called counterveillance or sousveillance, is “where the activity is undertaken by or on behalf of the less powerful, commonly an individual or a group, and the purpose is as a countermeasure against behaviours of powerful organisations or individuals (‘sous’ [French] = ‘beneath’)” (Clarke 2012). The term sousveillance was coined by Steve Mann and from a technological point of view it can be exemplified as participants in a certain activity, e.g. partaking in a demonstration, having hand-held cameras or wearable cameras in order to monitor the activities of the police (Mann 2013, p.6). Especially with the emergence of new wearables, like the Google Glass, sousveillance techniques might become more prominent – however also bearing the risk of increased surveillance practices, as the device can also be equally implemented for surveilling. Counter-veillance techniques or neutralisation moves in general seldom remain unnoticed, often triggering “counter-neutralisation” techniques, like for example technologically enhanced surveillance methods, which have a higher performance of processing data, or a better algorithm analysing data, or a better X-Ray in order to also find *masked* products (Marx 2009, p. 299ff.).

Recapitulating III

Society is thus not only at the mercy of the surveillance practices around them, but also reacts to them. This means that individuals on the one hand have their behaviour shaped by the surveillance practice and technology – avoiding certain places, masking certain information – but on the other hand also shaped by their behaviour against the surveillance technology which is enhanced in order to perform better, to be more user-friendly for the operator, etc.

The dangers of surveillance technologies of which I have only shown two – discrimination and exclusion – can be manifold. Also other surveillance practices and technologies which appear harmless now can of course become dangerous when falling into the wrong hands – a fascist regime gaining control over the amount of data the NSA has stored about their own citizens can have severe consequences for marginalised populations and regime critics. But it is also important to note "that just because something negative could happen, does not mean that it must happen" (Marx 2009, p.295). While one can condemn all surveillance practices equally, trying to uncover the many facets and networks involved in the different practices appears more promising in understanding surveillance – at least for me.

5. Methods

*This chapter will give an overview of the methods used for the data collection and data analysis of the empirical research of this thesis. Choosing expert interviews as the method of data collection entails some (methodological) questions which need to be addressed here: the first (**5.1**) question which arises in regard to the expert interviews is: what exactly makes the expert an expert? In the second (**5.2**) part I will discuss the expert interview, the considerations I made in order to prepare for the empirical part of the research, the construction of the guidelines and questions for the interviews, but also how the expert interviews can differ practically from other forms of interviews. Finally (**5.3**), I will briefly give insight into why the qualitative content analysis is best suited for the analysis of the collected data.*

*****

The toolbox of methods from which we can select the method of choice is big, thus finding what one needs can be a challenging task. The choice of the method should always be guided by the research question(s) and how they are best to be answered (Diekmann 2012, p.19f.). As was already shown in Chapter 3, the "methodological monotheism" (Bourdieu 1992, p.224) which is closely tied to the strict division between theory and methodology (ibid., p.223) is often predominant in the Social Sciences, but should in my opinion be regarded as an outdated paradigm for analysing the social. The paradigm of pragmatism is better suited, as it foregrounds the research problem and not so much the method (or school of thought). Thus applying to my thesis here, it is my research question which forms the basis:

> "How are data collection and data protection practices managed and negotiated within organisations, facing an entanglement of these practices with legal, technological and societal implications?"

Before concretising on the method, there are some other considerations which also guide the choice of how to answer the research question: the practical – what kind of resources (time, funding, etc.) are available to the researchers, is the research done by one researcher alone or in a team, but also considerations regarding the access to the field of study shouldn't be neglected. Taking these aspects together, in this case the research involves two steps. The first step consists of a legal analysis of the existing data protection laws in Europe and Austria, as the further research depends on the understanding of the legal requirements and the exceptions.

On the one hand, this implies the actual legal documents (the Directive and the Austrian implementations), on the other hand, the consideration of the corresponding legal regulation is equally necessary. The second step consists of a reconstructive approach aiming at the sites where personal data is collected. Qualitative expert interviews will be conducted with people responsible for or involved in data collections in organisations as well as the data protection aspects of these collections. Although they might not always be the actual 'surveillance workers', in the sense of the daily operation with personal data, they should have great insight into the daily operations. The interviews will be semi-structured and around 10-15 interviews are targeted. Here the biggest difficulties might occur as this number depends on the responses and the commitment of the interviewees to the interview and the willingness of participating. In order to obtain a clear picture of the practices of the 'surveillance workers', the research sites will be composed of public and private, national and international organisations.

Also the methodological principles of *openness*, *theory*- and *rule-guided investigation* as well as the principle of *'Verstehen' as the basic action of social science research* are carefully taken into account in this research. While the first three principles are general principles of research, the principle of *'Verstehen'* is particularly important here due to the focus of the research being also on the reconstruction of knowledge-production and the consequences of a specific kind of knowledge on the interaction with "lay people" as well as on the interaction with technology (Gläser & Laudel 2009, p.29-33).

5.1. Constructing the expert

Expert interviews are one of the most-used interview-techniques within the social sciences (Bogner & Menz 2009, p.8; Meuser & Nagel 2009, p.35f.; Kaiser 2014, p.V) and they are often treated as a quick way to gain information and knowledge on specific subjects without the necessity of going through masses of secondary literature – thus used from a perspective of research-economisation (Bogner & Menz 2009, p.8-19; Pfadenhauer 2009, p.113). This is also why expert interviews are often used in industrial-sociological, organisational-sociological, educational and political researches (Meuser & Nagel 2009, p.35).

It is necessary to approach the method of expert interviews in a reflexive manner and to locate it methodologically as well as theoretically, as the performance of expert interviews indeed needs a lot of prerequisites and is "thus also a distinctly elaborate instrument for generating data" (Pfadenhauer 2009, p.113). However, despite the frequent usage of expert interviews in social sciences and the importance of a reflexive approach to the method, there are only a few methodological 'text-books' on expert interviews, many of which have their origin in the German-speaking countries of social science research. The reflexive approach to the methodology of expert interviews is largely influenced by the sociology of knowledge by Schütz, or Berger and Luckmann.

Using expert interviews for my research thesis is not done with a research-economisation in mind, but instead as the best way of getting access to the knowledge and experience of 'surveillance workers' in regard to data collection and data protection in organisations. This thus leads us to the question of what makes an expert an expert? There are two approaches which can be used to define an expert relevant for the expert interviews:

- We can see an expert as someone who has a special *expert knowledge* which relates to a professional field, an occupation and where this knowledge is transformed into actions and practices (Littig 2013). The expert has access to some kind of professional knowledge, a knowledge not solely available to him but also not to everyone in his field. He thus has an advance in knowledge and it is this advance in knowledge which the expert interview wants to research (Meuser & Nagel 2009, p.37f.).
- But we can also see the expert as a source of specific knowledge which is deemed important for certain social actions and which we want to discover: "*Expert describes the specific role of the interview partner as a source of special-knowledge on the social*

circumstances which are researched. The Expert-interview is a method for making this knowledge accessible" (Gläser & Laudel 2009, p.12, own translation, italic in original). In this sense, everyone with a specific knowledge relevant for the research in question can be an expert for the interviews (ibid., p.43).

The two approaches are closely related and mainly differ regarding the relevance of the knowledge. In the first approach, the expert knowledge is a professional knowledge and thus always related to a profession. In this case there is also a differentiation made between specialised knowledge and expert knowledge – the latter is seen as a socially institutionalised expertise (Meuser & Nagel 2009, p.38). The second approach has a broader understanding of the expert and relates the knowledge to specified social situations and circumstances for which this knowledge is relevant. What should be kept in mind is that from a constructivist perspective, the role of the expert is always attributed to the expert, either by us – the researchers, but also by the society or the organisation: "experts are made by society" (Littig 2013).

It then remains to decide on what is the relevant knowledge of the expert and thus also to decide which expert is relevant for the research (Bogner & Menz 2009, p.10). For my research, the relevance lies on the *expert knowledge* of the 'surveillance workers' – the kind of knowledge they have (almost) exclusively access to. And while his or her profession plays a crucial role in why the expert is relevant for my research, it is not solely the professional knowledge, but also the wider social and technical implications of his or her professional knowledge to which the method aims to get access to.

Another question which arises with the determination of the expert and expert knowledge is the question of the explicitness of the knowledge. Not every part of the expert knowledge is coined by an explicit awareness of the expert about his or her status: "The behaviour of the expert is also shaped by relevancies which are not, or only partly available in a reflexive way. Not only common knowledge, but also expert knowledge entails pre-theoretical practical knowledge and experience" (Meuser & Nagel 2009, p.50). This also leads to three dimensions of expert knowledge, being the technical knowledge (thus the expertise of a specific profession), the process knowledge or the practical expertise, and the interpretative knowledge which relates to the subjective perspectives of the expert (Bogner & Menz 2009a, p.70f.). The interview thus aims at a reconstruction of the technical and practical knowledge, but also of the subjective dimensions the experts include in their knowledge (ibid., p.66).

Finally, the production of knowledge of the experts can give important insight into the functioning of the practices in organisations. Especially the socio-cultural conditions in which the expert knowledge is produced and also transmitted to other relevant actors within the organisation. The perception of my analysis in regard to the expert interviews should thus also focus on the cultural circumstances, the communities and networks, the arenas and institutions, in which the experts sojourn and which in further consequence also influence the way knowledge is produced, managed and transferred (Meuser & Nagel 2009, p.45ff.; Knorr-Cetina 1999, p.5ff.).

5.2. Expert Interviews as a method

As I have shown, the expert interview is mainly defined through the subject of research, in this case the 'surveillance workers', as the experts have access to specified knowledge which is important for their profession and for certain social actions. The method of the interview itself is not so different than with other forms of qualitative interviews, but still requires some delimitation. Especially in comparison with narrative or ethnographic/open interviews, the expert interview is probably the most structured form of collecting interview data as the method nonetheless aims at gaining insight into information processes (Kaiser 2014, p.2). Mostly, expert interviews are interviews which are supported by a guideline of questions in order to ensure that all the (presumed) relevant aspects are covered during the interview, but still – in comparison with standardised/quantitative interviews – being open enough to leave space for deviation (in terms of sequence of the questions), interpretation and (counter-) questions by the expert and for further ad-hoc questions by the interviewer (Gläser & Laudel 2009, p.42f.; p.111f.).

The first step of the interview is the selection of the interview partners, as this influences the subsequent steps. There are several thoughts which one should make upon selecting the interview partners. The foremost question to ask is who is equipped with the relevant information and knowledge – which closely relates to the question of who is to be considered an expert. But the selection of the expert should not stop here but also reflect on who is able to give precise information on the subject. Taking the case of my research – within the resources available to me, I am limited to conducting only interviews and cannot rely on further research methods in gaining additional insights. And also here the number of interviews must be considered, as it does not make sense to conduct interviews which will not be analysed later on (ibid., p.118).

While for a broader research, interviews with 'surveillance workers' who are on a lower level of employment can be interesting as a source of additional information, for this purpose experts in higher positions seem to be more suitable, as they can probably provide a wider picture of the required information. One should also consider who is ready to provide information on the topic – especially since in my case it may be possible that not everyone is willing to share insider information of data collection and data protection practices in public and private businesses which stand in a light of surveillance. And finally the interview partner should also be available time-wise for an interview. As I conduct my interviews mainly between May 2016 and July 2016 and aim at gaining partners which are at a higher position within the organisation, this can also be a problem which should not be neglected (ibid., p.117f.).

After the selection of the interview partners, the next step is to develop the guideline questions, which is the primary operationalisation step of the research question(s) into the (hopefully) right questions one can bring forth to the interview partners (Kaiser 2014, p.4). This is why the design of the guideline should be treated as one of the key tasks during the preparation for the expert interviews without being hastily ticked off (Gläser & Laudel 2009, p.113; p.142). The design of the interview guideline and the questions see also some important considerations in my research. The initial thoughts turn around how the research question is to be combined with a focus on the knowledge of the 'surveillance workers', its production and transfer. The research question has different aspects which need to be deconstructed in order to be suitably asked to the interviewees.[16]

There are also some general thoughts which need to be considered upon constructing the guideline for the interview (ibid., p.144ff.). As interview situations are different from normal situations of communication, careful attention needs to be put on the opening questions. The first question should be seen as the first step of establishing a basis of communication between the interviewer and the interviewee. It is thus wise to start with a more open introductory question which can also lead to a phase where the expert is estimated to talk for several minutes. As the main part of my research question concerns the work of the expert in relation to data collection and data protection practices, it seems fit to start with the initial question here. First by focusing on the general work in the organisation and second as a 'surveillance worker' related to data collection and data protection:

[16] I will provide some insight into the construction process of the guideline questions, including information on each of the topics and why I think they are apt to lead to the information necessary for addressing the research questions. I will however not list all the questions here. The final guideline with all the questions can be found in the appendix p.122f.

> Opening question
>
> Could you start by generally describing your position in the organisation and your daily occupations, especially in relation to the collection as well as the protection of personal data?

This question can also be divided into two parts as it is in many situations better to ask short and simple instead of long and convoluted questions. In one way or another, it is expected that this question leads on the one hand to a first initial understanding of what the expert does within the organisation and how this is related to 'the surveillance workers'. On the other hand, this should also enable the possibility of subsequently asking topic-related questions. Questions aiming at similar information can be consolidated into topics which can be addressed one after another. Like this each subject can be processed as a whole, keeping related questions together while remaining flexible enough to switch the order of the topics depending on the course of the interview.

The subsequent topics each try to address different aspects of the research questions and the way the 'surveillance worker' as expert shapes the processes on the basis of his or her expert knowledge. As such, one subject addresses the **knowledge production** – in regard to the specific field of occupation, data collection and data protection practices, but also how **knowledge management** is handled within the organisation: training for new employees, advanced training for existing employees. Questions regarding the **socio-cultural** background of the knowledge production are also included here – relating to the educational speciality/subject, previous relating occupations, relevant networks etc.

Connected to this, but more specifically addressing **data protection** within the organisation are questions on the **significance** of data protection within the organisation, amongst colleagues but also on the management level. The topic of data protection should address the knowledge production of the **legal regulations** also in relation to the new General Data Protection Regulation and the expected implications this has or could have on the practices within the organisation.

This relates to the subject of potential **conflicts, dilemma, and crisis** the experts might encounter or have encountered in relation to personal data collections. Here the emphasis lies on the **crisis management**: prevention, preparation and mitigation of such events, but also on (minor) conflicts which might occur – conflicts between expectations and actual possibilities regarding data collection practices.

Further considering the different aspects of the research questions, another topic covers the interplay of the legal regulation and the **technological capabilities and/or restrictions**. Thus considering if and how the legal provisions are still able to guarantee data protection bearing in mind the technological possibilities of data collection and processing, and addressing questions of how the law can be adapted. This also necessitates questions on the **potential**, but also on the possible **problems** the experts see in the technological development in relation to data collection and data protection.

Finally, the topic of the connection of data collections/protection and the **societal implications** will also be addressed. This involves questions of **immediate contact** with data subjects/persons, how this is handled within the organisation and how the expert is involved – especially related to the **right of access to personal data**. Here also questions of 'lay-knowledge' are to be addressed, considering if and how lay people are aware of their rights and how 'lay-knowledge' effects data protection. It could be worth keeping this topic as a last topic to cover, as it provides the possibility of leading to **concluding questions of data protection and society**, in terms of how society is generally informed on data collection practices and the dangers as well as their rights.

After the finalisation of the guideline, it should be tested in a test interview. I conducted an interview with a friend of mine who is also partly responsible for data collection and protection practices in his organisation, so he also has – at least partly – expertise in relation to the topics of the guideline. This enables a first adaption of the guideline as a reaction to the answers obtained through the test interview. The guideline however can also be adapted during the inquiry phase, for example if during the first interviews information arise which one hadn't considered yet. Questions aiming at this can be added for the subsequent interviews (Gläser & Laudel 2009, p.151f.)

Finally, some practical considerations regarding the conducting of expert interviews need to be highlighted. Ideally, these interviews are conducted face to face, as it allows a more direct interaction and also includes gestures and facial expressions which can be interpreted by the interviewer. However, if the interview partner insists or the physical distance between the interviewer and the expert is too far, then interviews via phone or web-meeting software (like Skype) are also possible (ibid., p. 153f.). The transmission of the questions prior the interview should be avoided, but in this context, if the interview partner insists, it is also better to agree than having no interview at all. More important however is the recording of the interview on tape. This is of course only possible upon consent of the interview partner. Particularly with interviews containing sensitive information, obtaining the agreement might not always be straightforward. In the case of my interviews, absolute anonymity is guaranteed, person-wise but also in relation to the respective organisations. The importance of the recording lies in the fact that it captures a lot more information than if the interviewer took notes and wrote a protocol after having conducted the interview based on the notes. Having a recording makes sure that an important principle of social science methodology is guaranteed: the replicability and comparability of social situations (ibid., p.157f.).

In regard to conducting the interview, general standards of practice, which apply to all interview situations, should be considered. The status of the interview partner as an expert however can create a different situation in comparison with classic interview situations. It is important to show respect to the interview partner and also demonstrate that one is specifically interested in his or her expert knowledge. It is however also important to show one's own expertise in order to establish a balanced atmosphere and a situation in which both are aware of the specific expertise and interest of the other, without trying to create a situation of intimidation based on the expert knowledge (ibid., p.172). If these considerations are followed during the interview, then even the situations which are not anticipated can be mastered. Finally, "[p]erhaps the single most important rule is – to quote from *The Hitchhiker's Guide to the Galaxy* – 'DON'T PANIC!'" (King 1994, p.24, quoted in Gläser & Laudel 2009, p.184)

5.3. The qualitative content analysis

The systematic analysis of the interview data is a further important step to guarantee the transparency of how the empiric data leads to the results. The approach I have chosen here is the qualitative content analysis, a method which is often used for the analysis of qualitative interviews as it is well-suited to extract descriptions of social matters from text, especially in reconstructive research approaches (Gläser & Laudel 2009, p.47). Although originally used for the analysis of quantitative data, it was adapted for the analysis of qualitative data by Phillip Mayring (2007) by comparing the theoretically established categories of the content analysis to the empirical material.

While Mayring has established a pioneering work with his adaption of the quantitative content analysis to qualitative data, I will however follow the qualitative content analysis used by Gläser & Laudel (2009). The main difference between the two is how the categories are used for the analysis. While Mayring uses a closed categorical system for the analysis of the text, Gläser & Laudel constantly adapt their categorical system to the text, which allows an adjustment in case new information emerges (Gläser & Laudel 2009, p. 198-201).

The qualitative content analysis uses the textual basis – in this case the transcripts of the interviews – as the material containing the data of analysis. So the first step is to extract the data from the text: Scanning the text and applying a search grid with the categories, and by doing so deciding which of the information is important for the analysis and which is not. By use of this approach, the amount of text is already quickly reduced and structured according to the needs of the research questions (ibid., p.200). The extraction and categorisation of the information is the most important step of the analysis as the main rendition of the material is done in this phase. For the extraction and classification of the data, different programs can be used, which are specifically designed for the qualitative content analysis (for example MAXQDA or Atlas TI).

Following the extraction of the information, the material is sorted: the information is condensed in order to reduce redundancies, and possible contradictions are verified. The result should be a structured base of information containing the main empirical information. In a last step the evaluation of this information is done, in which cases can be grouped and coherences are analysed (ibid., p.202; Meuser & Nagel 2009, p.56-57). In this last step the final interpretation of the material is done and ultimately the initial research questions are tried to be answered. But before we continue with the empirical results of the interviews, I will first have to digress and include a broad analysis of the legal framework in relation to data protection in Europe and Austria.

6. Legal Framework

Data protection in Europe and Austria

In this chapter the legal framework of data protection in Europe and Austria will be outlined – with a historical approach establishing an overview of the current Data Protection Directive and other regulations (7.1) and the future Data Protection Directive and Regulation (7.2) at the European level, as well as the translation of the European law in the Austrian Data Protection Act including its particularities (7.3). This not only enables the reader to better understand the data protection principles in regard to the technical understanding of the empirical data, but was also a necessary focal point of research in preparation for the expert interviews with the surveillance workers, data protection officers and others involved in the collection and protection of personal data.

