Celebrating Privacy Day:

The Right to be forgotten and individual privacy in the digital age

Student: Thea Kunz
Supervisor: Vaia Doudaki

Spring 2018
Abstract

This thesis explores the current status of privacy in the context of the upcoming implementation of the General Data Protection Regulation (GDPR) and, more precisely, focuses on the redefined Right to be forgotten as its most controversial component.

Norman Fairclough’s three-dimensional model of critical discourse analysis was deployed to show how the Right to be forgotten is reshaping the privacy discourse in the age of big data, digitalization, surveillance and data driven business. Qualitative content analysis was used to serve critical discourse analysis as the first stage of the three dimensions, which built the foundation for the analysis of the broader discursive and societal practices. The digital age requires a rethinking of privacy in terms of the protection of personal data due to the embeddedness of technology in everyday life, big data, easy retrieval and cheap cloud storage. Forgetting and remembering are two facets that constitute human behavior but within the regime of technological advancements, both have lost, or changed their meaning. The new legislative framework aims to enhance forgetting but seems more of a façade to legitimate remembering. Several online blog posts written by experts in diverse fields of knowledge have shown that the current legislative framework is no longer sufficient due to technological change and unequal hegemonic relations, which contribute to reshaping the privacy discourse.

The thesis does not give a final answer to the questions raised but contributes to the debate and to a comprehensive understanding of the new legislation in Europe.

Keywords:
GDPR, Right to be forgotten, critical discourse analysis, privacy, data protection, democracy

Word Count: 18.373
# Table of contents

Preface ................................................................................................................. 5  
Acknowledgements ............................................................................................... 5  
Abbreviations ......................................................................................................... 6  

1. **Introduction** ................................................................................................... 7  
   1.1 Aim and research question ............................................................................. 8  
   1.2 Contribution to the field ............................................................................... 9  

2. **Background** .................................................................................................... 10  
   2.1 Data Protection in Europe until Mai, 2018 ..................................................... 10  
   2.2 The General Data Protection Regulation (GDPR) ......................................... 10  
   2.3 Major Changes .............................................................................................. 12  
   2.4 The Right to Be Forgotten ............................................................................ 13  

3. **Literature Review** .......................................................................................... 16  
   3.1 Setting the scene ............................................................................................ 16  
   3.2 Understanding Privacy ................................................................................... 17  
   3.3 The Right to be forgotten – controversy ....................................................... 20  

4. **Theoretical Framework** .................................................................................. 22  
   4.1 Digitalization and Privacy Theory ................................................................ 22  
   4.2 A theoretically informed approach .............................................................. 22  
   4.3 Discourse analysis ....................................................................................... 25  
   4.4 Fairclough’s three-dimensional framework ................................................. 26  
   4.5 Critical discourse analysis (CDA) ............................................................... 27  

5. **Methodology** .................................................................................................. 29  
   5.1 Data collection - Blogs as genre and Sampling ............................................. 29  
   5.2 Data selection criteria .................................................................................. 31  
   5.3 Data analysis – (critical) Discourse analysis and qualitative content analysis .. 32  
   5.3.1 Coding ...................................................................................................... 33  
   5.4 Ethical considerations and limitations ......................................................... 34  
   5.5 Researcher’s position and role ..................................................................... 35  

6. **Presentation and Analysis of Results** .............................................................. 37  
   6.1 RTBF – unidentifiable threat or silver lining? – A textual analysis ............. 38  
   6.2 The social perspective .................................................................................. 41  
   6.3 Discussion ...................................................................................................... 46
7. Conclusion ........................................................................................................ 49
8. References .................................................................................................... 50
Preface

Acknowledgements

First, I would like to thank Vaia Doudaki for calming my nerves with precious advice and words of encouragement; and for simply being an awesome supervisor and teacher during this past year. Thank you for always taking care of us!

Second, without my Mum and Dad, all this would not have been possible. Thank you for letting me leave for Sweden, for saying ‘you can do it’ every time when we were on the phone and for always being there!
## Abbreviations

2. **ECJ** – European Court of Justice
3. **CJEU** – Court of Justice of the European Union
4. **LIL** – Loi Informatique et libertés
5. **UNESCO** – United Nations Educational, Scientific and Cultural Organization
6. **TFEU** – Treaty on the Functioning of the European Union
7. **EU** – European Union
8. **RTBF** – Right to be forgotten
1. Introduction

“I have as much privacy as a gold fish in a bowl” – Princess Margaret

Princess Margaret, the former Scottish countess, may not have lived in the age as it is today, but already then, she saw the impending problem very clearly, and she had not even experienced the invention of Web 2.0. Today, the internet has opened up many paths for innovation, progress, communication and publication; it has provided us a tool, that enables us to do, what was once a utopian idea, now have become ordinary. Without the internet, our daily life would not be as it is today; progressive, fast and convenient. Whether this is good or bad, lies in the eye of the beholder.