*****

6.1. The European Data Protection Regulations – from a juridical innovation to an outdated tool

With the emergence of computers and automated data processing, considerations about data protection emerged in the USA and Europe in the 1960s. While the advantages of the automated data processing due to the gain in efficiency prevailed at first, it was only in the late sixties that the possible dangers for citizens and society were discussed. Concrete legal implementations didn't emerge until a decade later (Riccardi 1983, p.246). Data protection laws at first appeared on a regional and then on a national basis. The German Federal State of Hessen adopted the first data protection act ever with the *Hessische Datenschutzgesetz*, the Data protection act of Hessen (Hessisches Datenschutzgesetz vom 7. Oktober 1970), also coining the term *Datenschutz* for the first time which was later adopted in English with the term 'data protection' (Fuster 2014, p.56). In 1974 the Federal State of Rhein-Pfalz also adopted its first data protection act. On a national level, Sweden was the first country to adopt a data protection act in 1973, followed by the German Federal Data Protection Act of 1977 (Bundesdatenschutzgesetz, BDSG) and the French Law on Computers, Files and Freedoms of 1978 (Fuster 2014; Galetta & de Hert 2014; Riccardi 1983).

Data protection regulations on an international level have not appeared until the beginning of the eighties, starting with the Organisation for Economic Cooperation and Development

(OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980 (OECD 1980, updated in 2013), which was however not legally binding for the OECD member states. In 1981, the Council of Europe established the Convention 108 for the protection of individuals with regard to automatic processing of personal data (Council of Europe 1981) being "the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the transfrontier flow of personal data" (Council of Europe 2016). The European Data Protection Directive of 1995 (Directive 95/46/EC) – currently the main legislation in Europe regulating the processing of personal data – has adopted many of the legal provisions which were introduced by the OECD Guidelines and the Convention 108 (Galetta & de Hert 2014, p.3). The Directive established in 1995 applies to all EU member states, as well as to the European Economic Area (EEA) which includes Iceland, Norway and Liechtenstein, and emphasises the free movement of personal data while trying to create some forms of individual data protection (ibid, p.1).

This can already be observed when looking at the Objective of the Directive (Art. 1), where the Member States should not only "protect the fundamental rights and freedoms of natural persons (…) their right to privacy with respect to the processing of personal data", but also make sure to "neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection" (Directive 95/46/EC, Art. 1). Still, the Directive has set important principles, ranging from data quality[17] (Art. 6) which addresses a fair and lawful processing of personal data, collected for specified and explicit purposes, as well as setting out the criteria making data processing legitimate (Art. 7) – e.g. when the data subject gives his consent, but also if necessary for the performance of a contract to which the data subject is party.

Another example in which the Directive attempts the balancing act between data protection and the free movement of data is within the processing of special categories of data – thus "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" (Art. 8 § 1). While these special categories of data are generally prohibited from processing, this does not apply when "the data subject gives his or her consent (…)"; "processing is necessary (…) in the field of employment law (…)"; "processing is carried out in the course of its legitimate activities

[17] The principles regarding the quality of data can already be found in the Convention 108 of the Council of Europe and have been implemented almost in the exact same wording in the Directive 95/46/EC.

(…) by a foundation (…) with a political, philosophical, religious or trade-union aim (…)"; or if "the processing relates to data which are manifestly made public by the data subject (…)" (Art. 8 § 2). Furthermore, Member States can set further exemptions "for reasons of substantial public interest" (Art. 8 § 4), which is a term that is vague enough that it can be interpreted in various ways by the different Member States.

More relating to the research in question here are the provisions specifically relating to the data subject, as these should also require prior action, as well as trigger a reaction from the data controller of the organisation processing personal data. Here the Sections IV to VII are the main provisions, essentially providing the main tools for data subjects to access and thus control their data.[18] These Sections consist of important steps that should in theory guarantee that a data subject not only knows what kind of personal data is processed by whom but also the possibility to obtain information on the ongoing collection and processing of data – including the rectification and erasure of the personal data as well as the objection to the processing of data relating to him or her.

From a data controller point of view, this means that he or she must provide to the data subject first of all information on the identity of the controller, the purposes of the processing, the recipients or categories of recipients of the personal data and also inform the data subject about his or her right to access to data and the right to rectify the personal data (Art. 10 & Art. 11). This information is necessary so that the data subject can obtain not only "confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed" by the data controller, but also "communication (…) in an intelligible form of the data undergoing processing and of any available information as to their source" (Art. 12). If upon the right to access to data, the data subject notifies incomplete or inaccurate data or a processing of personal data not complying with the provisions of the Data Protection Directive, the data controller should as well provide the right of rectification, erasure or blocking of data.

It is mainly upon these points, where data subjects are given the possibilities to actively perform the protection of their personal data which is why Galetta and de Hert correctly mention that access to personal data "constitutes the first but irrevocable step towards the full protection of

[18] The rights of access to personal data were, similarly to the quality of data, already included in the OECD guidelines and the Convention 108, and are thus not entirely new legal tools to guarantee a data subject specific rights regarding their personal data.

personal data", however the data controller is also in the obligation "to notify [the] data subject about the processing of their personal data" (Galetta & de Hert 2014, p.7), in order to guarantee the right to access.

The Data Protection Directive however provides a set of exemptions and restrictions for member states which also apply to the Article 12 – the right of access to data – and mainly concern measures to safeguard:

(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic of financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others. (Art. 13 § 1).

Although some of these restrictions are necessary and also logical in the terms of the objective of the Directive to also guarantee the free movement of personal data between the member states, the terms used can be interpreted in different ways by the member states implementing the Directive and thus also leave relatively vague provisions for the interpretation of each and every data controller when it comes to the information given to the data subject as well as to the right of access to data.

Finally addressing further tasks of the data controller and, in order to be complete, the Directive also sets provisions concerning the Confidentiality (Art. 16) and the Security (Art. 17) of the processing, and also the obligation of the data controller to notify the supervisory authority – being the data protection authorities (DPAs) in each Member State – of any wholly or partly automatic data processing operation (Directive 95/46/EC, Section IX). Especially the notification of the data processing can in theory simplify the right to access to personal data for the data subject, as the notifications of the processing operations have to be published in a registry by the DPA which may be inspected by any person and should at least contain the name and the address of the data controller, the purpose(s) of the data processing as well as a description of the category or categories of the data subject – thus already some of the information stipulated in the Art. 10 and necessary in order to being able to contact the data controller for the access to data.

Beside of the Data Protection Directive, also the European Convention on Human Rights (ECHR) guarantees the right to respect for private and family life (Art. 8). Adopted in the Charter of Fundamental Rights of the European Union in the year 2000, the Charter also includes the Protection of personal data (Art. 8) which even specifically mentions that "[e]veryone has the right of access to data which has been collected concerning him or her, and the right to have it rectified" (Charter of Fundamental Rights of the European Union 2000: Article 8). Finally, data protection was also included in the 2007 Treaty on the Functioning of the European Union (TFEU) in Art. 16, which guarantees that everyone has the right to the protection of personal data concerning them, however specifically mentioning individuals instead of the term 'data subjects' used in the directive. But this also means that for more than 20 years – or 15 years in the case of the Charter of Fundamental Rights – there has been no further development in terms of data protection provisions on a European level, except for a range of case law on a European and Member State level interpreting the different, sometimes vague provisions.[19] And all of this despite the rapid development of automated processing of data on the one hand, including a surge of different and globally acting internet services collecting and processing personal data and on the other hand more and more requirements of law enforcement, national security and intelligence agencies regarding access to all different kinds of processed data – often without having the legitimacy to do so.

Thus, before proceeding to the translation of the Data Protection Directive 1995 into the Austrian Data Protection Act 2000, we will have a look at the new developments on the European level, triggered in 2012 by the European Commission to update the old Directive and proposing a new Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data and a new Directive on the protection of individuals with regard to the processing of personal data for the purposes of prevention, investigation,

[19] This is not to say that the European Case Law in regard to the interpretation of the data protection provisions is not important. Many of the cases have seen important interpretation of the 1995 Directive: The case of Max Schrems which resulted in the Court of Justice of the European Union (CJEU) declaring the Safe Harbour agreement governing the data transfer between the EU and the United states invalid (Maximilian Schrems v Data Protection Commissioner, C362/14); the case of the CJEU paving the way for the so-called *right to be forgotten*, ruling that internet search engines upon request by individuals have to remove links from their search containing the name of the individual if these links are inadequate or not relevant anymore (Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C131/12). Another important case from a data protection point of view was the judgement of the CJEU declaring the highly criticised Data Retention Directive invalid (Digital Rights Ireland and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others, Judgement in Joined Cases C-293/12 and C-594/12).

detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

6.2. The General European Data Protection Regulation and Data Protection Directive – was it worth the wait?

With more than 20 years passed since the Directive 95/46/EC containing provisions adapted from the 1970s, it was only a matter of time before a new legal data protection tool would be introduced on a European level. Starting in 2009 with a public consultation to review the data protection legal framework (European Commission 2009), the Commission issued a first Commission Communication on their approach (European Commission 2010) in 2010, upon which all the relevant participants of the process responded with their views on the communication as well as on their amendments for the Directive 95/46/EC – namely the Council conclusion on the communication (Council of the European Union 2011), the European Parliament Working Paper (European Parliament 2011), the European Data Protection Supervisor (EDPS) Opinion (European Data Protection Supervisor 2011) and the Art. 29 Working Party Letter (Art. 29 Working Party 2011). The first draft, respecting the issued views of the participants, was released by the Commission in 2012 proposing a new General Data Protection Regulation concerning the protection of individuals with regard to the processing of personal data and also a new Directive specifically for the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (European Commission 2012).

Having to pass the different steps of the legislative process in the EU, it would take a few more years before the final Regulation and Directive could be published. The first to publish its views on the drafts of the Commission was the European Parliament in 2013, which had assigned its Committee on Civil Liberties, Justice and Home Affairs (also known as the LIBE Committee) on assessing the drafts (European Parliament 2013). The Council took even more time to propose its rectifications on the drafts of the Commission. The Working Party on Information Exchange and Data Protection was assigned with the task of the Council, which released its views on the draft Regulation and Directive only in June 2015 (Council of the European Union 2015), having already had also time to consider the amendments of the LIBE Committee. The trilogue – a joint discussion between the Parliament, the Commission and the Council – finally started on the 24th June 2015 and lasted until the 15th December 2015 (European People's Party group 2015; European Commission 2015a) to reach consensus on the final Regulation and Directive, which was adopted on 27th April 2016 and will enter into force on 25th May 2018 (General Data Protection Regulation, Art. 99).

The question that one has to ask is if it was worth the six years of work from the first public consultation in 2009 to the final documents in 2015, also keeping in mind that the first draft of the Regulation and the Directive was published in 2012 and will not enter into force until 2018. In those almost ten years in total, technological development and technology usage has changed drastically – smart phones and tablets have resulted in a broader processing of personal data (including an even wider range of location data) and with digitalisation and the internet-of-things (IoT) even more technology products have started processing personal data, all of which result in 'big data' collections (de Hert & Papakonstantinou 2016, p.180). Focusing mainly on the General Data Protection Regulation[20] (GDPR), the main changes in regard to the old Directive and the influences of the new Regulation on the data subject and on the data controller will be analysed here.

One of the main changes in regard to the old Directive is most obviously the choice of the legal instrument for the new data protection provision: a Regulation. By opting for a Regulation, the Commission has eliminated the problem of harmonisation which had resulted from the old Directive. As the personal data in question is seldom locally collected and processed, but rather at any point or another processed globally, having at least the same legal framework for the European Union and EEA is a big improvement also for guaranteeing the same rights to all data subjects. Although there is some room left for interpretation on national levels – e.g. in regards to the age of consent for persons under 16 years (General Data Protection Regulation, Art. 8 §1; Ryz & Grest 2016, p.18f.), the Commission signals through this choice that "data protection is no longer perceived as a local phenomenon" but "is considered from now on an EU concern" (de Hert & Papakonstantinou 2016, p.182).

Content-wise, the GDPR starts as the old Directive with the duality of on the one hand promoting the protection of personal data while maintaining the free movement of such data (Art. 1). This is insofar no surprise as the freedom of movement is a cornerstone of the European Single Market which not only includes goods, workers and capital, but has also been expanded to a 'Digital Single Market for business and consumers' (European Commission 2016a). However,

[20] Although the Data Protection Directive concerning the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, the free movement of such data also sets important legal provisions which are worth analysing, however for the research in question the data processing of law enforcement agencies and other similar agencies is not primarily, which is why the focus of the analysis will be on the General Data Protection Regulation.

and also as a result of the recent case law of the CJEU, the GDPR has greatly extended the territorial scope (Art. 3) of the Regulation, not limited to the 28 EU Member States anymore. With the new provision coming into effect in 2018, the processing of personal data of data subjects in the Union by controllers or processors not established in the Union will also fall under the GDPR in certain conditions, for example if the processing is related to the offering of goods or services, or to the monitoring of behaviour (Art. 3 § 2), e.g. in relation to internet activities: The new scope does not automatically include every webpage which is accessible from the EU but if services are directly addressed to citizens of EU Member States – mentioning of specific Member States, offering of goods in the Euro or the currency of the Member State – the processed personal data will fall into the scope of the GDPR even if the controller or processor is located outside the EU and EEA (for more information on the territorial scope of the GDPR and the consequences, see Heywood 2016; Marcoccio & Veneri 2016). The impact of this ambitious, globally targeted scope will be interesting to see in the future of the GDPR, but it will provide data subjects located in the EU with more possibilities to control the personal data also outside of the EU borders.

Regarding the roles of the data controllers and data processors, the GDPR has not been changed drastically in regards to the old Directive, and also further using the term ‘data subjects’ instead of individuals as it is used in the TFEU (see subchapter 7.1; de Hert & Papakonstantinou 2016, p.184). The problem with this distinction is – as argue also de Hert & Papakonstantinou (ibid.) – that this is not in line with the processing reality anymore. In modern data processing operations, the identification of a single data controller as “the natural or legal person […] which, alone or jointly with others, determines the purposes and means of the processing of personal data” (Art. 4 (7)) is not so easily feasible anymore. Although the role of the data processor has been included into more of the provisions, most importantly also into the territorial scope outside of the EU (Marcoccio & Veneri 2016, p.2), data processors are still defined as the person or body “which processes personal data on behalf of the controller” (Art. 4 (8)), even though in many recent cases, processors act rather independently from the data controller (de Hert & Papakonstantinou 2016, p.184). The GDPR introduces “joint-controllers” for cases where two or more controllers determine the purpose of the processing. However, having still as many roles on the data processing side makes it on the one hand difficult for DPAs upon investigation (ibid., p.185), but can also be troublesome for the data subjects when trying to exercise their rights.

Particularly the individual rights have seen some important improvement in the GDPR. While for some rights, the results of the recent case laws were specifically included into the GDPR – for example the 'right to be forgotten' is explicitly mentioned as an own article (Art. 17), other provisions and rights have gotten a lot more detailed. The Articles 12 to 14 set out a comprehensive list on "transparent information, communication and modalities for the exercise of the rights of the data subject" as well as information that has to be provided to the data subject and are mainly addressed at the data controller. The right of access (Art. 15) has not been changed greatly by the GDPR, however the right to rectification has been moved to a new Article (Art. 16) under a new Section – rectification and erasure – which also includes the above mentioned right to be forgotten.

Two new rights have furthermore been included into the section on rectification and erasure: the right to restriction of processing (Art. 18) and the right to data portability (Art. 20). The former can be obtained by the data subject if he or she contests the accuracy of the personal data or suspects an unlawful processing and limits the processing of the personal data by the data controller only to the storage of the data without further processing. The latter right is especially interesting for personal data being processed as result of internet activities. The right to data portability provides the data subject with the possibility to obtain his or her personal data in a 'machine-readable' format[21] in order to being able to transmit those data to another data controller, or have it transmitted automatically. A helpful right in the highly competitive field of internet services and social media sites, which seldom have an interoperability between the sites and in theory facilitates for example a change of the e-mail-provider by a lot for the individuals. Here again, the actual implementation and feasibility will be interesting to observe in the future.

The right to object (Art. 21) does again not differ greatly from the old Directive. An interesting new addition however is related to the automated decision-making and explicit profiling. While from a data protection point of view the provisions included in Article 21 are not as satisfying, since profiling mainly is allowed as it falls in the category of automated decision making. However, "suitable measures to safeguard the data subject's rights and freedoms" (Art. 22 § 3) need to be implemented.

[21] And by this underpinning the concept of the machine-readability of individuals as presented by Kreissl & Ostermayer (2011, p.281; see also chapter 4.2.1 p.40ff.)

Finally, some other important data protection provisions are included in the GDPR, which have been missing in the current data protection Directive (de Hert & Papakonstantinou 2016, p.192f.), starting with the provision on data protection by design and by default (Art. 25). Article 25 includes the privacy by design approach which was developed in the 1990s by the Information and Privacy Officer of Ontario (Cavoukian 2011) and was recognized in 2010 by the International Conference of Data Protection and Privacy Commissioners "as an essential component of fundamental privacy protection" of which the usage should be encouraged (Resolution on Privacy by Design 2010). Privacy or data protection by design "is based on the insight that building in privacy features from the beginning of the design process is preferable over the attempt to adapt a product or service at a later stage" (ENISA 2014). The Article 25 is not as specific in setting out the rules for data protection by design and only specifically mentions pseudonymisation and data minimisation. Thus also here the effectiveness of the implementation has to be awaited once the GDPR comes into force.

But not only the data protection by design and by default provision can be welcomed from a data protection point of view, but also three other provisions are an interesting addendum to the GDPR: the data protection impact assessment (Art. 35), the implementation of a data protection officer (Art. 37 – 39) and the codes of conduct and certification (Art. 40 and 42). The assessment of the impact of the processing on the protection of personal data is especially required when using new technologies or the processing "is likely to result in a high risk to the rights and freedoms of natural persons" (Art. 35 § 1). The implementation of a data protection officer is required for public organisations as well as private companies which have their core business in the processing of personal data, or process specific/sensitive data (Art. 37 § 1). The role of the data protection is described in the GDPR as on the one hand advising the data controller on data protection regulations and on the other hand surveilling the legality of the data processing (Art. 39 § 1).

The usage of codes of conduct (Art. 40) will mainly be beneficial for small companies processing personal data – small companies without a specific legal department or data protection experts can obtain specific aid in terms of how to comply with the GDPR in their specific field of operation. The functioning of the code of conduct practice will however depend on the acceptance and willingness of state authorities like DPAs and others in preparing, amending and extending codes of conduct in the different fields of application (Art 40 § 2; de Hert & Papakonstantinou 2016, p.192). Lastly also certification has found its way into the new GDPR (Art.

42). Also here the impact of the new provision will be interesting especially since Article 42 § 3 specifically states the voluntary character of the certification. However, as with other certifications in the industry and elsewhere, if there is enough supply and demand, the data protection certification model could be interesting in fostering trust of individuals towards certified data processing operations. Definitely benefiting from this new provisions are already existing schemes, like the European Privacy Seal (EuroPriSe 2016) or certification schemes in development, like the CRISP certification scheme (CRISP 2016). Also the co-regulatory character, combining legal provisions with self-regulatory aspects might prove beneficiary for the success of privacy seals and data protection certification, as also Rodrigues et al. (2013) discuss in their analysis of existing privacy seal schemes.

Although I was not able to fully analyse the new General Data Protection Regulation here – which content-wise could be a master thesis on its own – overall it can be said that the GDPR introduces interesting and important new changes and also updates some of the current provisions to be applicable with the current 21st century technology. Also the detailed provisions are welcomed, but necessary – already due to the legislative nature of the Regulation being adopted directly into Member State law and not requiring translation as with Directives. The harmonised approach will hopefully convey more consistency into the data protection provisions across the EU borders. But there is no reason to be too euphoric. The (new) provisions will also have to be implemented on the data controllers' and processors' side, the CJEU will probably also require to assess from case to case how the GDPR is implemented – and thus continuing to bring forth important Case Law. And it will also be important to continuously adapt to the rapid technological development, which will be no easy task keeping in mind that it took almost ten years from the first public consultation from the Commission in 2009 to the entering into force of the Regulation in 2018. It is however an important step to adapt data protection provisions to the requirements of the digitalisation of today and possibly the future. Instead of ignoring the ongoing digitalisation, the European Union has chosen the path of trying to shape the way by which personal data will be handled and protected in the digitalised future.

6.3. Data Protection – the Austrian Way

After having analysed the current Data Protection Directive and the new General Data Protection Regulation, the translation of the former into the Austrian Data Protection Act (Datenschutzgesetz – DSG 2000) will be presented in this subchapter. Also here, although there are many other different national laws addressing data protection principles,[22] I will mainly focus on the current DSG 2000[23] which has implemented the provisions of the 1995 Directive. Also the nine different Data Protection Acts of the Austrian Federal States will not be part of the analyses, as they mainly only complement the DSG 2000 (Sterbik-Lamina 2014, p.2). The first national Data Protection Act was introduced in 1978 (see Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten) and has since been amended several time before being replaced by the DSG 2000 on the 1st January 2000.