With the focus on today’s almost completely digital world, with new technological developments that are deeply embedded in everyday life, it seems we have completely forgotten the analogue world. What the majority of internet users do not know or try to ignore is the fact that every digital item they possess gathers huge amounts of data. Personal data has become the currency we exchange for services that are being sold to us as ‘free’. Bruce Schneier (2015:4) calls this surveillance. Technology constitutes our everyday life without us actively being aware of it. Max Schrems, an Austrian privacy advocate, demanded in 2011 that Facebook hands over all the data they would held on him. Two years later, he received 1.200 pages with everything he had ever liked or clicked on, his friends, photos and all the advertising material he had ever viewed. Even though all this data may not be used, it is there. Eric Schmidt, Google chairman, admitted “We know where you are. We know where you’ve been. We can more or less know what you’re thinking about” (Schneier, 2015:22). With this it becomes very clear that the rules we have established to protect us from threats that emerge online are no longer valid. Times have changed, demanding new forms of legislation.

We live in the digital era where data storage, easy retrieval and the global reach of electronic information is easy and where the phrase ‘knowledge is power’ is taken to a whole new level. Secretive monitoring, undisclosed transfer and monetization of personal data through marketing justify and demand new regulatory safeguards for people, since, as Floridi noted, we are our information (Mckay, 2017:539). Within normative theory, the notion of control allows individuals to decide themselves what information and to what extend they communicate, defining privacy as the voluntary withdrawal from society (Westin, 1967:7). Westin’s theory will provide the framework for this research.
The General Data Protection Regulation (GDPR) is an attempt to adapt privacy law to reality. It entails a number of personal rights that are meant to give the people back the power and control over their own personal data and to, unlike the former Directive, try to unify data protection within the European borders. Even though the GDPR appears to have been written with good intentions, it also raises a number of controversial issues concerning, for instance, the fundamental right of Freedom of Expression and Information (Article 11, Charter of Fundamental Rights of the European Union) as these will be important and costly burdens that businesses will now have to face. Since treaties like Safe Harbor, the Edward Snowden revelation or the very recent case of Cambridge Analytica, where data of more than 71 million people has been leaked from Facebook, have indicated that international data flows are becoming more present, the GDPR will also have to be considered within a global context.

The Right to be forgotten gives people the possibility to have companies like search engines delete links to their personal information. It came into force after the 2014 Google Spain ruling where a Spanish citizen demanded from Google the deletion of old and irrelevant data that would affect his current situation. Rather than deletion, delisting is the more appropriate term to use as information is being delisted by deleting URLs from the search engines. However, it strongly enables individuals to edit their personal, digital history. Within the GDPR, the definition of personal data has been expanded providing the Right to be forgotten with a new frame which facilitates and widens the applicability of it. Yet, this process has underlying rules, as the requested information has to fulfill certain requirements in order to be deleted (see Article 17, or above). However, the Right to Freedom of Expression and Information play a crucial factor, as it possibly constitutes an opposition to the former. It therefore lies in the hands of the courts to find a balance between these two rights. Controversy always provides for discussion and expression of opinion. This I will take as a starting point for my research.

1.1 Aim and research questions

This thesis aims at analyzing this change of legislation in the perspective of privacy discourse and tries to reveal controversies and taken-for-granted assumptions within the privacy discourse that becomes present in the selected texts. The main theme will be the Right to be forgotten which is one of the most controversial rights entailed in the GDPR. My focus lies on blogpost authors, who are primarily experts in the fields IT, marketing, law and writers and reporters who focus their writings specifically on privacy, and statements as well
as the ways in which they present their arguments in order to draw conclusions or assumptions on how the **Right to be forgotten** will potentially affect the online world and its users. Accordingly, the main topic of this thesis will revolve around how the discourses of the **Right to be forgotten** are constructed by these authors. The major issues, questions and concerns will be studied to explore the right’s potential influence on (personal) privacy and data protection, primarily. Aspects of human rights, globalization and digitalization will also be explored as they constitute parts of the greater discourse around privacy and data protection.

Therefore, two research questions will be the guideline for analysis.

**RQ 1:** What are the main issues at stake regarding the **Right to be forgotten** according to the blog posts under study?

The discussion of this question will mainly be based on textual analysis as a first step.