In the DSG 2000, the first Article defines the fundamental right to data protection and also includes the right to access, correction and deletion (Art. 1 § 1), as a result of the constitutional status of the ECHR in Austria (see also Sterbik-Lamina 2014, p.2). In general however, the DSG 2000 does not differ a lot from the 1995 Directive: The provisions on data quality and the legitimate use of data are ruled out in the § 6 and § 7, protection for the use of sensitive data is handled in § 9, the duties of the data processor are set in § 11 and the transmission of data inside and outside the EEA are regulated in the § 12 and § 13. As laid out in the Directive, the obligation of the data controller to notify the supervisory authority about data processing operations are to be included in a public Data Protection Registry [Datenverarbeitungsregister – DVR] (Part 4 Publicity of Data Applications §§ 16-22). However, exemptions to the obligation to notify the data processing operation were published by the Austrian Chancellery in the ordinance on the standard and sample applications of the Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004). If personal data is processed for reasons included in the standard applications (e.g. accounting and logistics, memberships, etc.) and the data is processed only for a certain duration, then the data controller does not need to notify the data processing operation to the DPA. There are 37 standard applications and 5 sample applications in total (e.g. hotel reservations, access control systems, etc.).

[22] See for example the Austrian Register Act (Meldegesetz 1991) or the Telecommunications Act (Telekommunikationsgesetz 2003). For a comprehensive list see: http://www.dsb.gv.at/site/6200/default.aspx (only available in German).

[23] The unofficial English translation of the DSG 2000 serves as a solid document for the analysis, as both the German as well as the English version are displayed side by side, by which differences occurring due to the translation can be reduced. The translation can be found on the homepage of the Austrian DPA: http://www.dsb.gv.at/DocView.axd?CobId=41936.

The data controller's duty to provide information, as well as the obligation to disclose the identity of the controller (§ 24 and § 25) are similar to the Directive and are considered to be the main method by which the data controller can inform the data subject about data processing operations and thus are again important for the following rights of the data subject (Part 5 of the DSG 2000).

The right of access to personal data is regulated by § 26 of the DSG 2000, by which the "controller [Auftraggeber] shall provide any person or group of persons with information about the data being processed about the person or the group of persons who so request in writing and prove his/her identity in an appropriate manner". The refusal of the right of access to data is possible by the data controller in accordance with several reasons stated in § 26 (2), but the refusal is subject to control by the DPA. In order to simplify the effort of the access to personal data for the data controller, the data subject must cooperate with the information procedures (§ 26 (3), meaning that if he or she knows in what data bases personal data might be processed, knows his or her customer identification number or similar, this information should be passed on to the controller. If the data subject is not cooperative, the right of access to personal data might be refused by the data controller.[24] In the DSG 2000, the right to access to personal data is also accompanied by the right to rectification and erasure (§ 27) and the right to object (§ 28).

One important amendment of the DSG 2000 was introduced in 2009 and came into force in 2010. The amendment introduced a whole new section to the DSG 2000 on video surveillance, which was handled until then like all other data processing operations. Since the processing of potential sensitive data had to be permitted by the DPA before the commencing of the processing – which included the recording of CCTV data – many of the installed CCTV systems

[24] This was confirmed by a ruling of the Austrian DPA upon a complaint of a data subject against a refused access request. The appellant filed a complaint with the DPA since the district authority had refused his request to access to data, reasoning that the authority had 38 data-bases in which the data subject might or might not be present. Since the search within all these collections would be too time-consuming, the district authority asked for specifications on the possibilities in which data base his personal data could be present. Although the appellant responded that he could not know in what data-bases the district authority would process his personal data, the authority still rejected his access request due to non-cooperation. The DPA ruled against the appellant and in favour of the district authority, with the reasoning that even though the data subject cannot specifically know in what data-bases his personal data is being processed, he could simplify the request by indicating additional details as his job situation, health status, residence, leisure activities, etc. See Datenschutzbehörde (2015): DSB-D122.272/0004-DSB/2014 vom 3. März 2015. This ruling shows the difficulty of the right of access to information: Not only can the data subject never really be sure what personal data is processed by the controller and thus has to rely on the validity of the statements of the data controller. But also in order to be cooperative with the controller and simplify the process, the data subject has to disclose even more personal information to the data controller. In the above mentioned case the DPA even advised to disclose sensitive data like the health status.

where not permitted (Sterbik-Lamina 2014: 3; ORF 2013). The amendment changed the necessity of a prior checking by the DPA if the installed system has only real-time observation, the recording is made on an analogue video recording system, or if "the video surveillance data are to be encrypted and (…) [the] analysis of the video surveillance data may only take place through a certain institution in a specific case by depositing the sole code key with the Data Protection Authority" (§ 50c). Also exempted from the notification to the DPA are CCTV systems operated for reasons of crime prevention amongst others in banks, jewelleries, petrol stations (see Bundeskanzleramt 2004 Standard- und Muster-Verordnung).

In the case of CCTV systems, the right to access to personal data is not handled differently than with personal data in general. §50e (1) regulates that the processed personal data can be either sent in a common technical format, or the data subject can request to inspect the data on a reading device of the data controller (including obtaining a digital copy of the data). If in some cases the requested information cannot be disclosed (i.e. "because of an overriding legitimate interests of third parties or of the controller" (§50e (2)), the data controller has to provide a written description of the behaviour processed by the CCTV system, or obtain access where third persons have been made unrecognizable. Only in case of real time CCTV surveillance, the data subject has no right of access to data.

An important exemption of access rights in the case of CCTV has been issued by the DPA regarding the video surveillance system of the public transport company of Vienna – the Wiener Linien. The CCTV system of the Wiener Linien records the images for 120 hours for the security of the passengers and the staff, but also in order to reduce vandalism. If no incident is reported, the footage is deleted already after 48 hours (Sterbik-Lamina 2014, p.9). Also the footage is encrypted with the DPA as the only encryption-key holder. The Wiener Linien argue that since the data is not analysed, granting the right of access to data would start the data processing, requiring an analysis of the data and thus potentially identifying the individuals – which is why the access to data of the non-analysed CCTV data is not granted by the Wiener Linien. This practice was complained to the DPA who however confirmed the lawfulness by the Wiener Linien in handling the subject access requests in a ruling in 2008 (Datenschutzkommission 2008). Although this ruling was cancelled by the Austrian administrative court of justice in 2011 (Verwaltungsgerichtshof 2011) due to the partiality of the DPA as declared by the European Court of Justice (see next section), the ruling was repeated (against another complaint) by the newly established – impartial – DPA in 2013 (Datenschutzbehörde 2013). This ruling was later confirmed by the Austrian administrative court of justice in 2014 (Verwaltungsgerichtshof 2014). The reasoning behind this ruling is insofar interesting as for the data controller as well as the DPA and the administrative court of justice data is not identifying if it is only stored for a short period of time and not further analysed (as it is the case with the CCTV data of the Wiener Linien) and the analysis of the material, in order to comply with §26, would be potentially identifying also other individuals and thus is an intrusive act. Theoretically this reasoning could be applied to CCTV footage which is only stored for 48 hours and is in general encrypted, making an analysis only possible for a specific reason – and thus not eligible for a disclosure to the data subject as stated in §26 and §50e.

Lastly another important deviation of the Austrian data protection legislation from the Directive is the installation of the national data protection authority at the Austrian Chancellery. Before the 1995 Directive came into force, the Datenschutzkommission (DSK) in Austria was part of the Austrian Chancellery. Since the Directive 95/46/EC requires the "complete independence in exercising the functions entrusted" to the national supervisory authority (Art. 28), this would have required a separation of the Datenschutzkommission from the Austrian Chancellery. The Austrian government however, upon implementation of the Directive in the DSG 2000, did not only not foresee this separation and independence of the DSK, but the managing member of the DSK also always had to be an official of the Federal Chancellery, making all "day-to-day business of the DSK (…) thus de facto managed by a federal official, who remains bound by the instructions issued by his employer and is subject to supervision" (Grand Chamber of the European Court of Justice 2012).

The Commission sent a letter of formal notice to the Republic of Austria in 2005, stating that with this combination, the DSK was not completely independent as required by the Directive. Since the observations of the Republic of Austria did not satisfy the opinion of the Commission regarding the independence of the DPA, the Commission filed a case at the European Court of Justice (ECJ) in 2009. The Grand Chamber of the ECJ decided in favour of the Commission's point of view by observing that "[t]he fact that the office is composed of officials of the Federal Chancellery, which is itself subject to supervision by the DSK, carries a risk of influence over the decisions of the DSK. In any event, such an organisational overlap between the DSK and the Federal Chancellery prevents the DSK from being above all suspicion of partiality and is therefore incompatible with the requirement of 'independence' within the meaning of the second subparagraph of Article 28(1) of Directive 95/46" (Grand Chamber of the European Court of Justice 2012). Resulting from this ruling, the DSG 2000 had to be amended in order to guarantee the independence of the DPA, restructuring the DSK and by this also renaming it into the Datenschutzbehörde (DSB) starting 2014.

Finally, the role of the Data Protection Officer (DPO) needs to be highlighted here. While in Germany public and private organisations with more than nine employees carrying out the automatic processing of personal data on an ongoing basis (Federal Data Protection Act 2009, §4f.) need to install an internal Data Protection Officer who ensures the compliance with the Act (ibid, §4g.). This is not compulsory for Austrian organisations. While there might be changes regarding this with the forthcoming GDPR, currently every organisation can choose whether a Data Protection Officer is appointed or not. This is insofar important as the empiric data in the next chapter will partly rely on interviews with internal Data Protection Officers of organisations, but also partly on interviews with organisations which have no internal DPO appointed. Their role will thus also be analysed in the next chapter.

Overall, as I have shown above, the Austrian practice regarding the data protection law does not differentiate drastically from the European Directive. The case of the access rights of CCTV data of the Wiener Linien is however definitely a particularity – probably also in comparison with other countries. If the new GDPR, aiming at more harmonised data protection laws in the Member States, will change anything regarding this practice, has to be seen, also since the right of access to data will not be changed drastically.

7. DPA – Data Protection in Action

*This chapter will present the findings drawn from the interviews with 'surveillance workers' in different organisations in Austria. Firstly (**7.1**) I will provide a short outline of 'who' was interviewed, and an overview of the diverse fields of organisation will be included. It needs to be noted however that I will neither give specific information on names and details on the persons, nor on the details of the organisational affiliation of the interviewees, guaranteeing anonymity for the participants. Secondly (**7.2**) I will show the results of the interviews. The data which were collected consist of a broad variety of information, each of the interviews giving detailed insight into the many influences on data collection and data protection practices in Austria and how they are dealt with – on a personal/interviewee level and on an organisational level. The analysis of the interviews provides details on how legal requirements are interpreted and sometimes even tried to exceed, but also what kind of struggles are experienced in the day-to-day operations concerning data collection and data protection.*

*****

7.1. The Preparations – Interview partners, Interview conduction and Interview data

Let's first start with some general information on the empirical research of this master thesis: the interview conduction, the interview partners and the analysis of the data. A total of eight qualitative expert interviews was conducted during the months June and July 2016. While in total at least 10 interviews were envisioned, and 15 interview requests were sent out by e-mail, a lot of these requests remained unanswered to-date, even after re-inquiring and thus already showing that there appears to be a lack of desire in talking about data collection and data protection practices in some organisation.

Although the identification of the specific sites was not so difficult, the identification of the interview partners was more challenging. As with the identification of the data controller in the research by L'Hoiry, Norris et al. (2014), finding specific contact points, names, phone numbers or e-mail addresses is often not possible. Data protection notifications on websites have frequently listed only a generic contact address, like 'info@organisationxyz.at', with some researched sites even lacking data protection notifications. Obtaining contact details through the public Data Protection Registry was also not always successful, as not every organisation which was planned to be included in the research was listed in the DVR or if, sometimes lacked contact details. While the specific names of the companies and institutions will not be listed here for reasons of anonymity towards the research subjects, I will give a general overview on the types of organisation.

Successfully conducted	Non-response
Administrative body	Administrative body
Educational institution	e-commerce company
Educational institution	Financial institution
Financial institution	Retail company
Retail company	Social networking provider
Telecommunication provider	Social networking provider
Transportation company	Social networking provider
Transportation company	

Table 2: Types of organisations with which interviews were conducted or where no response was obtained.

The choice for the businesses in Table 2 was mainly based on their field of operation and the included processing of personal data. Each of these organisations has a wide range of personal data which is processed and can also contain sensitive data. Also each organisation – whether public or private – is located in a field which the data subjects generally use on daily or weekly basis and thus in which they are also regularly part of the data processing and surveillance operation.

Why almost half of the requests remained unanswered can only be speculated – whether the potential interview partner never got the request due to getting lost in the inbox of the generic contact address, or whether the requested interview partners did not want to participate. I suspect that the reasons for non-participating could be twofold. On the one hand, especially smaller organisations could have been intimidated by the topic of research, with data protection being a sensitive topic. If there is no one available who feels confident enough to talk about such a complex theme, the willingness of participating probably goes down by a lot. On the other hand, organisations and corporations with their main operation being data collection and data analysis probably did not want to provide insight into their practices. But as I mentioned above, this can only be speculated.

I initially already considered that obtaining access to organisations could be difficult, which however turned out other than expected: While I anticipated that mainly larger organisations would deny my interview requests, they were generally more willing to provide information than smaller organisations. Almost none of the smaller organisations (small mainly in the terms of a smaller reach of data collection as a result of having fewer clients/data subjects) answered my interview requests. With larger companies and administrative bodies, I was confronted with a lot of interest in my research topic and an openness I had not expected. Exceptions to this were foreign multi-national organisations. While some of the interviews I conducted were with employees of corporations which also had large international operations, their main location was nonetheless situated in Austria. Non-responses were however obtained by large foreign corporations which *also* operated in Austria but were mainly situated in other countries.

Nonetheless, the lower amount of interviews than initially planned had no influence on the quality of the data analysis and the validity of the results, as also every none-response provided a result in its own – the presence of certain organisations which do not want to disclose their practices concerning personal data. The material which was collected contains a lot of detail, with some practices which were observable among multiple interview partners, while others only applied to individual partners. As Table 2 shows, the range of organisations where interviews were conducted is diverse, comprising publicly run institutions and businesses and private companies and also some of which have international operations. The variety of operations of these organisations is thus also diverse, including different kinds of personal data they are dealing with, ranging from basic customer data to sensitive data. The organisations also vary in terms of size – some of them having more than ten thousand employees, operating in several countries, or having millions of customers. Each of these organisations produces a large amount of personal data that needs to be dealt with and requires protection. But also in regard to the interview partners, the positions they hold within their affiliation varied. While the majority were specifically the data protection officer or head of data protection and compliance, some other interviewees were simply employees with data protection and data collection tasks or knowledge.

Face-to-face interviews were chosen for all but one interview, which was conducted on the telephone. Most of the interviews were conducted with only one respondent, except for one interview, where two interviewees were present. Also with the exception of one, all the interviews were recorded and transcribed afterwards. Only for the telephone interview, extensive notes were taken and translated afterwards into memory minutes. The interviews lasted between half an hour and one hour, often consisting of a main, formal part which was recorded and a more informal part at the end of the interview, which occurred only after the ‘official’ interview was concluded. In the course of the two month of conducting interviews, a research diary was kept in which notes and memos of interesting and noticeable moments, which had occurred during the interviews, were kept. This included also some notes on the informal parts of the interviews. Demographic data on the interviewees was not collected, as this data has no importance for the analysis of the data and the answering of the research questions.

The transcripts of the interviews were analysed and categorised using the program MAXQDA12. Initially seven main categories were created, with some sub-categories, which related to the main aspects of the research questions and sub-questions. In the course of the analysis, the main categories were extended to twelve as a lot of additional information came up during the interviews, which was worth including into the findings. Finally, for the presentation of the findings, some overlapping categories were consolidated again, reducing them to the following five which will be addressed in detail in the next section:

- Organisational structure and data protection
- The intertwined roles in data collection and protection:
    - Surveillance Worker
    - Surveilled Worker
    - Data protection officer
    - The technological backstage
- Expert knowledge in data protection
- The relevance of data protection
- Pressure groups and the ‘others’ as surveillance workers

As a final disclaimer, the findings of the interviews will in general be presented as paraphrased and interpreted sections. The use of direct quotes from the interviews will be reduced to an absolute minimum as some of the respondents preferred not to be quoted directly.

7.2. The complex state of organisational data protection

I will start the analysis with a quote by Marx (2011, p.85), which serves very well as an introduction to the broad field of what I call "the complex state of organisational data protection" in my sub-header:

> "We can identify the surveillance agent as watcher, observer, seeker, inspector, auditor or tester, while the person about whom information is sought is the surveillance subject. However, given the multiplicity of the new surveillance both, agent and subject play increasingly both roles in the socio-technical environment, although hardly in the same form or degree. They are sometimes blurred and may overlap, even for the same person in the same setting. Certainly the camera, audio recorder, or motion detector will capture whatever is encountered independent of social factors – whether economic level, gender or ethnicity."

The overlapping and blurring of the roles of the agent and the subject in the new surveillance, as Marx calls it, or of the techno-social hybrid as Kreissl nicely puts it, is also something brought forth in some of the interviews, as a shaping factor of the practices in the organisations. But before we get there, I will start with some framework conditions, a description of the status-quo of organisations (see Preisendörfer 2011, p.58): Using Abrahams and Büschges (2009, p.163f.) model of organisational roles, which are empirically assessable through the relating behaviour, can serve in describing *how* data collection and protection is handled inside organisations.

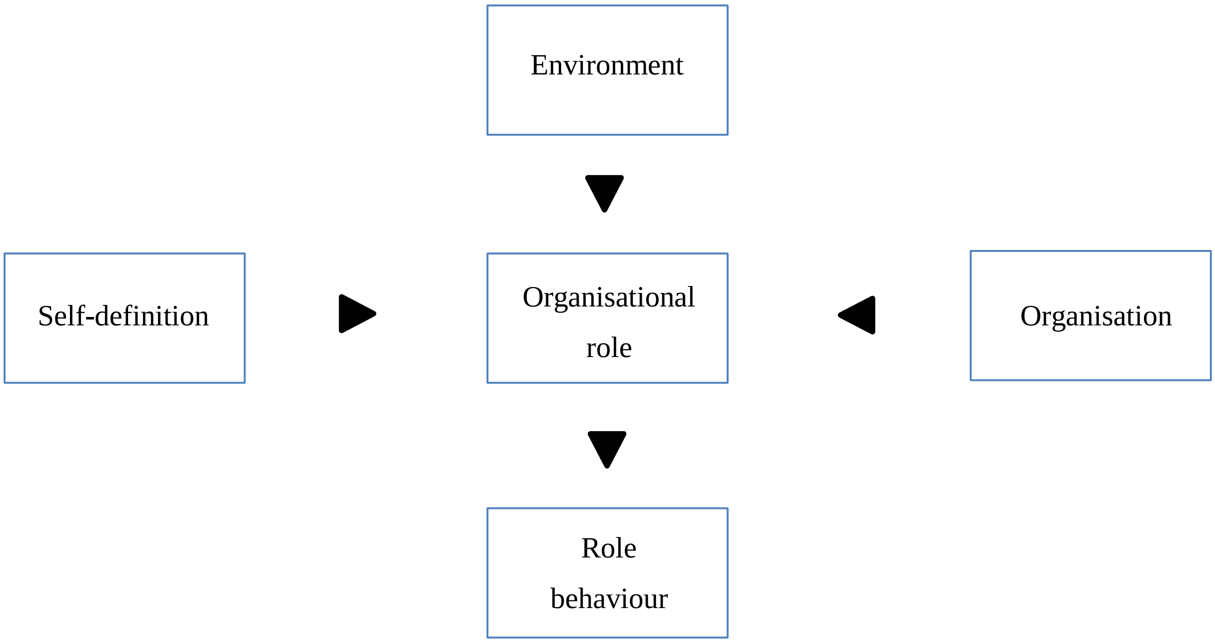

Figure 2: Factors influencing the organisational role and in consequence the behaviour related to the role (c.f. Abrahams & Büschges 2009, p.164).

As Figure 2 shows, there are different factors which influence how roles within the organisation are structured, tasks and goals related to that role defined and thus also how role-bearers behave. In relation to the analysis of the interview, it is the ‘data protective behaviour’ of those involved in data collection and data protection practices which is influenced by the organisational structures of data protection, the roles involved in the practices, the managing of the required knowledge, and also the relevance data protection has within organisations – which subsequently is of analytical significance. And finally also of what I call pressure groups, a range of environmental factors with causal relations on the described practices.