**RQ 2:** How will the **Right to be forgotten** contribute to shaping future data protection legislation and the privacy discourse, according to the blog authors? This question aims to analyze the bigger picture and the discourse on privacy and the **Right to be forgotten**.

In the following chapters I will first give a theoretical background on the topic and current conceptions that can be found in literature as well as a broad explanation of the whole concept of the GDPR. Thereafter I will define the theoretical framework that lays ground for the analysis of the data, followed by the methodological approaches that was applied to conduct this research. A discussion and final conclusion with recommendations for further research will end this thesis.

**1.2 Contribution to the field**

With the enforcement of the GDPR on the 25th of May this year, privacy receives a huge wave of attention. The protection of personal data now becomes a major focus within the privacy discourse and digitalization. However, the literature raises points on rethinking privacy in today’s digital world, but it lacks clarity and timeliness since the GDPR is so short upon arriving. This research builds upon understanding privacy in a more contemporary context as well as its absolute relevance. Drawing on Westin’s and Taylor’s theories, this research is placed in context but tries to apply the theory to reality.
2. Background

2.1 Data Protection in Europe until May, 2018

In 1981, the Council of Europe established legal standards to enable the free flow of information among all EU member states without threatening personal privacy. The UK introduced their Data Protection Act in 1984, Germany regulated data protection through their Federal Data Protection Act and France’s Loi Informatique et libertés (LIL) dates back as far as 1978. However, the legislation concerned with data protection was too dissimilar among the member states for a company to comply with the legislation in all countries in which it operates and not only in its home country (Calder, 2016:14-16).

On October 241995, Directive 95/46 was enacted by the European Parliament and Council “on the protection of individuals with regard to the processing of personal data and on the free movement of such data” (UNESCO, 200:123) and since then has been the foundation of data privacy in Europe. Due to the nature of the Directive, EU countries were facing a “legal minefield” of different interpretations when applying it to national law, which led to fragmentation within the Union and the perception that there were significant risks to the protection of natural persons (Tankard, 2016:5; Article 1 (9)). Moreover, fines were negligible under Directive 95/46 (The Economist, 2018). This fact and the rapidly changing data driven environment demand a new and more adequate framework for data protection. Back in 1995, less than one percent of the world’s population was using the internet, but in today’s digital era of smartphones, tablets and social media, it is almost atypical to stay out of the online world (Tankard, 2016:5). Almost all information and data is produced and consumed by technology, which poses an underestimated threat to its protection (ibid.). The GDPR is meant to update and unify the data protection standards in the EU, in order to improve transparency and give stakeholders power over their own data (EU GDPR Portal: eugdpr.org).

2.2 The General Data Protection Regulation (GDPR)

While a Directive sets out minimum conditions, leaving room for interpretation and application to the national laws of individual EU member states to achieve a set goal, a regulation is a binding legislative act that must be applied in its entirety by all member states (EU GDPR Portal: eugdpr.org, Calder, 2016:17). Due to its legal weight, it takes longer to be enacted but it also ensures a greater consistency (Calder, 2016: 36). The GDPR will
finally come into force on the 25th May 2018 with all its 99 articles and for all 28 member states simultaneously and immediately (Sobolewski et al., 2017:208). After it was agreed on in December 2015, a final version followed in July 2016 following a two-year waiting period for organizations and companies to meet compliance (Tankard, 2016:6). The GDPR is based on the fundamental belief that privacy and the protection of personal data are basic human rights, which is now protected by the Charter of Fundamental Rights as a right of an individual (Sobolewski et al., 2017:208). Its main purpose is to align data protection legislation across all EU countries, providing the people with a number of rights that give individuals control and power over their own data. One of them, and the most controversial among all, is the Right to be forgotten (Article 17, GDPR), which will be the main point of discussion in this thesis.

In order to be able to understand the GDPR and the following chapters, it is crucial to define certain terminology based on the regulation itself and contemporary research.

A data collector is the entity, natural person, agency, public authority or other body, that determines the purpose, conditions and means of the processing of personal data whereas a data processor is responsible for the processing of personal data on behalf of the controller (Calder, 2016:21; EU GDPR Portal: eugdpr.org). Often, they will be the same, and a data controller might have several data processors (Calder, 2016:22). A significant difference is that a data controller is responsible for the lawful, fair and transparent processing of personal data which is expanded in Article 6, GDPR, where it is clarified that consent must have been given, and that the processing is necessary for certain tasks (Calder, 2016:43). Processing in this case means any operation which is performed on personal data or any kind of interaction with personal data (Calder 2016:26; Article 4 (2)).