7.2.1. Organisational structure and data protection

Providing an overview of how data collection and data protection is structured within private businesses and public institutions not only gives a better understanding of the chapters to come. I think it also helps getting a first grasp of how implementation of data protection in organisations can be managed differently and by this already laying the path of how ‘data protective behaviour’ is shaped. According to Preisendörfer (2011, p.59; p.66) and following Scott and Davis (2007), organisational structures are one of the core elements of an organisation, which can be divided into the formal and the informal structures. First I will focus here on the formal organisational structures, “the construction plan of an organisation” or the “totality of the precepts of how an organisation should be like” (Preisendörfer 2011, p.66, own translation). In general, organisations are structured and planned, often hierarchically according to which individuals of the organisation can interact with each other and to which the tasks are arranged amongst them. These structures can be seen as mechanisms leading to stable patterns of behaviour within such associations (Abrahams & Büschges 2009, p.131).

As such, also the organisations included in my research follow this hierarchical formal structure, shaping the arrangement of the tasks of the company or administrative body accordingly. However, how these are arranged differs greatly in my sample and thus also how data collection and data protection as essential tasks of the organisation are arranged. Some are divided into specialised institutions and units each with their own responsible for data protection, sometimes with one general employee ‘overseeing’ the operations or serving as contact point. Data protection being decentralised can be seen as an advantage, and some of the respondents also saw it as such. It implies that single institutions or units need to be aware of their data collection practices, of what is allowed and what is not, thus generally raising the awareness of the data protection within the structures, and also denying the possibility of laying the responsibility of data protection off to other units, like the legal department. Although externally there needs to be one specific legal responsible – the data controller – in these cases this responsibility is internally transmitted to each separate unit.

The functioning of such a structure however depends highly on the actual awareness of the importance of data protection in each unit. And also the required knowledge needs to be managed and transferred amongst multiple employees, which can be challenging for larger organisations. As such and something that was reported in one of the interviews, it can also happen that this division of responsibilities leads to a negation of such tasks and in further consequence to a point where data protection is scarcely cared about or even considered as a nuisance.

Other organisations are structured differently. Here, specific units for data protection and privacy are often the way of managing data protection, overseeing the handling of personal data of all kinds and thus responsible for ensuring the correct processing of such data. Especially for large institutions or internationally operating corporations it appears as if this is considered the easiest way of having oversight and managing all the employees and the personal data they might come in contact with. The structure in this context is often that the data protection unit is assisted by representative ‘data protection officers’ in all the other units, facilitating the communication amongst them and enabling a close cooperation between them in terms of data protection issues. Businesses operating internationally but with their parent company located in Austria administer this structure similarly – with the main data protection office located here overseeing all the other foreign branches which each also have specific data protection officers operating at a local level.

The data protection units – where established – are also organised hierarchically within the companies and administrative bodies. For some of the units, a clear positioning of the hierarchy within the company or institution is difficult to identify. And although none of them appears to be ‘a toothless body’ within the organisation, some respondents expressed a certain lack of understanding from time to time when raising data protection concerns. Other respondents revealed that their unit reports directly to the management, with one data protection officer even having a universal veto power which can only be overruled by the CEO of the corporation. This can already indicate how the structure of an organisation and the localisation of the data protection within these structures can also influence the way how personal data is dealt with, as we will see in the following chapters. A certain structural division can also be observed in regard to whose personal data is concerned. Some organisations have for example a specific data protection advisory board which is solely responsible for the protection of personal data of employees and has thus a large focus on the prevention of workplace surveillance within the company and subsequently also brings forth a high importance of data protection.

While the above mentioned practices only entail data protection from a legal / operational point of view, data collection, protection and security from a technical point of view is – at least in the majority of the interviews – mentioned separately. The technical aspect of personal data processing is obviously located within the IT-department due to most of the operations in relation with personal data being done electronically (with some exceptions which are outlined in the next chapter). Data protection thus also needs to be coordinated with the IT-unit of the organisations, which at least concerning the structural hierarchy within the organisation received only little attention during the interviews. Although the technical security of personal data is considered as an important factor in the protection of data, it is treated on a whole different level by the respondents, which often also combines with a missing knowledge of the technical processes behind the operations, as I will show in sub-chapter 3.

Finally, an interesting side note which was mentioned by some of the interview partners en passant was the changes their units dealing with data protection had undergone in the last several years, which crucially shaped the operations of each of the units or of the data protection management in general even. In some organisations, the unit privacy and data protection was initially located within the legal and compliance department and separated into a single unit. In other organisations, data protection as such saw an increase of importance by institutionalising it newly into the company. It seems as if in some of the companies, generally an increase of importance of data protection issues has emerged within the last two decades. This seems to be in line with the general increased awareness of the problematic behind surveillance and data collection practices in the society, observable for example in the emergence of the field of surveillance studies and thus the theoretical and empirical involvement with such practices by researchers. With the new GDPR coming up, a further increase of importance can be expected like also some of the DPOs mentioned – especially in relation to the requirement for data protection certification and Privacy Impact assessments (PIA). PIA is “a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme and finding ways to mitigate or avoid any adverse effects” and is thus also considered as a useful tool which demonstrates internally as well as externally the importance for privacy and data protection within the organisation (Wright et al. 2010, p.351).

7.2.2. The intertwined roles in data collection and protection

Having shown how data protection can be structured within organisations, I will continue with the different roles operating in data collection, data processing and data protection. Smith's notion of surveillance workers as the "responsible for the daily operation of surveillance" (Smith 2012, p.107) can be seen as a starting point for this subchapter – bearing in mind the more general notion of surveillance *as the monitoring or scrutiny of individuals and groups of people, their actions and communications, as well as their different contexts by technological means in order to extract specific information* defined in Chapter 3. However, the roles which have been unveiled by the respondents often go further than this, encompassing multiple tasks beyond the simple extraction of information from data, sometimes apart from technological means. This is why in this sub-chapter I will introduce three roles involved in data collection and protection which are often closely intertwined and which are all influenced by the 'technological backstage' managing the data:

- The surveillance worker and other employees involved in personal data processing
- The surveilled worker
- The data protection officer

The technological backstage

The surveillance worker

The role of the surveillance worker involves a wide range of contacts with personal data, irrespectively of their affiliation. Although not having been my prime source for data collection – except for one interview – the other interview partners could also provide some important insights into their roles and tasks within the company. As Table 2 (p. 90) shows, the range of activities of the organisations vary greatly and thus involve different kinds of personal data that are processed, from communication data, over financial data to socio-demographic data. The majority of this data is managed in large data-bases, often managed by the IT-department utilising specific data-management software. It is in this kind of software where specific data protection parameters can easily be included, and which is indeed also one of the tasks of the data protection officers – to decide on what an employee has the right to access and process what kind of personal data. These decisions depend on what unit requires what kind of data and often involve a re-traceability of the steps taken by the employee, increasing the reliability of the data protection measures and manipulation of personal data beyond the access rights.

However, mismanagement often happens where this is not the case and personal data is processed in other ways. Spreadsheets like excel files are still a popular method of storing personal data, especially if these only contain small lists, need to be stored quickly or edited on a frequently basis. Also amongst other employees who are not as much confronted with personal data, the collection and management of such data is often done rather carelessly and without consideration of the possible implications of unauthorised accesses.

While for the first, the centralised data-bases, in general a certain awareness on the nature of the processed data is present amongst the surveillance workers, this is frequently not the case for decentralised data-bases like excel sheets. Even though this is generally done unintentionally, the dealing with such data is often careless as the data itself is not identified as personal data. Thus there appears to be a certain discrepancy between certain forms of data processing, depending on the technical means/software used. A more specialised – as data processing identified – software introduces an authoritative character on the surveillance worker. He or she is not only *forced* to use the data processing technology, but the usage is also often followed by a lack of understanding of the actual methods behind the technology. Yet, the technology is programmed in such a way that the data protection mechanisms are forced upon the user/surveillance worker and as such he or she does not need to specifically consider privacy implications in relation to the management of the data. This is what Zhang et al. (2016, p.74f.) call authoritative technology adoption, which is shown here that this approach can have success in enforcing certain regulations. However, as Zhang et al. also note, it is important to understand how the users adopt the technology and if they “make the best use of it and perhaps motivate (…) to improve their knowledge”, enabling a maximisation of “the benefits that the technology can bring to the society” (ibid., p.75). It can be assumed that this is not always the case and some examples of the interviews also show this. When surveillance workers use spreadsheets next to their centralised data-bases and maybe handle the personal data included rather carelessly, it seems like the intended message of the authoritative technology has not been transferred. Despite the technology working as planned, its message of being careful with personal data is not translated on other – even very similar – technologies. As such it creates situations where the awareness for data protection is high amongst the surveillance workers in general, it sometimes lacks in the detail.

Some of the respondents were also aware of this issue and stressed the importance of dealing with this through increasing the knowledge and raising the awareness amongst the surveillance workers in this regard. Specifically, interviewees described that promoting data protection amongst co-workers also entailed rather trivial explanations like not having other customers watching the screen, being careful of scraps of paper containing personal data, or especially in the educational sector not hanging out lists with marks of the students after exams. Also access to personal data by thirds needs to be included here, in which it is important that the surveillance workers are wary about the impact of granting others access to personal data of their customers. While it might in general be clear that thirds are not to be granted access, if the thirds are related to the data subjects in some way, this is not always obvious – if for example parents ask for the process of their son's studies, or employers want to access the telecommunication data of the phones of their employees. Often these kinds of details of data protection principles are the ones the surveillance workers need to be made aware of. And although in general the standard of data protection in the organisations which are included in the research seems to be high, there are some exceptions nonetheless.

The reasons for these exceptions can only be speculated about, as the interview material provides too few data for this. It can be assumed that due to the irregularity of such events to happen and not being part of the daily routine of data processing, the knowledge and consciousness for these practices are lower than with other data protection practices. And furthermore, as already noted above, not entirely understanding the operations behind data processing and thus also not being made fully aware of the width of the operation can also contribute to having surveillance workers not being entirely knowledgeable on the required extent of data protection. Thus, as shown above, and relating to Abrahams and Büschges (2009, p.162f.), the roles within organisations are shaped by different influences, like the organisation itself or its environment. However, it is also the self-consciousness of the role-bearer, a self-consciousness on the tasks and duties combined with self-interests and goals, which has an influence on how the employees define their role – in this case the role of the surveillance worker and in further consequence the relating behaviour contributed to that role – in this case the 'data protective behaviour'.

The surveilled worker

Although not addressed in particular during the interviews, the role of the surveilled workers was also discussed by some of the respondents. Especially in the companies with a data protection advisory board, the importance of the protection of personal data of employees was mentioned. With the advisory board serving as a 'lobby' for the protection of employee data, it is tried to ensure that workplace surveillance is kept to a necessary minimum in terms of administrative processing and that new initiatives of surveillance are assessed on their potential of being intrusive. Already when viewed historically, employees in Austria have always had a strong lobby supporting the rights of the employees, due to the existence of strong trade unions and the institutionalised co-operation between the representations of employers and labour in Austria, also called the *Sozialpartnerschaft*. And thus particularly with regard to the automatization and digitalisation of work-related processes, where the possibilities related to workplace surveillance have become increasingly relevant, the availability of a lobby against workplace surveillance is more important than ever.

It is particularly in relation with the introduction technologies of control where constraints in terms of data protection occur. Access cards which are employed in many of the companies involved here can easily be misused for controlling the whereabouts of the employees. Thus generally being of purpose, the misuse of the technology for surveillance purposes was mentioned as being equally important in terms of prevention as the misuse of customer data.[25] Also here, the acceptance of limitations due to data protection concerns is not always given, especially by proponents of certain control mechanisms. Although often not with bad intentions, the oversight of the employees' activities through technology and data collection is considered as an appropriate means.

The hierarchical structure which shapes organisations entails an unequal distribution of power and authority. And although such structures are necessary for the functioning they are not incontestable, specifically if the results of the asymmetrical power distribution are in conflict with the goals and interests of participants of the organisation, as is the case with workplace surveillance (Abrahams & Büschges 2009, p.126f.). In the organisations included in my research, the introduction of restrictions on such practices and, similarly as with customer data or administrative personal data, raising awareness on what is allowed with the personal data of employees

[25] This however does not mean that this was not of importance for other respondents. As workplace surveillance was no specific topic to be addressed by the interviewer, statements on the level of importance cannot be made.

and what is not seen as the approbate means of contesting surveillance. Leading to a self-identification of the role of surveillance workers – here in terms of watching over co-workers and employees.

The data protection officer

Finally, the role of the data protection officer – with whom most of my interviews for my thesis were conducted – was often described as being the lobbyist of the customer data. As already described before, it is not every company or administrative body which has installed an employee or unit specifically designated as data protection officer. However, in these organisations the tasks which are linked to the DPO are covered in some way or another by other employees and units. Thus when I describe the role of the data protection officer here, this does not specifically mean the legal concept – as it is for example provided in the German data protection legislation and in the forthcoming General Data Protection Regulation.

The tasks of the data protection officer can mainly be broken down to three areas: *prevention*, *operation* and *crisis management*. Although only one company had their data protection unit specifically divided into those three areas, all other organisations which had a data protection officer installed functioned with the same logic. Looking at each of the areas I will start with the *prevention*, entailing behavioural as well as process-related prevention. For the first this means raising awareness amongst the employees of what personal data consists of, how to handle such data and why data protection is considered to be important. While this is often done in a more informal way, awareness-raising is also included in general staff training and in specific data protection trainings for personnel dealing with personal data. Only if a specific knowledge on data protection is available and the importance of this topic is transmitted, the self-consciousness of the role of the surveillance worker can be established.

Process-related prevention encompasses the more technical part of data protection and includes tasks like the issuing of authorisations and access rights – who is permitted what kind of processes and manipulation to what kind of data – in order to guarantee that no one has access to data for which there is no 'business-need.' Access rights serve as a good example as one of the tasks of the data protection officers, which come closest to controlling the employees as well. Access rights in organisations require some kind of oversight for making sure that these are not misused by employees, in which thus the behaviour of the surveillance workers is monitored. Furthermore, it is in the process-related prevention – which is executed through technical means – in which the authoritative technology (Zhang et al. 2016, p.74f.) is programmed in such a way that the interests and goals of data protection are enforced on the surveillance worker. In the terms of the Actor-Network Theory, this is a good example for the black-boxing of a value-laden technology which, as shown before, requires a deconstruction by the surveillance worker if the value of data protection should be induced more thoroughly. Finally, situated between the more technical process-related prevention and the behavioural prevention is the classical risk analysis, in which (new) projects are assessed on the identification of legal, economic and technical risks in relation to data collection and data protection and how these can be mitigated. This task often includes the analysis of both the behaviour of the employees as well as the process behind the data collection and management practices.

The second area of tasks of the data protection officers is the *operational* part. Operations of the DPO include both external as well as internal orientated actions. The first are practices like the notifications for the data processing register, the general contact with the data protection authority of Austria, or public communications. While for many smaller businesses, the amount of notifications is often not so high, some of the organisations interviewed here have more than hundreds of uses of data in their entire corporation which all need to be registered one by one at the data protection agency and kept up-to-date. And although this no longer becomes necessary with the new GDPR, the use of data still needs to be protocolled thoroughly. External communication with the DPA can be necessary in case of proceedings or when violations are suspected, but also for informational exchange. Some data protection officers explained the good relations they had with the DPA, often due to previous affiliations, which facilitated the exchange of information and the communication between the organisation and the DPA.

Furthermore, a very important part of the externally orientated actions of the data protection officers is being the contact point for the general public and the data subjects. Requests for information, rectification or deletion of data are generally addressed to the data protection officers, in organisations without a designated DPO, these requests are generally addressed to the IT-department where the requests are processed and answered. The right of access to personal data – §26 in the Austrian data protection regulation – is often the main contact point between the organisation and the data subject in terms of data protection issues. Interestingly, these requests are handled slightly differently amongst the organisations. Only few have installed an automated process of granting access to data.

If such a process is installed, the access granting is a normal operation which requires only little effort, as the employees only need some basic information like the name of the customer upon which all information of all the data-bases and uses of data are collected automatically, printed with the top sheet being blank for not disclosing information to others handling the file and finally sealed in an envelope and sent to the requester. One organisation did not even require an identification of the data subject, as the access to data is always sent as a personal registered letter for which the recipient must provide an identification upon accepting the letter and thus in further consequence does not need to disclose more personal data (by sending a copy of his or her identification document) for obtaining access to data.

If the process of access to data is not done automatically, some involved persons like the data protection officers noted the time-consuming effort behind answering those requests. As already shown, some businesses and agencies have multiple data-bases and hundreds of uses of data. Without the help of the data subject him- or herself, providing access would require a great effort in searching through x-hundred applications of data and collecting all the pieces of information. It is thus necessary that the data subject contributes to the process by indicating at least in what kind of applications and data-bases he or she could be included. And while a cooperation of the data subject in the subject access requests is also designated in the data protection legislation, it entails a problem of what L'Hoiry and Norris (2014, p.34) refer to as "unknowables" when dealing with incomplete personal data disclosures. L'Hoiry and Norris describe how data subjects cannot know if the disclosures of their personal data upon requesting access are complete or not due to often having too little information on the full amount of data being collected by organisations. Thus, if asked for cooperation through the organisation by indicating in what data-bases the data subject could be included, similar difficulties can emerge. One does not only need to know what data-bases are used within the organisation, but also in what data-bases personal data could be processed. Although the organisations most of the time only require some information relating to the data subject in order to assess the possible location of the data, it still makes it un-transparent for the data subject as possible data-bases where he or she has no idea about can be excluded easily.

Thus, in organisations where the access to data still requires manual operations, such requests produce a lot of work. Since the requests are however only rarely made to the data protection officers – the estimated numbers fluctuated between less than 10 to around 30 per year – it appears as if the answering is of no real problem. However, as many of the interviewees also revealed, an increase in subject access requests would probably be unmanageable due to the amount of time each request takes to answer. Especially where this work needs to be done or monitored by the data protection officer, an increase of workload with subject access requests is experienced as having less time available for other data protection tasks.

It appears nonetheless that subject access requests – which are obtained by the data protection officers – are answered in the completest way possible by the respondents, disclosing the personal data which is processed in the organisation. But it also appears as if not every request is immediately obtained by the data protection officer. If such requests are for example posted on the Twitter or Facebook account of the organisation, it is possible that they get lost in the meantime. As such the advice L'Hoiry and Norris (2014, p.42f.) have already given in relation to the subject access requests is that a clear information, a better communication of the right of access to data, the required information for the data protection officer as well as the correct address to send the request to can facilitate the process of disclosing personal data immensely – of which not only the data subject benefits, but also the data processing organisation in the form of the data protection officer. Which was also something one DPO noticed and already initiated, that due to the increase of subject access requests they had obtained, and the difficulties they had encountered upon responding to those requests, their internet presence needed to be redone in order to provide clear information, first on what data subjects should expect upon sending a request (thus specialising what kind of personal data is really collected, where it could be stored but also what kind of information cannot be obtained) and second what to include in the subject access request.

Although not specifically included into the task of the data protection officer, a few of the interviewees also acknowledged their societal obligation as 'lobbyist for the data subjects'. Creating awareness not only within the organisation but also towards the data subjects was seldom but nonetheless seen as something the data protection officers could influence. Data protection should not only be put in the hands of the others, but should also be actively practiced by the data subject. It is however here a lack of awareness which was identified by some:

> "We can do a lot, but they also need to do themselves . . they need to manage their own data. . But it is the same problem as it is with the passwords, it is . it simply is like this that no one can remember the passwords, even though everyone says, god please use a complicated password. It doesn't matter. Everyone uses easy passwords, or many of them . . ." [Interview 2; Position: 57-57]

Addressing these issues already at an early age is seen as a key factor for promoting data protection by some of the interviewees, which is also why one the respondents actively engages in schools, talking about the importance of data protection.

But the *operational* work of the data protection officers does not only extend to external actions. Internally, the area of operation largely entails to serve as a consultation point for personal data related concerns of employees or in projects, requiring information and assistance. Particularly for corporations working internationally and also outside of the European Union, the importance of consultations of data protection matters are increasingly acknowledged and thus also increasingly requested. With the new GDPR in close vicinity, some of the interviewees have noticed a growth in uncertainty within the organisation often related to the announced fines in relation to non-compliances with data protection regulations, which has brought forth the importance of data protection for some.

As was already described above, due to the hierarchical differences of the data protection unit within the companies and administrative bodies, the internal operations can vary in relation to the obligation of the issued consultations of the data protection officer. In some organisations, these have a binding character and thus are treated as directives which need to be complied to internally. In other organisations, the consultations are only regarded as recommendations upon which decisions can be made if these are included or not.

Lastly, *crisis management* although not often required is considered as an important task amongst the respondents. In comparison to the other two tasks, crisis management often involves only a supportive role by the data protection officers, with the main tasks related to IT-security. Nonetheless specific strategies for managing crisis like a data breach or hacking attempts are in place, which in case of occurrence only need to be slightly adapted to the extent of the crisis. And while the general crisis strategies in place follow a similar structure – identifying and closing the leak, and communicating internally as well as externally on the issue – there are still some distinctions between the organisations. Often depending on the sort of data processed, the frequency of attacks can vary. Predominantly exposed to external threats and attacks are the telecommunication as well as the financing institutions who thus in turn also seemed to have more experience in dealing with such crisis.

With crisis management, the communication with the scrutinized was equally considered an important step, on the one hand for informing the data subject about the issue and what the possible implications could be. On the other hand, the communication also has the goal of customer relations, trying not to lose customers despite the mismanagement of their personal data. Having the clients’ trust that their personal data is still safe within their company is essential here, although not always feasible. One respondent for example explained that after they had

had a data breach as a result of social engineering by an internal operator, several customers responded with subject access requests – wanting to know what personal data is still processed by the organisation – of which again a few followed up with requests for deletion of data.

As is shown, the role of the data protection officer is broad with a range of tasks requiring different skills, from communication to managing. While in the Austrian data protection legislation a formal data protection officer is not provided for, the instalment of this position seems to have an important impact on the data collection and data protection practices within the organisations – which I will further elaborate in the next sections of this chapter. In general, the organisational roles described here, the surveillance worker, the surveilled worker and the data protection officer, are closely related to each other. Specifically, the first two can be incorporated by the same person as controlling of employees can quickly evolve into a surveillance practice. Thus having a data protection officer as a lobbyist for personal data – of the employees as well as of the customers and data subjects – can help in mitigating data analysis for controlling and manipulative reasons of organisations.

7.2.3. Expert knowledge in data protection

The experts interviewed served as a source for their special-knowledge on the social circumstances which are researched here and as a source of professional knowledge (Gläser & Laudel 2009, p.12; Meuser & Nagel 2009, p.37f.) – mainly on the organisational structures, roles, tasks and goals in data collection and data protection practices and how these are negotiated and contested in the broad field of operation and influenced by the many internal and external pressures. But also the specific function of expert knowledge within the organisation should not be excluded here. This sub-chapter will show how the gaining and management of expert knowledge in organisations can have a large impact on how data protection is dealt with by the people involved.

In most of the companies and administrative bodies the importance of the professional knowledge is recognised but is nonetheless dealt with differently. Mainly in companies in which data protection is considered as a highly significant task – and they also recognise the business aspect of successful data protection (see sub-chapter 7.2.4 p.110) – the data protection officers seemed to be selected accordingly. Previous relevant affiliations of the employees appear to be important for the task, some having worked in data protection authorities, others having a strong legal background with a focus on data protection rights and some even a combination of data protection rights and information security.

Professional knowledge is often a combination of gained knowledge through basic educational measures – for many of the data protection officers in terms of legal studies – and further educational measures, like additional seminars, conferences and workshops in order to keep up-to-date regarding changes in the field of operation or to further improve already existing knowledge. Furthermore, experience plays an important role in shaping the knowledge required. This entails know-how gained in previously held positions and jobs inside and outside of the current organisation, as well as know-how gained in the present position as data protection officer.

Also networks of experts can play an important role in the shaping of expert knowledge. Particularly amongst the interviewees which held the position of data protection officers, an exchange with other experts in similar positions appears to be essential on a regular basis. While some seem to rely on a more national level of expert networks here, others also orientate themselves by international networks like Germany, where the role of the data protection officer is already more developed due to having a longer history and culture.

With the upcoming changes of the new General Data Protection Regulation, particularly the data protection officers who engage in regular further training measures and who are involved in strong networks of experts feel confident about being able to adapt the changes easily as they have followed the development of the GDPR thoroughly to anticipate upcoming changes at an early stage. And also since the publication of the final text of the GDPR, some businesses and bodies have initiated projects to analyse the upcoming changes and assess what needs to be done within the organisation. The respondents are confident about the changes as they already have high data protection standards in place – as for example the position of the data protection officer. Others, while still being confident on being already well prepared, still prefer to wait for the national adaption of the regulation, even if the regulation needs to be adopted directly into the Austrian data protection legislation:

> “We have followed the development for years. And ahh also all the different negotiation results, which, how should I put it, have changed a lot during the years. And now we are, it depends on the precise implementation, although the General Data Protection Regulation will have immediate applicability, it will still depend on the praxis, how the Austrian data protection legislation will be adapted. For us it is of course also interesting if the public Data Protection Registry will still be required? And if we can still use it? Will it be voluntary? I mean we are prepared anyway, even if it won’t be needed anymore. We are now, with what we have, sure that we can fulfil the requirements.” [Interview 6; Position: 32-32]

One effect the GDPR has already had from the beginning is that due to the high rate of penalties which are to be expected in case of non-compliance with the legal requirements, the data protection officers internally have a strong leverage for addressing data protection considerations. Even for organisations where data protection has a lower priority, the change of the maximum fine has brought forth a situation where data protection is better acknowledged.

Besides the adaption of new expert knowledge and experience, as here for example with the GDPR, I will also briefly present the management and transfer of existing knowledge within the organisations. Part of this knowledge management is the training of employees, as I have already shown in the previous chapter. Especially for the surveillance workers, these – often mandatory – trainings are crucial in transmitting data protection knowledge and are also perceived as such by the data protection officers. While these trainings are generally led by external professionals, most of the DPOs are at least involved in the shaping of the content of the training, thus deciding what knowledge needs to be included and transferred to the surveillance worker. In some cases, the trainings are mainly implemented to raise awareness amongst the employees on the data protection practices – often through games or e-learning methods. In other cases, organisations provide educational measures with the aim of fully transmitting the professional knowledge. Or, as one respondent put it, they do not only train their employees in the basic data protection regulations, but even to the point where theoretically the employee could replace him as a data protection officer, as he also has not more training. Especially such training measures often, but not solely aim at a higher management level widely accepted by the surveillance workers.

We thus see here that in the examples presented above, the importance of a successful knowledge management or of an institutionalised knowledge transfer is recognised by the respondents. Being able to shape the practices of the employees by contributing to their professional knowledge and expertise has the advantage for the organisation of deciding on how the organisational role of the employee should look like. As I have already shown before, the role of the employee within the company is influenced by his self-definition of this role and his identification with it. But not solely. Abrahams and Büschges (2009, p.162f.) describe how equally the organisation itself, represented by the upper management and decision makers, contributes to the organisational roles and in further consequence to the behaviour of the role-bearer. In the case of implementing data protection knowledge into the roles of the organisation, the data protection officers seem to be trusted entirely by their respective upper managements.

While the interviews showed some best practice cases in the way knowledge can be managed and transferred, there were also some cases where no such practices seemed to be in place. In one organisation, this could already be related to the lack of general expertise in regard to data protection knowledge, as the relevance has only shortly been discovered as a result of the upcoming GDPR. In another case however, while an apparently good source of knowledge is available in the form of an employee with a personal interest related to data protection, this is not systematically used by the organisation. Although the employee serves as an initial contact point for data protection questions, there seem to be no mechanisms of institutionalising this knowledge. While this currently serves as an informal source of knowledge, it can in further consequence lead to a situation where this knowledge is lost due to having no systematic institutionalisation of the knowledge in place and thus can become a missed opportunity for the business.

As a final point to address in this sub-chapter, specific expert knowledge on the technological part of data collection and protection was ambivalently dealt with by the respondents. Here, the data protection officers who have a technical background are in an advantageous position. And while none of the respondents were technologically illiterate, some mentioned that they often simply need to rely on the IT-department in the technical matters of the data collection, processing and protection, due to the complexity of the technology behind the operations.

This is insofar of importance as an incomprehensive technology – here in the form of a data processing technology – not only remains obscure for the data subject who is often not aware of the technology itself. But the processes and the functioning involved in the technology also remain obscure for the "lobbyist of personal data" – the DPO. Going back to Bruno Latour's black-box, which I have discussed previously (Chapter 0, p.44f.; Latour 1999, p.304), a dismantling of the technology as an actant in the connected network of relations, by the data subject or its vindicator is increasingly difficult and consequently also exacerbates a dismantling of the network itself. In these cases the DPOs and the respondents with a superior knowledge in regard to the technical operations are those who have the advantage of being able to deconstruct the black-boxed technology at least partially – of which also the organisation can benefit, due to having a more holistic and well-functioning network of behavioural and procedural data collection and protection in place.

7.2.4. The relevance of data protection

The relevance or importance of data protection within the organisation in general has shown some close connection with how data protection is managed in the businesses and administrative bodies. Like I already mentioned in the previous sub-chapter, with the forthcoming GDPR and the increase in fines for non-compliance with data protection regulations, an acknowledgement of the importance of data protection has been reported in all the interviews. However, the interviews have also shown that in some organisations a high standard of data protection is incorporated up to the board of the organisation.

Thus, while in some companies data protection is implemented as a simple adaption of legal regulations, others have applied higher standards and thus more than the required minimum. This appears to be translating into how data protection is accepted throughout the organisation. High standards can of course already be a result of legal requirements: in some sectors like financing or telecommunication, sector-specific regulations further shape how personal data can or cannot be used, considering for example the bank secrecy in Austria. But also the type of data can be decisive on higher data protection criteria – within the public administrative body, due to also having access to sensitive information, the importance of protecting such data is recognised. Similarly, the type of organisation and their field of operation also have an influence on this. Companies with personal data as their core business, for example banks or telecommunication companies, have a higher awareness of data security and data protection in general. A quote by the data protection officer of the telecommunication company nicely illustrates this:

> "Data protection is included in our DNA. It is especially this that is of importance for a telecommunication company." [Interview 2; Position: 5-5]

Another factor for increased data protection and privacy is business. This can be expressed in a twofold way. On the one hand, having a high data protection standard and being able to promote this can serve as a publicity. A respondent explained this by referring to how nowadays people not only want to know where their 'Schnitzel' is from, but also where their personal data will be stored and how it will be processed. Due to an increased awareness in regard to data collection practices and the knowledge that some countries have a more secure approach to data, this can be used as a business model. Specifically in the telecommunication company I interviewed, the high standards of data protection were tried to be promoted and seen as a way of gaining an advantage over the competitors. On the other hand, business through data protection was seen by a corporation in the sense that each company within the corporation hermetically sealed off their data collections. Not sharing personal data, even within the corporation, was also perceived as creating an advantage over the internal competitors.

Data protection however also obtains recognition due to it being of importance for decisive members of the board. Shaping the orientation of the organisation in such a way highly influences how data collection and data collection practices are incorporated amongst the employees. Recurring the model introduced by Abrahams and Büschges (2009, p.162f.), the roles of the employees within the organisation are shaped by a variety of effects and subsequently impact on the behaviour of their roles. Beside the self-definition of the role-bearer, as was described in Chapter 7.2.2 (p.97f.), it is also the organisation itself which determines how the goals and ideas will be executed by its employees. And while these can be influenced by educational measures and training (Chapter 7.2.3 p.106f.), they are also influenced by the general orientation – defined by decision makers in the organisation.

In further consequence this is also observable in those companies where data protection is not included in the organisational orientation. Not having data protection as a priority but rather as a legal criterion is also adopted as such into the organisational structures and the 'mentality' of the employees, making it increasingly difficult to actually raise awareness regarding data protection issues.

7.2.5. Pressure groups and the ‘others’ as surveillance workers

Having covered the self-identification character of organisational role bearers as well as the organisation itself in shaping ‘data protective behaviour’, I will finally demonstrate the environmental effects on the organisational role and its behaviour. During the interviews, a range of environmental influences or pressure groups was addressed by the respondents. While I have already mentioned some of these pressure groups in the previous sections, I will address them here individually with the intention of providing a clear analysis of the causal effects on data protective behaviour.

Starting with the legal and governmental environment, it is clear that the legal frameworks have a big influence on how data collection and data protection is handled within the organisations. With data protection heavily relying on a legal framework, as I have also presented in Chapter 6 (p.73ff.), it is often the prime driving force behind the organisational practices. Especially if strictly enforced or in combination with severe penalties, as is to be expected with the new GDPR, the compliance with data protection regulations is seen as an important point within the companies and has also increased the awareness on data protection issues – even if it is a rather fear-related awareness. The same relates to the data protection authorities. The possibility of (ombudsman-)proceedings and complaints by data subjects which can be taken up by the DPAs require that organisations are aware of their data processing practices.

New regulations can be encountered with scepticism by some of the respondents, due to it not being clear how it will be implemented precisely. It is a certain legal uncertainty, which also relates to a lack of specific knowledge and expertise that makes it difficult for some respondents to anticipate the upcoming changes. Especially in relation to new requirements like the data portability, the precise legal provisions are unclear or the actual technical implementation is not assessable. This creates an ambivalent situation – one where some of the data protection officers prefer to wait for more precise guidelines while others have mentioned that some bigger changes are required, for which the two years’ implementation time is extremely short.

In relation to other organisations, especially in Austria where no data protection officer is appointed, some of the respondents hope that the new regulation will nonetheless create an improvement in data protective behaviour which might even induce a change of the cultural understanding of data protection. The Austrian praxis is particularly compared with Germany, which is seen as one of the countries with the highest data protection standards. As in Germany the data protection officer is legally required in certain organisations, the data protective behaviour is considered to be higher and more professionalised, being a state that in Austria also should be achieved:

> "(…) I am already since 18 years a member of a data protection workgroup of a sector in Germany, which discusses many data protection matters. And there has been a massive cultural change within the last 15 years (…) These are all people who really deal with the topic of data protection – the one more and the other less – but who are really into the topic. And that's something I hope for in Austria as well. The German culture specifically regarding the normative implementation is different as the Austrian. But I hope that this will change, because it is also from a legal policy point of view not really satisfying if we have rigorous norms but no one who is interested in implementing them." [Interview 8; Position: 37-37]

It is thus a cultural divergence in the understanding of data protection laws that is influencing the data protective behaviour in organisations in general. And although comparisons are also made with laxer data protection practices, e.g. in the UK, the Arabic countries or in China, it appears as if the German practice is the one that – from a data protection officer point of view – should serve as a model.

The interviewees however are also aware of the limitations of the legal framework. If legal requirements are not enforced, then even the most severe penalties do not help in shaping the desired behaviour. The typical examples brought forth here by the respondents – and which indeed show the problematic nature of the legislative processes – are practices by companies like Facebook or Google, which often appear to be above the law and are not really contestable, particularly not by ordinary citizens and data subjects. But also in general, already some of the data protection officers are aware of the difficulty for data subjects to effectively enforce their rights. As the data protection law can mostly only be enforced by data subjects through a civil court, the threshold of really going so far can be high, specifically for lay citizens. Although legal assistance can often be utilised by citizens, the effort for imposing their legal rights is high – lengthy procedures, the risk of costs and all of this for something 'as minor' as data protection related issues. As one of the respondents said, the barriers for legal protection are extremely high for something as trivial as having your name and e-mail address deleted out of a data-base.

As such, the aggravation of the data protection law and the increased rights for the data subjects by the new GDPR are also partly confronted with scepticism, since it is not clear if the right levers have been tightened. If the data subjects cannot be guaranteed to really being able to exercise their data protection rights and non-compliance by organisations will seldom be prosecuted, the increased penalties and regulations will mainly hurt the smaller and medium sized organisations, which do not have the resources of adapting to the changes so easily and will struggle with the new requirements.

The limitations of the legal framework can also be used advantageously for the organisations. This becomes apparent in a trade-off process, in which the effort required for a full compliance with the regulations is weighed against the possible limitations. Particularly in terms of access rights for data subjects, this becomes visible for some organisations. As a result of the low number of subject access requests that are received but the time which is required for responding adequately to each request, the incentive of facilitating the execution of data protection rights for the data subjects appears to be low as well as the incentive of enhancing the process of responding and disclosing the personal data. This can lead to a situation where for the data subject his or her data protection rights are hindered and he or she becomes frustrated due to the difficulties encountered when trying to execute his or her rights – if the data subject is aware of the rights at all. For the surveillance worker or the data protection officer, it is frustrating as the requests which are obtained risk being incomplete or written in a confusing manner, requiring to check back with the data subject and going to lengthy processes of searching for the available data.

Besides the legal and governmental environment, the <u>societal</u> environment including the <u>data subject</u> also has a big contribution to data protective behaviour in companies and administrative bodies. Pressure by the societal environment on data protective behaviour is often linked with the legal rights they have – requesting access to data, or erasure of personal data being one of them. Although in day-to-day situations, the interaction between organisations and the data subject in regard to data protection issues are limited, it is specifically in exceptional situations where the pressure by individuals is increased. This can be based on events which relate to the organisation in question, e.g. a data breach, or based on more general events relating to data protection. Some data protection officers for example reported an increase in awareness in the general public after Edward Snowden released the NSA-files and citizens became conscious about the extent of data collection practices. It is also suspected that citizens utilize their data protection rights when having another issue with the organisation – for example when being unsatisfied with their contract – and want in that case another instrument for putting pressure on the organisation. In other cases, more trivial events seem to trigger an action by the data subjects. Lectures in legal studies covering data protection rights can be one of them, after which an increase of subject access requests can be observed.

It should however also be stressed that the data protection officers included here in the empirical research often also valued the input of ‘lay’ citizens – on the one hand as it also gives input on the practices of the organisation and the possibility of enhancing certain mechanisms and data protection measures. On the other hand, it also shows a certain degree of awareness amongst the society, even if many of the DPOs criticised that in this matter still a lot of work needs to be done, as not only the organisations and the data protection officers in their role as representatives of the data subjects can be solely responsible for the data protection of the citizens, but also the citizens themselves. Although they – as lobbyist for the data protection of the citizens – can contribute to this, also through their own practices within the organisation and the contact with data subjects, an informing is necessary:

> “I mean, I am simply for public awareness. But I am for an honest awareness raising. And I also make clear, I am often on events, what I like, where I, not in front of an expert audience but lay listeners, where I simply explain in thirty, thirty-five minutes, everyone tell them what personal data is and what do we as organisation and also other organisations do with this data. Very easy. A bank. What does a bank do with personal data? What can they do with it and what do they really do. Same for the administrative register of residents. Everything we have in Austria. This is better than if they are only told to complain, they get suggested they should complain about it, but put into relation it is only a very small amount where they really should complain about.” [Interview 7; Position: 57-57]

Citizens need to be made aware of the practices also to be able to distinguish between ‘good’ practices and ‘bad’ practices, thus being able to distinguish between ‘general’ surveillance – where they nonetheless can urge for data protective behaviour – and ‘intrusive’ or ‘controlling’ surveillance – where it is necessary to urge data protective behaviour. This is also seen as important, because in relation to the ‘others’ as surveillance workers, thus other organisations which often have more coercive surveillance practices due to having a monopoly or acting globally, it is often difficult for ‘law-abiding’ organisations to establish a data protective behaviour amongst their employees. Gaining acceptance of why they should comply with data protection regulations while other, larger organisations do not, is in these cases a challenge for the data protection officers. Pressure through the society and citizens on the ‘others’ as surveillance workers would in this regard also help in increasing the data protective behaviour in organisations in general.

In close relation to the pressure of the society is the pressure which is exercised by the media. As they have a large contribution to how the public opinion is shaped, they also add to the environmental shaping of the data protective behaviour in organisations – often in a twofold way. First through increasing the relevance of data protection in terms of 'business' – reports on personal data related incidents are bad publicity for every organisation no matter whether they are private or public. This translates into an increased awareness of the requirements in daily operations as well as in a professional communication in cases of incidents. As I have shown in the roles and tasks description of the data protection officers, the external communication is an important aspect and is also directed to the media, especially as a step in crisis management.

Second, it is also the possibility of triggering the society in data protection concerns through media reports, which is also generally acknowledged and welcomed by the respondents. Similar with the contribution of other data protection experts. Certain known experts, like Max Schrems or Hans Zeger with their efforts in contributing to a data protective behaviour in organisations or in general and their – sometimes too little – coverage in the media, are seen as a good sign in increasing the consciousness of the public in these matters.