A data subject is defined by the regulation as “an identified or identifiable natural person” with no restrictions to nationality or place of residence. It cannot be a corporation or other entity but a natural person (Calder, 2016:22). Recital 14 gives the clearest definition of a data subject although it still retains an aspect of ambiguity. According to Recital 14, the GDPR applies to anyone who finds themselves located within the European borders at the point in time when the data processing starts, with no regard to citizenship or residence.

Personal Data means any information that can identify a natural person (data subject) such as a name, an identification number, location data or an online identifier (Calder, 2016:25). Under the GDPR the scope is further expanded to include cookies or IP addresses and data that could identify a person directly or indirectly (Tankard, 2016:5). However, sensitive personal data is being classed separately by the GDPR as ‘special categories’ of
information such as trade union membership, religious beliefs or sexual orientation (Burgess, 2018).

Personal data breaches are breaches of security leading to the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed (Article 4 (12)).

2.3 Major Changes

The GDPR will change the way we look at the handling of data completely. Compared to the Directive 95/46, the regulation will demand strict compliance from data controllers and grant users with the right to data erasure, the right to object to processing, the right to the portability of data on request and the right to object to profiling.

The foremost biggest change is that the GDPR expands the scope of privacy to every person or organization that collects or processes data related to EU citizens, no matter where they are based or where the data is stored with no exception for cloud storage as a very convenient way of data storage for businesses that share data with subsidiaries or other businesses (Tankard, 2016:5; Article 3(2)).

Moreover, consent must now be given and not assumed (Smart Insights). “Consent means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her” (Article 4 (11); Sobolewski et al., 2017:209; Voss, 2017:7). This can be done by ticking a box when visiting a website or choosing technical settings which clearly indicates in this context that the data subject accepts the proposed processing of his or her data (Recital 32). Consent can be withdrawn at any time and it should “be as easy to withdraw as to give it” (Article 7 (3)). “Silence, pre-ticked boxes or inactivity” must not be counted as consent by a data controller (Calder, 2016:39, Recital 32). The user will have to tick boxes manually, however, this is already in line with how various companies currently handle the matter of consent.

Another major change constitutes the Right to Data Portability. Data subjects can request a copy of any personal data an organization is holding on them and demand that this information is transmitted to another organization (data controller) in a structured, commonly used and machine-readable format (Article 20; Calder, 2016:42; Sobolewski et al., 2017:210). This is already possible for the changing of mobile phone service providers for example, but it will be extended by this right to any data controller. However, Sobolewski
et al. argue that the “actual meaning of this right depends on the efforts to be made to gain possession of the data and the willingness of the customer to use the new opportunity. Consequently, the GDPR gives people the right to request from a data controller all data held on them and the purpose for that. The information should be provided “in a concise, transparent, intelligible and easily accessible form, using clear and plain language” (Sobolewski et al., 2017:210). If data subjects then believe the processing to be infringing the GDPR, they have the right to “lodge a complaint with their relevant data protection authority” (Calder, 2016:39).

Failure to meet the compliance requirements by the GDPR can lead to hefty fines. A data breach is defined in Article 4 (12) as a “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed” (Calder, 2016:26). For a minor breach, companies can be fined with up to 2% of their world-wide revenue or 10 million Euro, whichever is higher. For first offences, a warning can be given (Tankard, 2016:5; Article 79 (6) (a)). For more serious misdemeanors, 4% of the world-wide revenue or 20 million Euro can be imposed (whichever is higher) (ibid.). The GDPR introduces compulsory breach notifications which includes that organizations suffering a breach must notify a data protection authority within 72 hours in the member state that functions as the company’s main establishment (Tankard, 2017:5). Calder argues that this threat alone will ensure the compliance of all data controllers and processors (2016:42). However, the GDPR unifies the sanctions across the EU and states that the fines are to be “effective, proportionate and dissuasive” (Article 83 (1); Calder, 2016:42).

2.4. The Right to Be Forgotten

The Right to be forgotten is one of the most discussed, controversial and important data protection and privacy laws of the decade and is likely to remain so in the following years. It is based on the Right to Data Protection, constituted in the EU Charta of Fundamental Rights with its legal and theoretical foundations that form the basis of modern European privacy laws and an extension to Article 12 (b) and Article 14 (a) of the European Data Protection Directive 95/46 (Shankar, 2014:229; Calder, 2016:12-13; DPD 95/46). It is based on the idea of having the power as an individual to “determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past” (Nohe, 2018). Data subjects now have the right to demand from any data controller or processor to have the data they hold on
the data subject to be erased. This must proceed as soon as consent is withdrawn. Organizations will not have a long list of possible reasons for refusal which is why they will be required to have their data clearly structured (Nohe, 2018; Calder, 2016:42). As Calder argues, anyone who understands the internet, assumes that this will hardly be possible, however, as data protection authorities will want to see that necessary steps have been taken and all procedural measures have been employed to delete all data that might be public, including news articles and databases for instance (2016:42). This is also a reason why its title “The Right to be forgotten” is rather controversial since ‘forgetting’ in the digital age is hardly possible. Moreover, the exception that organizations can use to refuse such a demand are the Right to Freedom of Expression and the Right to Know, which, same as the Right to Privacy, constitute the fundamental rights of an individual.