However, also the media is not perceived without critique. Similar to the critique of general awareness raising in the society, also for the media the coverage is perceived as skewed by some data protection officers. When practices of global internet corporations are put on the same level as ordinary organisations, the media coverage is experienced as misleading the public and not contributing to providing a differentiated picture of data collection and data protection practices in organisations:

> "Even if it is always shown differently. We have to live with it. We are the evil corporation. (laughs) It's like this. The Data leech with its transparent customers, the 'Transparent Man'. Obviously. What in reality happens with his data and how little we do with it and analyse it doesn't see anyone and doesn't know anyone." [Interview 7; Position: 40-40]

Some of the respondents thus hope that not only the public would benefit from a more comprehensive representation of data collections and protection experiences, but also how data protection is done in organisations as it would ease the enforcement of data protective behaviour amongst employees and colleagues on the one hand and the workload in relation to 'uninformed' data subjects on the other hand.

A final environmental influence on data protective behaviour is the technology involved. The topic of the technological involvement has already been raised a few times in my empirical analysis. It nonetheless deserves an own analytical paragraph as technology has often been brought up as having the potential of opposing the legal framework of data protection in certain circumstances. The inferences technology has with the other environmental factors are experienced of having an important effect on data protective behaviour not only in organisations but also in general. Some of the respondents see structural faults as the basis of the discrepancy between data protection laws and technology, in the sense that the legal frameworks cannot be adapted in the same pace as the technology is developed. The development of the GDPR is brought forth as a good example here: the old data protection Directive which was introduced in 1995 is based on the technological status-quo of the early 90s. Although it has been tried to adapt the legal framework to the technology of today, the principle structures of the Directive have been maintained. However, the distinction between the data controller and the data processor are not viable anymore in times of cloud-computing. The same goes with the right of erasure of personal data. Even if the Supreme Court rules that personal data *must* be erased in its totality within data processing organisations, it is technically inconvertible as this would also entail deleting the data from every backup which has been created.

A similar structural fault can be observed in the telecommunications act in relation to data protection, where the classification of three forms of data – core data; call detail records; content data – is a legal construct which dates back to times with solely landline telephone and has not been adapted to the use of smartphones or the internet. The globalism of data communication and data transfer has an equally important impact. Although the safe-harbour agreement has been squashed, it is experienced as impossible for data not to be transferred to the USA. These are only some of the examples mentioned by the data protection officers and surveillance workers where they experience a divergence of data protection regulations with the technological possibilities and thus an increasing complication of their work and the data protective behaviour in their organisations.

This heavily challenges the supposed technology neutrality of laws which assumes a “statutory longevity and equal treatment of old and new technologies” by laws and thus being broadly adoptable – which is also the current understanding of many scholars and legislators (Greenberg 2016, p.1495). The concept of technology neutrality requires a certain openness and anticipatory character, allowing that legal provisions are applicable to many technologies no matter of their novelty and thus not requiring a new regulation for every new technology or change in technology. As such also the data protection regulations are supposedly technology neutral.

While this general concept seems plausible, the above mentioned examples however show the structural flaws and non-applicability of the concept in several cases. As Greenberg (ibid., p.1562) also remarks:

> technology neutrality "leads to rules that are over-inclusive and speak poorly to unforeseen technologies. (…) It also, in turn, results in inconsistent treatment of similar technologies and increases uncertainty about whether and how the law will be or should be applied. And that undermines neutrality's goals of promoting statutory longevity and adapting the law to new technologies."

The general consideration of data protection as a fundamental right is seen as important by the respondents, as well as the possibilities for data subjects to execute their rights – information; rectification; erasure – which founds on the basis of knowing what personal data is held by the organisation through guaranteeing access to data. However, the execution of these laws and rights is not always possible and sometimes even impossible due to the technological developments and the globalism of the phenomenon.

It should nonetheless be mentioned that not in all of the organisations this was perceived with such a vehemence. Although the difficulties with developments and new technologies were recognised, more pragmatic approaches to this problem were that it is not considered to be a structural flaw in the legal provisions, but rather in the enforcement of the existing provisions. As such, technological development does not need to be specifically followed by new legal regulations, but rather investigation methods and possibilities need to be adapted constantly for being able to enforce the law. It nonetheless shows the influence technology has on the data protective behaviour in organisations – and in this case even on the general public.

Summarising, the interviews have nicely shown the entanglement of different influences on data protective behaviour in organisations and also how it is tried to be dealt with. The model of Abraham & Büschges (2009, p.163f.) for analysing organisations has also proven useful here, enabling to build the links between the different structures in the organisation, the roles included in the data collection and data protection practices as well as the environmental influences. While the envisioned comparative analysis of different organisations could not be achieved, also as a result of a lack of resources as well as a lack of feedback from potential interview partners, the empirical data has proven useful in establishing an extensive mapping of data collection and protection in organisations – and thus can nonetheless contribute to the field of study.

8. The contested state of Data Protection

The results presented above leave us with the important question of what the practices concerning data collections and subsequently data protection in organisations mean for the people impacted by data collection and processing practices – the data subjects and citizens. In order to discuss the implications of data protective behaviour, we first need to go back one step to the legal framework. The legal requirements for data protection are predetermined and set 'rigid' norms which leave only little room for interpretation by individuals. The persons involved in the rule-making process have an important definatory power as they can set the requirements of what is allowed and what is not (Menzel & Wehrheim 2010, p.514). As such, rule-making is a highly contested procedure in which of course many different interest groups want to have access to the definatory power. Also the new General Data Protection Regulation has thus seen the involvement of many stakeholders lobbying for their interests to be respected in the GDPR – be it amongst others by large internet corporations like Google and Microsoft who therefore even set up the think-tank European Privacy Association (Hirst 2014) in cooperation with the American Chamber of Commerce (Katzemich 2013), by the European Banking Federation (Peters 2013), or by medical research communities like the European Alliance for Personalised Medicine (EAPM) (McGuigan 2013) – and thus trying to define the boundaries of data protection.

The rule-making and the included definatory power is what MacNaughton-Smith (1975, p.197ff.) calls the "first code". In contrast to the official/formal norms of the first code, MacNaughton-Smith introduces the "second code", which represents the application and interpretation of the formal rules by individuals or organisations as well as the relating unofficial and informal rules. Particularly in organisations, the second code is often predominant in which the actions of the actors involved are largely shaped by the informal rules which need to be practical for everyday purposes (Fuchs & Kreissl 2011, p.17f.). It is this contrast of the first and the second code which forms a large part of the evaluation of the empirical research done here. The expert interviews have shown an interesting discrepancy in the different interpretations of the data protection regulations and the setting of informal rules amongst the organisations, resulting in a shaping of diverse data protective behaviours in organisations.

The results have shown how the first code – the data protection regulations – are implemented within the organisations, setting out specific rules and forming the organisational roles of the surveillance worker and the data protection officer who negotiate the expected behaviour within the company. With the introduction of the data protection officer in some companies, we see that there is the aim of keeping the second code as closely as possible to the first code, which can be observed through the high standards of data protective behaviour expected within the organisations. Specifically through the knowledge management and the promotion of an institutionalised expert knowledge, the formal and informal rules are closely tied in some organisations. In other organisations as well as on lower operational levels however, we also see a high amount of unofficial rules which can differ widely from the official data protection regulations of the first code. When personal data is managed in Excel spreadsheets or passed around more freely within the organisation or institution, data protection norms are – intentionally or unintentionally – partly suspended and the second code is predominant. This is often done unintentionally or without bad faith but rather on the background of being able to perform and react flexibly and according to the required purpose in the day-to-day organisational operations – something the ‘rigid’ legal norms of the first code are often not capable of (ibid., p.18).

The difference between the first and the second code, of the formal and informal rules, has a big influence on the way data protection can be enforced by the data subjects. As shown several times in the course of my thesis, the possibilities of interference by data subjects are limited. Already based on the first code, the data protection regulations, data subjects often solely have the right of access to data and from there on the right of rectification and erasure of data.

A large discrepancy between the first code and the second code, or a high amount of informal and unofficial rules regarding data collection, data processing and data protection practices create an even more difficult situation for data subjects in managing their personal data. This becomes mostly apparent in organisations where subject access requests require a lot of effort and are partly considered as a nuisance – and consume a lot of time which could be spent for other tasks. As I have shown, while the practice of responding to subject access requests could be enhanced, there seems to be a “second code” of dealing with these requests which has consolidated in the organisation. For the data subject this creates a situation where the practices within the organisations are not transparent as they are not part of the official rules – starting with missing information on what to include in subject access requests to possible incomplete answers on the requests as was shown by L’Hoiry and Norris (2014).

This furthermore relates to another problem for the data subjects which is often discussed in similar researches and which also seems to show itself in the present research. The access to personal data is complicated by the fact that many data subjects do not know and cannot know what kind of personal data is exactly processed by the company or administrative body, nor where it is exactly located. But what the empirical research furthermore shows here is that the "unknowables" of personal data disclosures for the data subjects (ibid., p.34) are often even intensified by the "unknowables" for the surveillance worker and the data protection officer. As personal data in large organisations is often collected and processed in multiple databases, which are seldom connected, the consolidation of all the personal data is a difficult task for surveillance workers and mostly also not desired from a DPO point of view. From a general data protection position, it is equally pleasant if personal data collected in large corporations or administrative bodies is not merged into one large database and analysed in such an intrusive way. However for the data subjects, this entails that their personal data is highly dispersed – on the one hand between multiple organisations and on the other hand also within the organisation.

This implicates an impossibility for the data subject to keep track of his or her personal data. If even for surveillance workers within some organisations, it is almost impossible to keep track of all the personal data they process, due to the overwhelming, but highly dispersed amount of data available to them, how should individuals be able to trace their personal data? Intensified by the second code of data protection in organisations it becomes apparent that in several instances the protection of his or her personal data is a highly complicated task for the data subjects.

The practices by some of the organisations included in my research here can be highlighted as really best practice cases, some of which showed a high interest in providing a good service for the data subjects and taking care of the personal data provided by the customers, users or citizens – also knowing about the value of the data and risks related to an improper use. However, the research has also shown some important lacks in data protective behaviour, most prominently by the non-responses of several organisations on my interview requests. If I as a researcher am confronted with opacity in identifying the interview partner in several instances, or by silence upon inquiring, it can be expected that ordinary lay-citizens are confronted with the same (non-)responses or even have more difficulties in identifying contact persons within the organisations.

I have already speculated a little further above on the reasons for this behaviour, the possibility of it being the result of "uninformed experts" or the missing of data protection experts within the organisation being one of them. As also some of the DPOs speculated, many organisations often process a significant amount of personal data without being fully aware of the legal norms of these operations. In these cases, it is largely the second code which governs the data protective behaviour as the first code is largely unknown to the surveillance workers and data controllers. For a lay citizen and even for an informed citizen this creates a situation in which the enforcement of his or her rights is almost impossible, especially if in combination also the enforcement through other instances – for example through legal courts or the data protection agency – is hampered due to high administrative barriers or possible legal costs.

A deliberate non-response of the data controller can also be assumed, as also the experts which responded to the interviews were often fully aware of the legal limitations and the difficulties in relation to enforcing the current data protection rights by citizens. In this case, it is also the second code which is predominant regarding the data protective behaviour. In comparison with the "uninformed experts" however, the organisations and the surveillance worker are fully aware of the existence of the first code but make a deliberate decision of relying on the second code. And while the outcome is the same – the citizen not being able to enforce his or her rights – the implications are different. In the latter case one can assume that the data controller is a fully informed expert and thus can probably better assess the limitations of his actions, in this case until what point can the data subject be ignored, how little information on the data processing can be disclosed to the data subject, etc. The deliberate ignoring is a conscious decision by the data controller to remain as obscure as possible, which in further consequence fuels the speculation that there are indeed data processing operations that require to be hidden and that data protective behaviour is rather limited within the organisation.

The empirical results thus show different types of organisational behaviour regarding data protection. While the above two cases show instances where there is a lack of data protective behaviour and a large discrepancy between the first and the second code, the best practice cases show instances where data protective behaviour is actively promoted and thus also the first and the second code are closely related to each other.

However, the results reveal another type – in the situations where the data processing and protection as well as the technology behind it is not entirely understandable for the surveillance worker, due to it largely being black-boxed within the technology. Or in the situations where the importance of data protection relies on the simple adaption of the legal requirements. In these cases, a data protective behaviour is present without being aggressively promoted as it consists in many instances of a simple implementation of the first code while being aware that digression into the second code seldom results in actual sanctions. And while the respondents are conscious of the upcoming change of the first code and most importantly the increase of sanctions as a result of non-compliance, this does not automatically induce a change of the practical routines of the day-to-day operations, thus of the second code. Although it is to be expected that the second code needs to be adapted, the extent of adaption will for example also depend on the enforcement of the new first code.

Which also leads me to my last point in this chapter. The situation of data protection which is simply considered as the adaption of the legal requirements is a result of personal data being regarded as a by-product of day-to-day operations. While in some organisations the monetarised value of personal data and its possibility of economic exploitation is perfectly known and also practiced within the legal boundaries – at least as far as the respondents disclosed – in other organisations the availability of personal data more often than not appears to be a necessary nuisance. The collection of personal data is necessary for the organisational operations, be it internal personal data or external personal data, while a commodification of the personal data is not envisioned. However, with the collection of personal data, legal norms are a concomitant which require extra attention and often also produce more work. Personal data is a necessary nuisance – as opposed to personal data being a commodity for some organisations, who specifically aim at gaining profit by exploiting data. In the above mentioned case the collection of personal data is necessary and can also lead to economic gains/growth, however it is not based on the exploitation of the personal data. Data is collected and processed for administrative purposes and helps in providing services, compared to cases where data is used and analysed for controlling customers and citizens. And it can be assumed that also in the case of the "uninformed experts", where no response for interviews was obtained due to the complexity of the topic, the collection of personal data is rather an operational by-product than a commodity. Nonetheless this leaves a situation in which exercising personal rights, such as the right of access to data, is hampered by organisations and the surveillance workers involved. Not on the basis of bad-will or secrecy but on the basis of not wanting to invest even more time in the by-product of day-to-day operations – called personal data.

9. Conclusions

Thus, who is contesting my personal data?

Personal data is a highly contested good – as I have already stated in the introduction of my thesis. This phrase is also expedient for the conclusion of my thesis, although I would like to extend my initial thought here. Over the last hundred pages, multiple actors, disciplines and fields of operations have been introduced, which all try to access personal data in some way or another. For example, many of the studies which I brought forth in the state of the art show the effects of personal data collection and analysis of citizens, consumers and data subjects alike, which aim at exerting a certain form of control on them and thus have a desire of gaining access to such data. Comparable results can also be drawn from the broad theoretical framework I have presented. Especially in the field of surveillance studies, as well as the more legal/privacy studies, the connection between personal data and the exertion of control through surveillant means show a contest for personal data on many levels.

In some way however, also the scholars and researchers in these (and other similar) disciplines are involved in this contest for personal data – keeping in mind the different positions on how surveillance and data collections should be perceived. Defining the settings of surveillance and the control of personal data collections induces a participation in the challenge for personal data – even though from this point of view more onto a protection of data and personal rights than an exploitation of such data. My thesis can be included into this area as well.

From the empirical research side, my thesis can also shine some light on the competition for personal data from an organisational point of view – the surveillance workers, the data protection officers and the whole organisational environment shaping data protective behaviour. It has broadened the analytical focus, shifting away from a narrower distinction between the watchers and the watched, between those exerting control and those who are being controlled, as it is often used in the respective literature. Instead, through depicting the shaping of data protective behaviour in organisations, I have been able to demonstrate how organisations on the one hand actively partake in the contest for personal data, but on the other hand also contribute to a protection of personal data and provide more or less solid tools for the data subjects, consumers and citizens to make sure they can also actively influence the usage of their data.

Like some of the respondents aimed at, the protection of personal data cannot be unidirectional in the sense that solely those involved in the data collection are responsible for the data protection, but it should rather be a bidirectional involvement. Putting this in line with the previously introduced theoretical framework of surveillance studies, we see that in some instances organisations expect from data subjects to react to surveillance and data collection practices. On the one hand related to big corporations like Facebook, Google and co., towards which a data minimisation approach should be aimed, as well as an active challenge for an increase in transparency about the usage of data is required. On the other hand, also related to their own organisations. Although not all expect an active challenge in regard to the day-to-day operations, most are aware of the risks linked to a data protective behaviour, a second code, which largely conflicts with the first code of data protection regulations – which can generally be challenged by the public. This creates the situation described in the previous chapter, where data protective behaviour is present amongst the surveillance workers and other personnel involved but in which the deviation between the practical and the required behaviour is carefully assessed in order to minimise the effort of personal data as an operational by-product.

What do surveillance workers do?

Which leads us to the next conclusive question for my thesis – the discrepancy between the first and the second code in regard to data protection regulations raises the question, which was again already previously asked in my thesis: what do the surveillance workers effectively do when they 'work in surveillance'? As the interviews had a strong focus on data protection and specific information on data collection was scarce, they might not have entirely revealed the daily routines and operations of surveillance workers. However, the interviews have contributed to showing how data protective behaviour is expected from the surveillance workers and how this behaviour is implemented. In further consequence this demonstrates how the organisational setting, the environment of the organisation, the self-definition of the surveillance worker and his or her tasks, as well as the technological setting define the role behaviour of the surveillance worker, which leans on the model of organisational roles described by Abrahams and Büschges (2009, p.163f.).

Recurring to Smith's conclusion (2012, p,114), who urged for an increase of research on surveillance which revolves around "how (…) organisational positioning influence surveillance worker decision making; the intricate and multi-dimensional social relations in which surveillance workers are situated; the social realities that surveillance workers produce, consume and inhabit; and the embodied consequences associated with human-technology interactivity in general", we can see how these influences are equally reflected in the empirical research here. While the general discussion on surveillance often revolves around abstract and broad topics, often around whether or not "control is *the* defining attribute" of surveillance (Marx 2011, p.90), instead of focussing on the surveillance workers, my thesis is able to demonstrate how surveillance *practically* functions and reconstructs the actual *performing* attributes of surveillance.

Furthermore, with special attention put on the human-technology interaction as a constitutive part of determining (non-)data protective behaviour, the authoritative (Zhang et al. 2016, p.74f.) or black-boxed technology (Latour 1999, p.304) demonstrates how the technology behind surveillance operations can enforce a certain behaviour without disclosing the necessity of such behaviour and in further instance leading to a situation in which also for the surveillance workers it becomes more and more opaque in regard to what operation requires what kind of behaviour.

All in all, my thesis provides further insight into the operations of surveillance workers as practically shaping surveillance operations and personal data collections. Which is why in this case I can only once again relate to Smith's conclusion and equally urge for the further empirical research on the daily operations of surveillance workers, as it is clear that their influence on the practical surveillance cannot be neglected by surveillance studies.

DPOs as the Holy Grail?

Finally, a small conclusion on the role of the data protection officers should be included here – also in foresight of the upcoming General Data Protection Regulation. The new GDPR provides for a more important role for DPOs within organisations, focussing on the enforcement of data protection regulations. In this regard, many of the organisations I included in my research have an advantage as they already have DPOs, in some cases even with a rather high standing and influence within the organisation. Although my empirical results do not allow for any generalising conclusions, the results show that the organisations which have a DPO installed appear to have a clearer understanding of data protection regulations and as such can also better introduce, in some cases even enforce a data protective behaviour within the organisation and amongst the personnel involved in data collections and data processes. However, the results also demonstrate that it does not solely rely on the availability of a data protection officer and instead many other factors have a big influence – from the organisational volition (at all levels), through the management with relevant knowledge, to the external factors such as media, society and technology.

10. Sources

Abraham, Martin and Günter Büschges. 2009. *Einführung in die Organisationssoziologie.* 4. Auflage. Wiesbaden: VS Verlag für Sozialwissenschaften / GWV Fachverlage GmbH.

Al-Khouri, Ali M. 2012. Data Ownership: Who Owns 'My Data'? *International Journal of Management & Information Technology* Vol.2 1:1-8.

Allmer, Thomas. 2011. Critical Surveillance Studies in the Information Society. *tripleC* 9 (2):566-592.

Allmer, Thomas. 2012a. *Towards a Critical Theory of Surveillance in Informational Capitalism.* Frankfurt am Main: Peter Lang.

Allmer, Thomas. 2012b. Critical Internet Surveillance Studies and Economic Surveillance. In: *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*. Ed.: Christian Fuchs, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval. 124-143. New York: Routledge.

Andrejevic, Mark. 2012. Ubiquitous surveillance. In *Routledge Handbook of Surveillance Studies*. Ed.: Kirstie Ball, Kevin Haggerty and David Lyon. 91-98. London and New York: Routledge.

Article 29 Working Party. 2011. *Letter from the Article 29 Working Party addressed to Vice-President Reding regarding the Article 29 WP's reaction to the Commission Communication "A comprehensive approach to personal data protection in the EU"*. 14.01.2011.

Article 29 Data Protection Working Party. 2016. Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision. 16/EN WP 238.

Austrian Parliament. 1978. *Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz – DSG*). Bgbl. 565/1978, http://www.ris.bka.gv.at/Dokumente/BgblPdf/1978_565_0/1978_565_0.pdf (Accessed: 29.09.2016).

Austrian Parliament. 1999. *Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000).* Bgbl. I Nr. 165/1999, as amended on July 19th, 2013. Unofficial English translation: http://archiv.dsb.gv.at/DocView.axd?CobId=41936 (Accessed: 29.09.2016).

Austrian Chancellor. 2004. *Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 - StMV 2004).* Bgbl. II Nr. 312/2004, as amended on July 23rd, 2013. http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003495 (Accessed: 29.09.2016).

Ball, Kirstie. 2003. Categorizing the workers. Electronic surveillance and social ordering in the call center. In *Surveillance as social sorting. Privacy, risk, and digital discrimination*. Ed.: David Lyon. 201-225. London and New York: Routledge.

Ball, Kirstie, Elizabeth Daniel, Sally Dibb and Maureen Meadows. 2010. Democracy, surveillance and "knowing what's good for you": the private sector origins of profiling and the birth of “Citizen Relationship Management”. In *Surveillance and Democracy*. Ed.: Kevin D. Haggerty and Minas Samatas. 111-126. London, New York: Routledge.

Ball, Kirstie and Keith Spiller. 2012. Introduction. In *Surveillance Impact Report*. Deliverable D3.2 of the project Increasing Resilience in Surveillance Societies (IRISS), 11-24. Open University.

Ball, Kirstie and Laureen Snider. 2014. Introduction. The surveillance-industrial complex: towards a political economy of surveillance? In *The Surveillance-Industrial Complex. A Political Economy of Surveillance*. Ed. Kirstie Ball and Laureen Snider. 1-8. London, New York: Routledge.

Bauman, Zygmunt and David Lyon. 2012. *Liquid Surveillance: A Conversation*. Cambridge: Polity

Baumann, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon and R. B. J. Walker. 2014. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology* 2014, 8:121-144.

Beck, Ulrich. 2015. *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt am Main: Suhrkamp.

Bellanova, Rocco. 2014. Data Protection, with Love. *International Political Sociology* Vol.8 1:112-115.

Bentham, Jeremy. 1995 (1787). *The Panopticon Writings*. Ed.: Miran Bozovic. 29-95. London: Verso.

Bigo, Didier. 2001. *Security(s): Internal and External, the Möbius ribbon*. https://www.academia.edu/3102803/The_M%C3%B6bius_ribbon_of_internal_and_external_security_ies_ (Accessed: 26.09.2016).

Bigo, Didier. 2006. Security, Exception, Ban and Surveillance. In: *Theorizing Surveillance: The Panopticon and Beyond*. Ed.: David Lyon. Cullompton: Willan Publishing.

Bigo, Didier. 2008. Globalized (In)Security: The Field and the Ban-Opticon. In: *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*. Ed.: Didier Bigo and Anastassia Tsoukala. London: Routledge.

Bogard, William. 2012. Simulation and post-panopticism. In *Routledge Handbook of Surveillance Studies*. Ed.: Kirstie Ball, Kevin Haggerty and David Lyon. 30-37. London and New York: Routledge.

Bogner, Alexander and Wolfgang Menz. 2009. Experteninterviews in der qualitativen Sozialforschung. Zur Einführung in eine sich intensivierende Methodendebatte. In *Experten-interviews. Theorien, Methoden, Anwendungsfelder*. Ed.: Alexander Bogner, Beate Littig and Wolfgang Menz. 7-34. 3. überarbeitete Ausgabe. Wiesbaden: VS Verlag für Sozialwissenschaften.

Bogner, Alexander and Wolfgang Menz. 2009a. Das Theoriegenerierende Experteninterview-Erkenntnisinteresse, Wissensformen, Interaktion. In *Experten-interviews. Theorien, Methoden, Anwendungsfelder*. Ed.: Alexander Bogner, Beate Littig and Wolfgang Menz. 61-98. 3. überarbeitete Ausgabe. Wiesbaden: VS Verlag für Sozialwissenschaften.

Boltanski, Luc and Eve Chiapello. 2007. *The New Spirit of Capitalism*. London, New York: Verso.

Bourdieu, Pierre. 1992. The Practice of reflexive Sociology (the Paris workshop). In: *An Invitation to Reflexive Sociology*. Ed.: Pierre Bourdieu and Loïc J.D. Wacquant. 216-260. Chicago and London: The University of Chicago Press.

Brown, Nik, Brian Rappert, Andrew Webster. 2000. *Contested Futures. A sociology of prospective techno-science*. Aldershot, Burlington, Singapore, Sydney: Ashgate.

Brown, Sheila. 2006. The criminology of hybrids. Rethinking crime and law in technosocial networks. *Theoretical Criminology* Vol.10 2:223-244.

Caddy, Becca. 2016. Food trackers: The best calorie counter apps and wearables. Tech yourself thin with these food apps and trackers. *Wareable*. April 11, 2016. http://www.wareable.com/health-and-wellbeing/food-trackers-the-best-calorie-counter-apps-and-wearables (Accessed: 26.09.2016).

Clarke, Adele E., Janet K. Shim, Laura Mamo, Jennifer Ruth Fosket and Jennifer R. Fishman. 2003. Biomedicalization: Technoscientific Transformations of Health, Illness, and U.S. Biomedicine. *American Sociological Review* Vol.63 2:161-194.

Clarke, Roger. 1988. *Information Technology and Dataveillance*. http://www.rogerclarke.com/DV/CACM88.html (Accessed: 26.09.2016).

Clarke, Roger. 1997. *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. http://www.rogerclarke.com/DV/Intro.html (Accessed: 26.09.2016).

Clarke, Roger. 2001. While You Were Sleeping … Surveillance Technologies Arrived. http://www.rogerclarke.com/DV/AQ2001.html (Accessed: 26.09.2016).

Clarke, Roger. 2003. *Dataveillance – 15 Years on*. http://www.rogerclarke.com/DV/DVNZ03.html (Accessed: 26.09.2016).

Clarke, Roger. 2006. *What's 'Privacy'?* http://www.rogerclarke.com/DV/Privacy.html (Accessed: 26.09.2016).

Clarke, Roger. 2012. *A Framework for Surveillance Analysis*. http://www.rogerclarke.com/DV/FSA.html (Accessed: 26.09.2016).

Cooper, Melinda. 2006. Pre-empting Emergence. The Biological Turn in the War on Terror. *Theory, Culture & Society* Vol.23 4:113-135.

Council of Europe. 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. CETS No.108.

Council of Europe. 2016. Details of Treaty No.108. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (Accessed: 26.09.2016).

Council of the European Union. 2011. *Council conclusions on the Communication from the Commission to the European Parliament and the Council – A comprehensive approach on personal data protection in the European Union.* 3071st Justice and Home Affairs Council meeting Brussels. 24 and 25 February 2011.

Council of the European Union. 2015. *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* 2012/0011 (COD).

Court of Justice of the European Union. 2015. The Court of Justice declares that the Commission’s US Safe Harbour Decision is invalid. *Press Release* No 117/15. Luxembourg.

Couvacian, Ann. 2011. *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices.* Toronto, Ontario: Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf (Accessed: 29.09.2016).

De Hert, Paul and Serge Gutwirth. 2006. Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power. In *Privacy and the Criminal Law*. Ed.: Eric Claes, Antony Duff and Serge Gutwirth. Oxford: Intersentia.

De Hert, Paul and Vagelis Papakonstantinou. 2012. The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law & Security Review*. Vol.28 2012:130-142.

De Hert, Paul and Vagelis Papakonstantinou. 2016. The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*. Vol.32 2016:179-194.

Deleuze, Gilles. 1992. Postscript on the Societies of Control. *October* Vol.59 Winter:3-7.

Denzis, Geroge, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Metayer, Rodica Tirtea and Stefan Schiffner. 2014. *Privacy and Data Protection by Design – from policy to engineering*. European Union Agency for Network and Information Security (ENISA) report, December 2014.

Diekrmann, Andreas. 2012. *Empirische Sozialforschung. Grundlagen, Methoden, Anwendungen.* 6. Ausgabe. Hamburg: rowohlts enzyklopädie.

Elmer, Greg. 2003. A Diagram of Panoptic Surveillance. *New Media Society* Vol.5 2:231-247.

Elmer, Greg. 2004. *Profiling Machines: Mapping the Personal Information Economy.* Massachusetts: MIT Press.

Elmer, Greg. 2012. Panopticon – discipline – control. In *Routledge Handbook of Surveillance Studies*. Ed.: Kirstie Ball, Kevin Haggerty and David Lyon. 21-29. London and New York: Routledge.

Esposti, Sara Degli. 2014. When big data meets dataveillance: The hidden side of analytics. *Surveillance & Society* vol.12 2:209-225.

Esposti, Sara Degli. 2015. *Big Data Protection*. Study Report. Open University.

European Court of Human Rights, Council of Europe. 2010. *European Convention on Human Rights*. Strasbourg.

European Commission. 2009. *Review of the data protection legal framework.* http://ec.europa.eu/justice/newsroom/data-protection/opinion/090501_en.htm (Accessed: 29.09.2016).

European Commission. 2010. *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union*. COM(2010) 609 final. 4.11.2010.

European Commission. 2012. *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*. Press Release. http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en (Accessed: 25.09.2016).

European Commission. 2015a. *Agreement on Commission's EU data protection reform will boost Digital Single Market.* Press Release. http://europa.eu/rapid/press-release_IP-15-6321_en.htm (Accessed: 25.09.2016).

European Commission. 2015b. *Questions and Answers – Data protection reform.* Fact Sheet. http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm (Accessed: 25.09.2016).

European Commission. 2016a. *Digital Single Market for business and consumers*. http://ec.europa.eu/growth/single-market/digital/ (Accessed: 29.09.2016).

European Data Protection Supervisor. 2011. *Opinion of 14 January 2011 on the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union"*.

European Parliament. 2011. *Committee on Civil Liberties, Justice and Home Affairs, Working Document (1 and 2) on a comprehensive approach on personal data protection in the European Union*. 15.03.2011.

European Parliament. 2013. *Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).* COM(2012)0011 – C7-0025/2012 – 2012/0011(COD).

European Parliament and European Council. 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal L 281, 23/11/1995 P. 0031 – 0050.* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (Accessed: 25.09.2016).

European Parliament and European Council. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. *Official Journal L 119/1, 4.5.2016.* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC (Accessed: 29.09.2016).

European People's Party group. 2015. *Data protection reform timetable*. http://www.eppgroup.eu/news/Data-protection-reform-timetable (Accessed: 29.09.2016).

European Union. 2012. *Charter of Fundamental Rights of the European Union.* 26 October 2012, 2012/C 326/02.

European Union. 2012a. *Consolidated version of the Treaty on the Functioning of the European Union*, OJ L. 326/47-326/390 26.10.2012.

Federal Data Protection Act. 2009. *In the version promulgated on 14 January 2003 (Federal Law Gazette I p. 66), as most recently amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I p. 2814).* http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0133 (Accessed: 29.09.2016).

Feely, Malcolm M. and Jonathan Simon. 1992. The New Penology: Notes on the emerging strategy of corrections and its implications. *Criminology* Vol.30 4:449-474

Finn, Rachel. 2011. Surveillant staring: Race and the everyday surveillance of South Asian Women after 9/11. *Surveillance & Society* Vol.8 4:413-426.

Fischer, Daniel, Wolfgang Bonß, Nils Zurawski. 2014. 1st Dilemma: Privacy and Convenience. In *Conduct the observation/interviews. Doing Privacy in everyday encounters with surveillance.* Ed. Alexander Neumann, Regina Berglez, Reinhard Kreissl. Deliverable D4.2 of the project Increasing Resilience in Surveillance Societies (IRISS), 37-58. Institute for the Sociology of Law and Criminology.

Foucault, Michel. 1995 (1977). *Discipline and Punish. The Birth of the Prison.* 2nd Edition. New York: Vintage Books.

Foucault, Michel. 2007. *Security, Territory, Population. Lectures at the Collège de France 1977-78.* Palgrave Macmillan.

Fuchs, Christian. 2008. *Internet and Society: Social Theory in the Information Age*. New York: Routledge.

Fuchs, Christian. 2010. Class, Knowledge and New Media. *Media, Culture & Society* Vol.32 1:141-150.

Fuchs, Christian. 2011. How to Define Surveillance? *Matrizes.* Vol.5 1:109-136.

Fuchs, Christian. 2012. The political economy of privacy on Facebook. *Television & New Media* Vol.13 2:139-159.

Fuchs, Christian. 2015. Surveillance and Critical Theory. *Media and Communication* Vol.3 2:6-9.

Fuchs, Christian, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval (ed.). 2012. *Internet and Surveillance: The Challenge of Web 2.0 and Social Media*. New York: Routledge.

Fuchs, Walter and Reinhard Kreissl. 2011. Steuerung durch Recht – das VbVG aus soziologisch-theoretischer Perspektive. In *Generalpräventive Wirksamkeit, Praxis und Anwendungsprobleme des Verbandsverantwortlichkeitsgesetzes (VbVG). Eine Evaluierungsstudie*. Ed.: Walter Fuchs, Reinhard Kreissl, Arno Pilgram and Wolfgang Stangl. Institut für Rechts- und Kriminalsoziologie. Wien 2011.

Fuster, Gloria Gonzales. 2014. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Switzerland: Springer international publishing.

Galdon Clavell, Gemma, Lohitzune Zuloaga Lojo and Armando Romero. 2012. CCTV in Spain: An empirical account of the deployment of video-surveillance in a Southern-European country. *Information Polity* 17:57-68.

Galetta, Antonella & Paul de Hert. 2014. A European Perspective on Data Protection And Access Rights. Deliverable D5: Exercising Democratic Rights Under Surveillance Regimes – of the project Increasing Resilience in Surveillance Societies (IRISS). Vrije Universiteit Brussel.

Germain, Séverine, Laurence Dumoulin and Anne-Cécile Douillet. 2013. A Prosperous 'Business': The success of CCTV through the eyes of international literature. *Surveillance & Society* Vol.11 1/2:134-147.

Giddens, Anthony. 1985. *The Nation-State and Violence: Volume Two of a Contemporary Critique of Historical Materialism.* Cambridge: Polity Press.

Giddens, Anthony. 1990. *The Consequences of Modernity*. Stanford: Stanford University Press.

Giddens, Anthony. 1995. *A Contemporary Critique of Historical Materialism*. Stanford: Stanford University Press.

Giddens, Anthony. 1999. Risk and Responsibility. *The Modern Law Review* Vol.62 1:1-10.

Gläser, Jochen and Grit Laudel. 2009. *Experteninterviews und qualitatitive Inhaltsanalyse*. 3. Überarbeitete Ausgabe. Wiesbaden: VS Verlag für Sozialwissenschaften.

Grand Chamber of the European Court of Justice. 2012. Case C-614/10. ECLI:EU:C:2012:631.

Greenberg, Brad A. 2016. Rethinking Technology Neutrality. *Minnesota Law Review* 100:1495-1562.

Hacking Ian. 1986. Making Up People. In *The Science Studies Reader*. Ed.: Mario Biagioli. 161-171. New York: Routledge.

Haggerty, Kevin D. and Richard V. Ericson. 2000. The surveillant assemblage. *British Journal of Sociology* Vol.51 4:605-622.

Haggerty, Kevin D. and Minas Samatas. 2010. Introduction: surveillance and democracy: an unsettled relationship. In *Surveillance and Democracy*. Ed.: Kevin D. Haggerty and Minas Samatas. 1-16. London, New York: Routledge.

Hayes, Ben. 2012. The surveillance-industrial complex. In *Routledge Handbook of Surveillance Studies*. Ed.: Kirstie Ball, Kevin Haggerty and David Lyon. 167-175. London and New York: Routledge.

Hempel, Leon and Eric Töpfer. 2004. *CCTV in Europe. Final report*. Working Paper No.15. Berlin: Centre for Technology and Society. Technical University Berlin.

Hempel, Leon, Susanne Krasmann and Ulrich Bröckling. 2011. Sichtbarkeitsregime: Eine Einleitung. In *Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert. Leviathan Sonderheft 25/2010.* Ed.: Leon Hempel, Susanne Krasmann, Ulrich Bröckling, 7-24. Wiesbaden: VS Verlag für Sozialwissenschaften.

Heywood, Debbie. 2016. *Territorial scope and establishment under the GDPR*. https://unitedkingdom.taylorwessing.com/globaldatahub/article-gdpr-territorial-scope.html (Accessed: 29.09.2016).

International Conference of Data Protection and Privacy Commissioners. 2010. *Resolution on Privacy by Design*. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/10-10-27_Jerusalem_Resolutionon_PrivacybyDesign_EN.pdf (Accessed: 29.09.2016).

Introna, Lucas D. and David Wood. 2004. Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. *Surveillance & Society* Vol.2 2/3:177-198.

Jasanoff, Sheila. 2004. The Idiom of Co-Production. In *States of Knowledge. The Co-Production of Science and Social Order*. Ed.: Sheila Jasanoff. 1-12. London: Routledge.

Jasanoff, Sheila. 2015. Future imperfect: science, technology and the imaginations of modernity. In *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*. Ed.: Sheila Jasanoff, Sang-Hyun Kim. Chicago, London: University of Chicago Press.

Kaiser, Robert. 2014. *Qualitative Experteninterviews. Konzeptionelle Grundlagen und praktische Durchführung.*Wiesbaden: Springer Fachmedien.

Katzemich, Nina. 2013. *Film über die Lobbyschlacht um die EU-Datenschutzverordnung*. Lobby Control. https://www.lobbycontrol.de/2013/05/film-uber-die-lobbyschlacht-um-die-eu-datenschutzverordnung/ (Accessed: 29.09.2016).

King, Nigel. 1994. The Qualitative Research Interview. In *Qualitative methods in organizational research. A practical guide.* Ed.: Catherine Cassell and Gillian Symon. 15-36. London: Sage.

Knorr-Cetina, Karin. 1999. *Epistemic Cultures. How the Sciences Make Knowledge*. Cambridge, Massachusetts, London, England: Harvard University Press.

Kosinski, Michal, David Stillwell and Thore Graepel. 2013. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America* Vol.110 15:5802-5805.

Krasmann, Susanne and Sylvia Kühne. 2014. 'My fingerprint on Osama's cup'. On objectivity and the role of the fictive regarding the acceptance of a biometric technology. *Surveillance & Society* Vol.12 1:1-14.

Kreissl, Reinhard. 2014a. Assessing Security Technology's Impact: Old Tools for New Problems. *Science and Engineering Ethics*. Vol.20 3:659-673.

Kreissl, Reinhard. 2014b. Introduction and Overall Framework for WP4. In *Conduct the observation/interviews. Doing Privacy in everyday encounters with surveillance.* Ed. Alexander Neumann, Regina Berglez, Reinhard Kreissl. Deliverable D4.2 of the project Increasing Resilience in Surveillance Societies (IRISS), 6-22. Institute for the Sociology of Law and Criminology.

Kreissl, Reinhard and Lars Ostermeier. 2011. Wer hat Angst vorm Großen Bruder? Datenschutz und Identität im elektronischen Zeitalter. In *Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert. Leviathan Sonderheft 25/2010.* Ed.: Leon Hempel, Susanne Krasmann, Ulrich Bröckling, 281-298. Wiesbaden: VS Verlag für Sozialwissenschaften.

Land Hessen. 1970. Datenschutzgesetz GVBl. II 300-10 vom 7. Oktober 1970. Gesetz- und Verordnungsblatt für das Land Hessen Teil I, 1 Y 3228 A.

Latour, Bruno. 1990. Technology is society made durable. *The Sociological Review* 38:103-131.

Latour, Bruno. 1996. On actor-network theory. A few clarifications plus more than a few complications. *Soziale Welt* Vol.47 369-381.

Latour, Bruno. 2000 (1999). *Pandora's Hope. Essays on the Reality of Science Studies.* 2nd printing. Cambridge, Massachusetts, London, England: Harvard University Press.