The origins of the Right to be forgotten are constituted in the 2014 Google Spain vs. Mario Costeja González ruling. However, the original roots of this right can be found in French and Italian law which recognize ‘le droit à l’oubli’ or the ‘right of oblivion’ that allow convicted criminals who have served their time to object to the publication of facts of their conviction (Oghia, 2018: www.cima.net.org). The Right to be forgotten came into being in 2014 by a ruling of the ECJ (C-131/12). Mario Costeja González, a Spanish citizen, lodged a complaint to the Agencia Española de Protección (the Spanish National Data Protection Agency) to have La Vanguardia, a newspaper, remove information on him and his social security debts as well as Google Inc. and its Spanish subsidiary Google Spain to remove the links to that newspaper article. The proceedings concerning his debts have been fully resolved and had therefore become irrelevant and outdated. The Court rejected the complaint against La Vanguardia but ruled against Google Inc. and Google Spain since they would fall in the Directives meaning under the definition of a data controller, engaged in the concept of data processing, with its activities as an online search engine (Google Spain, C-131/12, para. 34). Google argued against the removal of data from Google Inc. since it would not fall into national law. However, the ruling ended in 2014 with Google Spain deleting links to La Vanguardia and therefore removing search results linking González to the newspaper article, which was lawfully published and therefore could not be deleted (Yuom & Park, 2016:280-284; Columbia University) In May 2014, Google complied with the CJEU ruling and established an electronic form for its users to request the delisting of one or more URLs connected to their identity, only applicable in EU member states. According to Google’s Transparency Report, 56,7% of all requested URLs have been deleted. Facebook is the site most affected by the ruling (Google Transparency Report, 2018). However, the Right to be
Forgotten is not completely new, the GDPR just expands its scope by extending the definition of personal data as well as the territorial scope for it to be applicable on a wider scale. “The new clothes of an old right” so to say, as Zanfir titled her article (2015).
3. Literature Review

3.1. Setting the scene

In the context of the protection of personal data, the literature agrees on the fact that “two moral duties need to be reconciled proactively: fostering human rights and improving human welfare” (Floridi & Kammourieh in Taylor et al., 2017:84; Jones, 2016:28; George Brock, 2016:2). Free speech and privacy have to be accorded ‘equal respect’ by the courts which are aiming to find a balance. This balance can only be achieved by reasoning from the facts of separate cases and cannot be guaranteed by automization. George Brock argues further that these two are not the only issues at stake but also “discovery, historical memory, forgetting, the integrity of the public record, the right to know, and forgiveness” (Brock, 2016:2) will have to be taken into account too. His concern is further focused on journalism as a “systematic attempt to establish the truth of what matters of society in real time” (Brock, 2016:4). Free speech is fundamental for journalists who have celebrated the technological achievements and the journalistic advantages it brought but who now have to face the consequences of a huge shift (ibid.). Accordingly, Jones states that “newsworthiness and public interest are not necessarily, or likely, diminished with the passage of time” (2016:61) meaning that public figures or persons of public interest should not be guaranteed the possibility to erase uncomfortable information by applying a Right to be forgotten, restricting free journalism and therefore the sowing seeds of censorship. Big data, cheap storage and easy retrieval in the age of digitization have facilitated the demise of forgetting and therefore we risk losing the ephemeral, a significant change in our society. The ephemeral is what enables us to forget by its transitory and temporary character.

Mayer-Schönberger pointed out: “There is no question, the erosion of individual privacy is a fundamental challenge we are facing in our times” (2009:12). This is the point that unifies the literature on contemporary privacy, but approaches by different authors differ. Danah Boyd argues that “people, particularly younger people, are going to come up with coping mechanisms. That’s going to be the shift, not any intervention by a governmental or technological body” (in Jones, 2016:75). Jeffrey Rosen argues that “the most practical solution to the problem of digital forgetting…is to create new forms of atonement and forgiveness” (in Jones, 2016:76). Other authors argue that relying on social adaption in a world where forgetting is impossible is questionable. Ruth Gavison points out that “the absence of privacy may mean total destruction of the lives of individuals condemned by norms with only questionable benefit to society” (in Jones, 2016:76).
Papacharissi and Gibson see privacy as a luxury commodity “in that (a) it becomes a good inaccessible to most, (b) it is disproportionately costly to the average individual’s ability to acquire and retain it, and (c) it becomes inversely associated with social benefits, in that the social cost of not forsaking parts of one’s privacy in exchange for information goods and services (e.g., free e-mail account, online social networking) places one at a social disadvantage. Luxury goods not only possess a price point beyond the average person’s reach, they also connote social status and advantage” (2011:85).

Furthermore, the privacy paradox, a well-established theory in social sciences, and privacy uncertainty are issues that contribute to the debate. Acquisti, Brandimarte and Loewenstein argue that through technological advancements the collection and processing of personal data has become merely invisible which, as a result, causes individuals to lack knowledge about what kind of information data firms or governments have about them, how it is used and with what consequences (2015:509-510). Therefore, they are very likely to be uncertain of how much information to share. Research showed that “people being asked intimate questions either point blank or with credible assurances of credibility, although logically such assurances should lead to greater divulgence, they often had the opposite effect because they elevated respondents’ privacy concerns which without assurances would have remained dormant” (ibid.). This is called the privacy paradox, a well-established concept in social sciences, that shows the discrepancy between people’s concerns and actual behavior (ibid.). The existence of the privacy paradox in the EU is indicated by, for instance, by the fact that 72 percent of people in Poland have concerns about not having complete control over online privacy, but only 44 percent of them having actively tried to change their privacy settings. In Portugal, 79 percent have concerns and 52 percent have tried to change something. There are also countries like Sweden or the Netherlands, where more respondents have tried to change their privacy settings than people who are actually concerned (Sobolewski et al., 2017:211).

3.2 Understanding Privacy

It has to be recognized at this point, that the concept of privacy entails a lot more than only the protection of personal information. Solove (2006) gives a clear taxonomy of all kinds of privacy for further consideration. Lanah Kammourieh is quoting Paul Whitman who says that “European privacy protections “are all rights to control your public image – rights to guarantee that people see you the way you want to be seen. They are, as it were, rights to be shielded against unwanted public exposure – to be spared public embarrassment or
humiliation” (Kammourieh et al. in Taylor et al., 2017:37). When considering privacy within the context of the digital age and technological progress, there are a number of authors with different relevant approaches to defining privacy. This study is primarily based on the notion about privacy as a form of dignity that further aligns with Alan F. Westin’s (1967) normative approach to privacy as one of the classical and most relevant perspectives that have endured until today. According to him,

“Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small group intimacy or, when among large groups, in a condition of anonymity or reserve. (1967:7)

Warren and Brandeis published a famous paper in 1890 which sees privacy as the “right to be let alone” which is different from Westin’s notion of control, but, according to timely circumstances, Westin’s approach is more appropriate (Jones, 2016:82).

This research sees privacy as a dynamic construct that varies according to change and progress as well as how individuals perceive it in different technological contexts. Westin defines 4 states of privacy: “Solitude is being free from observation by others. Intimacy refers to small group seclusion for members to achieve a close, relaxed, frank relationship. Anonymity refers to freedom from identification and from surveillance in public places and for public acts. Reserve is based on a desire to limit disclosures to others; it requires others to recognize and respect that desire” (Margulis, 2003:412). These states explain how privacy operates and their foundation is based on social norms and legal traditions. According to Westin, privacy is linked to secrecy, however, he does not give a clear definition of secrecy except the indication that curiosity is a way of penetrating secrets (Margulis, 2003:415). In sum, he argues that privacy and secrecy are related, even though he admits that this relationship lacks clarity, but the relationship itself is relevant. Westin (1967) argues further that privacy operates on the level of an individual, group, and organization/institution. This is why his approach, among others, was chosen as the foundation for this research, since discussion about the Right to be forgotten will cover facets relevant to individuals as well as groups and organizations. The normative approach takes privacy as a right, which contributes to the study’s approach within a legislative framework.
Taylor et al. have a different approach to privacy than the former directive or the GDPR have taken. Both legal frameworks focus on individual persons (Floridi in Taylor et al., 2017:98). Floridi argues that “sometimes the only way to protect a person is to protect the group to which that person belongs” (ibid.). The notion that data analytical technologies are directed at the group level is the main focus in Taylor et al., providing grounds for new ways of understanding privacy. In the world of Big Data, information is no longer gathered about one specific person but rather about a larger, undefined group. “Data is analyzed on the basis of patterns and group profiles; the results are often used for general policies and applied on a large scale” (Taylor et al., 2017:5). Even though the directive and regulation do give certain rights to individuals, it is questionable whether the focus on individual control remains efficient in the age of Big Data where “it becomes increasingly difficult […] to be aware of every data processing activity” (Taylor et al., 2017:6) and to what degree this happens legitimately. The authors suggest that “individual control is too narrow” (Taylor et al., 2017:6) requiring our legal attention to be adjusted and extended “to pay attention to the actual technological landscape unfolding before us” (Taylor et al., 2017:2) and should be supplemented by focusing on categories and groups. The idea of group privacy was also established by Westin as the so-called ‘relational-privacy’ or ‘family-privacy’ (Westin, 1967 in Taylor et al., 2017:8). Taylor et al. are aware that in order to evaluate privacy on a group level, a definition of a group is necessary. As Taylor et al. are a large collective of authors, they present different ways of defining a group, but with the focus on technology and the Right to be forgotten, their approach sees a group defined by digital technologies as the most appropriate (Taylor et al., 2017:7). Even on this level, the notion of the group remains unclear. However, this epistemic shift obligates a new way of thinking about privacy and data protection (Kammourieh et al. in Taylor et al., 2017:46).