L'Hoiry, Xavier and Clive Norris. 2014. *Exercising democratic rights under surveillance regimes.* Executive Summary. Deliverable D5: Exercising Democratic Rights Under Surveillance Regimes – of the project Increasing Resilience in Surveillance Societies (IRISS).

L'Hoiry, Xavier and Clive Norris. 2014a. *Locating Data Controllers – A Meta-Analysis of ten EU Member States*. Deliverable D5: Exercising Democratic Rights Under Surveillance Regimes – of the project Increasing Resilience in Surveillance Societies (IRISS).

L'Hoiry Duncan, Xavier and Clive Norris. 2015. The honest data protection officer's guide to enable citizens to exercise their subject access rights: lessons from a ten-country European study. *International Data Privacy Law*. Vol.5 3:190-204.

Lianos, Michalis and Mary Douglas. 2000. Dangerization and the end of deviance. The Institutional Environment. *British Journal of Criminology* Vol.40:261-278.

Littig, Beate. 2013. *Expert Interviews. Methodology and Practice*. IASR Lecture Series

Luhmann, Niklas. 1976. The future cannot begin. Temporal structures in modern society. *Social Research*. Vol.43 1:130-152.

Luhmann, Niklas. 1990. Risiko und Gefahr. In *Soziologische Aufklärung 5. Konstruktivistische Perspektiven.* Ed.: Niklas Luhmann. 131-169. Opladen: Westdeutscher Verlag.

Luhmann, Niklas. 1991. *Soziologie des Risikos*. Berlin: De Gruyter Studienbuch.

Luther, Catherine and Ivanka Radovic. 2012. Perspectives on Privacy, Information Technology and Company/Governmental Surveillance in Japan. *Surveillance & Society* Vol.10 3/4:263-275.

Lyon, David. 1994. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.

Lyon, David. 2001. Surveillance after September 11. *Sociological Research Online* Vol.6 Issue 3.

Lyon, David. 2003a. Surveillance as social sorting: computer codes and mobile bodies. In: *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. Ed.: David Lyon, 13-30. New York: Routledge.

Lyon, David. 2003b. Surveillance Technology and Surveillance Society. In *Modernity and Technology*. Ed.: Thomas J. Misa, Philip Brey and Andrew Feenberg. 161-183. Cambridge, Massachusetts, London: The MIT Press.

Lyon, David. 2014. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society* July-September 2014:1-13.

Lyon, David. 2015. The Snowden Stakes: Challenges for Understanding Surveillance Today. *Surveillance & Society* Vol.13 2:139-152.

MacNaughton-Smith, Peter. 1975. Der zweite Code – Auf dem Wege zu einer (oder hinweg von einer) empirisch begründeten Theorie über Verbrechen und Kriminalität. In *Seminar Abweichendes Verhalten II – Die gesellschaftliche Reaktion auf Kriminalität, Band 1*. Ed.: Klaus Lüderssen and Fritz Sack. 197-212. Frankfurt am Main: Suhrkamp Taschenbuch Wissenschaft.

Macnish, Kevin. 2012. Unblinking eyes: the ethics of automating surveillance. *Ethics and Information Technology* Vol.14 2:151-167.

Mäkinen, Liisa A. 2016. Surveillance On/Off: Examining Home Surveillance Systems From the User's Perspective. *Surveillance & Society* Vol.14 1:59-77.

Mager, Astrid. 2012. Algorithmic Ideology. *Information, Communication & Society* 1-19.

Mallet, Jean-Claude; FRANCE. Présidence de la République; FRANCE. Ministère de la défense. 2008. *Défense et Sécurité nationale: le Livre blanc*. Paris: Odile Jacob, La Documentation française.

Mann, Steve. 2013. *'Veillance and Reciprocal Transparency: Surveillance versus Sousveillance, AR Glass, Lifeglogging, and Wearable Computing'*. IEEE ISTAS: 1-12.

Manzerolle, Vincent and Sandra Smeltzer. 2011. Consumer Databases and the Commercial Mediation of Identity: a medium theory analysis. *Surveillance & Society* Vol.8 3:323-337.

Marcoccio, Gloria and Luciano Delli Veneri. 2016. *European General Data Protection Regulation – Territorial Scope at a glance*. http://www.diritto.it/docs/38074-european-general-data-protection-regulation-territorial-scope-at-a-glance (Accessed: 29.09.2016).

Marx, Gary T. 2002. What's New About the "New Surveillance"? Classifying for Change and Continuity. *Surveillance & Society* Vol.1 1:9-29.

Marx, Gary T. 2003. A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues* Vol.59 2:369-390.

Marx, Gary T. 2007. Desperately Seeking Surveillance Studies: Players in Search of a Field. *Contemporary Sociology* Vol.36 2:125-130.

Marx, Gary T. 2009. A Tack in the Shoe and Taking Off the Shoe: Neutralization and Counter-neutralization Dynamics. *Surveillance & Society* Vol.6 3:294-306.

Marx, Gary T. 2011. The New Surveillance. Some concepts and some implications for privacy and stratification. In *Sichtbarkeitsregime. Überwachung, Sicherheit und Privatheit im 21. Jahrhundert. Leviathan Sonderheft 25/2010*. Ed.: Leon Hempel, Susanne Krasmann, Ulrich Bröckling, 85-98. Wiesbaden: VS Verlag für Sozialwissenschaften.

Mayring, Phillip. 2007. *Qualitative Inhaltsanalyse. Grundlagen und Techniken.* Weinheim: Deutscher Studien Verlag.

McGuigan, Jim. 2013. Data Protection Regulation provokes intense lobbying. *European Journal of Cancer*. Vol.49 Issue 7/8.

McIntosh, Ian, Samantha Punch, Nika Dorrer and Ruth Emond. 2010. 'You don't have to be watched to make your toast': Surveillance and Food Practices within Residential Care for Young People. *Surveillance & Society* Vol.7 3/4:290-303.

McQuade, Brendan I. 2016. Police and the Post-9/11 Surveillance Surge: "Technological Dramas" in "the Bureaucratic Field." *Surveillance & Society* Vol.14 1:1-19.

Menzel, Birgit and Jan Wehrheim. 2010. Soziologie Sozialer Kontrolle. In *Handbuch Spezielle Soziologien*. Ed.: Georg Kneer and Markus Schroer. 1. Auflage. Wiesbaden: VS Verlag für Sozialwissenschaften / Springer Fachmedien Wiesbaden GmbH.

Meuser, Michael and Ulrike Nagel. 2009. Experteninterviews und der Wandel der Wissenproduktion. In *Experten-interviews. Theorien, Methoden, Anwendungsfelder*. Ed.: Alexander Bogner, Beate Littig and Wolfgang Menz. 35-60. 3. überarbeitete Ausgabe. Wiesbaden: VS Verlag für Sozialwissenschaften.

Mommsen. Wolfgang J. 2004. *Max Weber und die deutsche Politik 1890-1920*. 3. Auflage, Tübingen.

Myers, Monika and Michael Wilson. 2014. Leprosy and the Plague: State Surveillance of Low-Income Fathers. *Surveillance & Society* Vol.12 1:124-139

Norris, Clive and Gary Armstrong. 1999a. CCTV and the Social Structuring of Surveillance. In *Crime Prevention Studies* Vol.10. ed.: Kate Painter and Nick Tilley, 157-178. New York: Criminal Justice Press

Norris, Clive and Gary Armstrong. 1999b. *The Maximum Surveillance Society: the rise of CCTV*. Oxford and New York: Berg.

Objectives of "europe-v-facebook.org". http://europe-v-facebook.org/EN/Objectives/objectives.html (Accessed: 25.09.2016).

ORF. 2013. *Private Videoüberwachung im Vormarsch*. http://wien.orf.at/news/stories/2581260/ (Accessed: 29.09.2016).

Organisation for Economic Cooperation and Development (OECD). 1980 (updated in 2013). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborder-flowsofpersonaldata.htm#top (Accessed: 29.09.2016).

Patton, Paul. 1994. Metamorpho-Logic: Bodies and Powers in a Thousand Plateaus. *Journal of the British Society for Phenomenology* Vol.25 2:157-170.

Pearce, Lisa D. 2012. Mixed Methods Inquiry in Sociology. *American Behavioral Scientist* Vol. 56 6:829-848.

Pfadenhauer, Michaela. 2009. Auf gleicher Augenhöhe. Das Experteninterview – ein Gespräch zwischen Experte und Quasi-Experte. In *Experten-interviews. Theorien, Methoden, Anwendungsfelder*. Ed.: Alexander Bogner, Beate Littig and Wolfgang Menz. 99-116. 3. überarbeitete Ausgabe. Wiesbaden: VS Verlag für Sozialwissenschaften.

PoKempner, Dinah. 2014. The Right Whose Time Has Come (Again). Privacy in the age of surveillance. In: *Human Rights Watch World Report 2014. Events of 2013.* New York: Seven Stories Press, 41-52.

Poster, Mark. 1990. *The Mode of Information: Poststructuralism and Social Context.* Cambridge: Polity Press.

Poudrier, Jennifer. 2003. "Racial" categories and health risks: epidemiological surveillance among Canadian First Nations. Im *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. Ed.: David Lyon, 111-134. New York: Routledge.

Preisendörfer, Peter. 2011. *Organisationssoziologie. Grundlagen, Theorien und Problemstellungen.* 3. Auflage. Wiesbaden: VS Verlag für Sozialwissenschaften, Springer Fachmedien.

Purtova, Nadezhda. 2015. The illusion of personal data as no one's property. *Law, Innovation and Technology* Vol.7 1:83-111.

Riccardi, Lee J. 1983. The German Federal Data Protection Act of 1977: Protecting the Right to Privacy? *International & Comparative Law Review* Vol.VI 1:243-271.

Rodrigues, Rowena, David Wright, and Kush Wadhwa. 2013. Developing a privacy seal scheme (that works). *International Data Privacy Law*, Vol.3 2:100-116.

Rule, James B. 2007. *Privacy In Peril. How we are sacrificing a fundamental right in exchange for security and convenience.* New York: Oxford University Press.

Ryz, Lawrance and Lauren Grest. 2016. A new era in data protection. *Computer Fraud & Security*. March 2016:18-20.

Sandoval, Marisol. 2012. A Critical Empirical Case Study of Consumer Surveillance on Web 2.0. In: *Internet and Surveillance: The Challenge of Web 2.0 and Social Media*. Ed.: Christian Fuchs, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval, 147-169. New York: Routledge.

Schwartz, Paul M. 2004. Property, Privacy and Personal Data. *Harvard Law Review* Vol.117 7:2056-2128.

Scott, Richard W. and Gerald F. Davis. 2016 (2007). *Organizations and Organizing. Rational, Natural and Open System Perspectives*. New York: Routledge.

Smith, Garvin J.D. 2007. Exploring Relations between Watchers and Watched in Control(led) Systems: Strategies and Tactics. *Surveillance & Society Special Issue on 'Surveillance and Criminal Justice' Part 2*, Vol.4 4:280-313.

Smith, Garvin J.D. 2012. Surveillance work(ers). In: *Routledge Handbook of Surveillance Studies*. Ed.: Kirstie Ball, Kevin Haggerty and David Lyon. 107-116. London and New York: Routledge.

Sterbik-Lamina, Jaro. 2014. Mapping the Legal and Administrative Frameworks in Austria. In *Austria Country Reports*. Deliverable D5: Exercising Democratic Rights Under Surveillance Regimes – of the project Increasing Resilience in Surveillance Societies (IRISS). Institut Für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften.

Tschohl, Christof, Ewald Scheucher, Dieter Kargl, Julia Luksan, Alexander Czadilek, Herbert Waloschek, Reinhard Kreissl, Kilian Klinger, Walter Hötzendorfer. 2016. *HEAT Handbuch zur Evaluation der Anti-Terror-Gesetze in Österreich. Version 1.1*. Wien: Arbeitskreis Vorratsdaten Österreich.

Van Dijk, José. 2014. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society* Vol.12 2:197-208.

Vobruba, Georg. 2014. *Währung und Konflikt. Ambivalenzen der Eurokrise*. Serie Europa – Europe Series. No.2/2014.

von Laufenberg, Roger. 2017. Exercising Access Rights in Luxembourg. In *The unaccountable state of surveillance*. Ed.: Clive Norris and Xavier Duncan L'Hoiry. Routledge.

Waiton, Stuart. 2010. The Politics of Surveillance: Big Brother on Prozac. *Surveillance & Society* Vol.8 1:61-84.

Weber, Max. 1968. *Basic Sociological Term. Economy and Society*. G. Roth and C. Wittich. 3-62. Berkeley: University of California Press.

Weber, Max. 1980 (1922). *Wirtschaft und Gesellschaft*. Tübingen: Studienausgabe.

Winner, Langdon. 1980. Do Artifacts Have Politics? *Daedalus,* Vol.109 1:121-136.

Zaretsky, Robert. 2016. France’s Perpetual State of Emergency. The country’s extraordinary anti-terrorism measures are on the way to becoming entirely ordinary. *Foreign Policy*. July 16, 2016. http://foreignpolicy.com/2016/07/16/frances-perpetual-state-of-emergency/ (Accessed: 26.09.2016).

Zhang, Tao, Peer-Olaf Siebers and Uwe Aickelin. 2016. Simulating user learning in authoritative technology adoption: An agent based model for council-led smart meter deployment planning in the UK. *Technological Forecasting & Social change*. Vol.106, May 2016:74-84.

Zuboff, Shoshana. 1988. *In the Age of the Smart Machine: The Future of Work and Power*. Oxford: Heinemann Professional Publishing.

Zurawski, Nils. 2011. Local Practice and Global Data: Loyalty Cards, Social Practices, and Consumer Surveillance. *The Sociological Quarterly* Vol.52 509-527.

Zureik, Elia. 2007. Surveillance Studies: From Metaphors to Regulation to Subjectivity. *Contemporary Sociology* Vol. 36 2:112-115.

Zwick, Detlef and Nikhilesh Dholakia. 2004. Consumer Subjectivity in the Age of Internet: The Radical Concept of Marketing Control Through Customer Relationship Management. *Information and Organisation* Vol.14 3:211-236.

11. Appendixes

a. Interview Guidelines

Warm-up

I am interested in your work (as a data protection officer) in your organisation in terms of data collections and data protection and would like to ask you a few questions on those topics. The results of this interview will of course be anonymised. Would it be OK if I record the interview for analysing purposes only?

Opening question

Could you start by generally describing your position in the organisation and your daily occupations, especially in relation to the collection as well as the protection of personal data?

Topic-related questions:

Knowledge production:

How and where have you acquired the knowledge necessary for the tasks in relation to the operations at your organisation, especially in terms of data protection?

- Does your organisation provide also advanced training for your tasks/in regard to data protection?
- Are these organised and held externally or internally?
- Are these specifically promoted, or even obligatory?
- How welcomed are these advanced trainings within the organisation and the employees?

Conflicts, dilemmas and crisis:

- Have you experienced in your function within the organisation problems or crisis in terms of data collections or data protection, like for example a data breach or legal pursuits in regard to data protection rights? How have you and your organisation managed these problems?
- Do you know of situations in your organisation, where practices were not entirely in line with data protection regulations, and if so, how have you handled these situations?

Data protection within the organisation:

How do you perceive the importance for data protection in general within the organisation?

- How do the employees/your colleagues handle data collections and data protection? Is there an awareness for the importance of data protection?
- Does your organisation provide specific campaigns (e.g. sensibility for data protection) to promote data protection?
- How is data protection handled on the level of your supervisors/managers?

Access to personal data:

- How are the requests for access to personal data processed within your organisation? Could you please describe me the process how such a request is handled?
- What are difficulties which might occur when processing these request?
- Can you approximately assess the amount of such requests your organisation receives per years?
- According to you, do you have the feeling that citizens are aware of the rights they have and also make use of their rights for the right purposes (specifically wanting to know what personal data is processed by them, where, how and for how long)

New GDPR:

- The new GDPR was decided on by the European Commission after long negotiations. Have you followed the development of the GDPR and informed yourself already on the upcoming changes, and if so, how?
- Do you expect a lot of changes in regard to the new GDPR for your organisation and do you have the feeling that you are already well prepared in regard to the changes?
- One of the reasons for the European Commission to change the GDPR was to provide the citizens with more rights and control. In regard to the rights they already hold and the frequency and possibility/difficulty these are excreted – how do you consider that these will be accepted by the citizens?

Technology and data protection:

- In regard to the technological possibilities in terms of data collections and data processing, do you consider that the legal regulations are apt to guarantee a high level of data protection?
- What are the technological problems and difficulties you occur in regard to the day-to-day operations and how do you manage these?

Discussion-questions with general data protection and privacy topics:

Is the general public according to you well informed in the topic of data protection and privacy? What are the ways of improving the awareness of the public, also in regard to the sloppy way people handle their personal data – especially on the internet?

b. Abstract (English)

The rise of the massive surveillance and the large amount of data collections has an important effect on the society and on how privacy is perceived. There for it is important for data collectors to act as transparent as possible – in their way they handle personal data and not with the data itself. One way to obtain this transparency is the Art. 12 of the European data protection directive, giving the citizens a right of access to their personal data and thus an oversight of where their personal data is scattered and how it might be processed. However, these rights are only as far enforceable as they are complied to and promoted by the processing organisations.

In this research, the compliance with data protection regulations in national and international private and public organisations will thus be analysed. Interviews will be conducted with persons involved in the collection and protection of personal data in organisations in order to enlighten the way of how personal data is processed and how the citizens' rights are assured. Many internal and external factors influence how certain behaviours are implemented and manifested within organisations. The interviews will focus on the roles of the surveillance workers as the personnel operating the surveillance technology or performing the surveillance practice as well as on the role of the data protection officers (if implemented) and special attention will be paid on factors influencing organisational behaviour such as (expert) knowledge, societal pressures, as well as legal constraints and technological implications.

Embedded in the theoretical field of Surveillance Studies as well as Science and Technology Studies, the aim of the study is to highlight connected organisational structures which are able to promote or hinder 'data protective behaviour' and thus shape the way citizens and consumers are able to control their personal data.

c. Abstract (German)

Der starke Anstieg an Überwachungsmaßnahmen gepaart mit den großen Mengen an Sammlungen personenbezogener Daten hat einen großen Einfluss darauf wie Privatsphäre in unserer Gesellschaft wahrgenommen wird und wie mit Überwachung umgegangen wird. Aus diesem Grund ist es wichtig, dass datensammelnde Unternehmen transparent mit unseren Daten umgehen – transparent im Sinne ihrer Handlungen wohlgemerkt. Eine Möglichkeit diese Transparenz zu fördern ist der Art. 12 der Europäischen Datenschutzrichtlinie, welche den Bürgern das Recht auf Auskunft ihrer persönlichen Daten garantiert und somit ein Werkzeug bietet, eine Übersicht über die weitverstreuten personenbezogenen Daten zu erhalten. Dieses Recht ist jedoch nur so weit durchsetzbar wie die datensammelnden Unternehmen und Behörden diesem Recht Folge leisten, bzw. propagieren.

Deshalb zielt meine Untersuchung darauf ab, die Übereinstimmung mit datenschutzrechtlichen Bestimmungen in nationalen und internationalen, sowie privaten und öffentlichen Unternehmen zu analysieren. Personen, die in der Erhebung und Bearbeitung von personenbezogenen Daten, sowie im Datenschutz in Unternehmen tätig sind, sollen dazu interviewt um diverse Praktiken in den unterschiedlichen Unternehmen zu erleuchten. Viele interne als auch externe Faktoren sind dafür zuständig wie bestimmtes Handeln in Unternehmen eingeführt wird und sich manifestiert. Aus dem Grund zielen die Interviews auf die Rollen der „surveillance workers“ – als das Personal welches die Überwachungstätigkeiten durchführt – sowie der Datenschutzbeauftragten (wenn vorhanden) ab, um den Zusammenhang dieser Rollen und den beeinflussenden Faktoren organisatorischen Handelns, wie (Experten-)Wissen, gesellschaftlicher Druck, rechtliche Bedingungen und technologischen Gegebenheiten, herzustellen.

Theoretisch ist diese Studie eingeordnet im – recht jungen – Feld der Überwachungsforschung sowie in der Wissenschafts- und Technikforschung, mit dem Ziel unternehmerische Strukturen darzulegen, welche das „datenschutzrechtliche Handeln“ positiv wie negativ beeinflussen und somit auch vorgeben wie BürgerInnen und KonsumentInnen mit ihren personenbezogenen Daten umgehen können.