Moreover, the social shaping perspective sees society and technology as constantly influencing each other, causing people to eventually stop questioning individual technological devices. This process of domestication leads to the taken-for-granted perception of technology in everyday life (Baym, 2015:26). Baym quotes Nye who argues that in the dystopian perspective, technology may be seen as a way for elites to control masses or as “malevolent tricksters that promise positive change but in the end only make our lives more difficult” (Baym, 2015:33). Schneier argues “we are living in the golden age of surveillance” (2015:4). He points out that what we believe to be free services are not free at all, paid for with our data and therefore with our privacy, making the bargain an exchange of surveillance for free services (ibid.). The embeddedness of technology in our everyday
life gives governments and corporations the ability “to peer into our collective personal lives” (ibid.) especially because corporate and governmental surveillance now have merged, and although the intentions are different, the methods are the same. The fear of the terrorists, drug dealers or the child abductors allows for governments to have access to all this data and serves as justification for mass surveillance institutes like the NSA (ibid.). Schneier argues that there “will be a digital divide” between those who accept this surveillance and those who resist it (in Berghel, 2018:66). Privacy is an inherent human right, one that allows us to maintain human dignity and respect and to have control over our personal lives, but surveillance is a violation of such (ibid.). Solove defines surveillance as the “watching, listening to, or recording of an individual’s activities” (2006:490). In this context, it refers to online activities and the observation of behavior online.

3.3 The Right to be forgotten - controversy

Different authors argue, that the GDPR and especially the Right to be forgotten is not so much about forgetting (Zanfir, 2015:231; Bernal, 2013). The notion of forgetting enables us to leave our past behind and to think abstract thoughts. Digitization has brought with it a perfect digital memory, however, and Mayer-Schönberger argues that we have to become aware of the finiteness of memory suggesting attaching an expiry date to information in order to be able, as human beings, to evolve over time and have the capacity to learn (2009:13-14).

The main controversy of the Right to be forgotten is based on the fear it would threaten the Right to Freedom of Expression and therefore the protection of privacy as a fundamental human right. However, since it is within the nature of the courts to find a balance between two opposing rights, it is argued that there is no reason to believe this tradition will be disrupted (Zanfir, 2015:246; Yuom & Park, 2016:289). Tirosh argues, the right is neither an infringement of the right to free expression nor a guarantee for privacy but rather the right to construct one’s own narrative, appealing to the fact that people are given more of a ‘control-right’ over their own personal data and therefore their identity (2017:645; Ausloos, 2012:144). The concept of a ‘fresh start’ on the internet is not new, but was proposed already in 2008 by Jonathan Zittrain under the name ‘reputation bankruptcy’ (Ausloos, 2012:144). Although there is some overall agreement on the shift of control towards the end-user and a provision of autonomy, self-determinism, liberty and identity in an over-digitalized world, many scholars are concerned about the practical issues and applicability of such right in a

The biggest problem constitutes the overall perception that deletion from the internet is hard, if not impossible, and may result in data simply being harder to find, copied or anonymized, rather than erased (Meeks, 2016:1-2; Calder, 2016:42; McKay, 2017:501; Ausloos, 2012:144). The resulting question McKay poses is “how to maintain the benefit of uncensored data while simultaneously reducing privacy harms?” (2017:544). Yet, it is not the task of the data controller to delete the information itself, but the link connecting to it, meaning the information can still be found on the web by other means of research. The notion of deletion online has to be considered within a global context. At the moment, Russian politicians are more than willing to edit the internet and they have already done so in 2016, when they enforced a new law that requires search engines to delink information which is ‘inaccurate and dated, [or] which has lost meaning’ without mentioning Freedom of Expression rights (Brock, 2016:10). The Center for Media Rights in Russia has noted that the law may be incompatible with the European Convention of Human Rights (ibid.). Further, the US does not have privacy law at all, although legal actions concerning data protection are possible (ibid.). These are just two examples that draw the importance of the protection of personal data onto a global level, emphasizing that not every state values the same rights as Europe.

Moreover, Zanfir (2015:235), Bernal (2014), Ripoll Servent (2017) and Lee (2016:544) see difficulties for companies in the decision-making process when applying the Right to be forgotten to delisting demands as well as the extreme financial and time-consuming burden to individually assess every request. On the other hand, there need to be guidelines and transparency for search engines in order to not over- or under-reach compliance when assessing delisting requests (Jit Singh Chima, 2016:4). Lastly, the Streisand effect by which the attempt to hide information only draws more attention to it, is a very common side effect of making use of the right (McKay, 2017:545). It was named after Barbara Streisand whose attempt to suppress photographs of her Malibu Home resulted in extensive publicity (The economist, 2013). The overall discussion focuses on the question if the Right to be forgotten is rather censorship in the guise of privacy, if there will be a clash with the Right to Freedom of Expression as a fundamental right and how the rapidly developing online world will challenge the right’s effectiveness. The analysis will explore whether these concerns are also prevalent throughout online discourse as well and how the right will most likely shape future data protection legislation.
4. Theoretical Framework

4.1 Digitalization and Privacy Theory

Privacy in the digital age has become a very sensitive topic with grey zones and loopholes that allow organizations such as Facebook or Google to perform their business without any strong restrictions. According to Couldry and Hepp, digitalization can be related to the computer and digital media but also to the internet, mobile phones and the increased embeddedness of computer-based ‘intelligence’ in everyday life through all of which data is freely exchangeable (2017:37). Search engines have gained increased power in the internet. With Google’s indexing algorithm, it has built a recursive process meaning with each new link, the data was increased over which they ran their calculations which in turn increased the mechanisms power infinitely (Couldry & Hepp, 2017:45). This mechanism enables Google to transform their search engine into a robust commercial platform which opened up for a marketization of online space (ibid.).

Related to digitalization is also the shift in business models, especially within marketing, towards the effective targeting of specific audiences by personalized tracking (Couldry & Hepp, 2017:45). With these promising achievements of digitalization also come controversial topics such as privacy related issues. “Privacy is now less a line in the sand beyond which transgression is not permitted, than a shifting space of negotiation where privacy is traded for products, better services or special deals” (Haggerty & Ericsson, 2000 in Altheide, 2014:117). As Schneier points out, the belief of the people to receive free services is the driving force for online platforms to make their profit with the data individuals voluntarily provide about themselves (2015:4). Within normative theory, Westin defines privacy as the claim of individuals to determine themselves what, how and to what extend their share information about themselves (1967:7). Although this approach seems very suitable, it needs to be considered that it was developed already 50 years ago. The theoretical premise, however, still is fundamental to this research, yet with digitalization, automization, Web 2.0 and extensive data storage as only a few components of today’s digital world, a rethinking of his theory might be necessary. The concept of sociality as mentioned by Schneier (2015:4) plays a role within privacy discourse. As humans are social animals, their need for communication and connection to others could override their wish for privacy which could imply a restricting effect on data protection. Moreover, awareness about legal
possibilities for individuals is necessary in order for legal framework such as the GDPR to be effective.

In the following chapter a brief list of topics that will most likely be present in the data is provided as a framework and theoretically informed approach for this thesis.

4.2 A theoretically informed approach

This research is based on a theoretically informed inductive analysis, guided by a number of theoretical ideas and assumptions on what to find in the data. These assumptions were made before and at the very beginning of data collection and during literature research. Moreover, my personal stance in social media advertising has contributed theoretical ideas of what the online discussion on the Right to be forgotten and data protection in general will most likely be about.

As a first idea, the concept of security and the protection of personal data are of major interest, as an overarching umbrella covering more concrete ideas. As Ariadna Ripoll Servent states, the European courts will now have to find a balance between security and liberty as fundamental rights (in Schünemann & Baumann, 2017:11). The relationship between data protection and security, or better cybersecurity, have led us to a clash of values, or more explicitly, into a mere dilemma of freedom versus security. Accordingly, digitalization will play a role since this is the main reason for a new regulation demanding a new form of data protection. Every society in today’s world is based on the exchange of personal data and thus, the protection of such is more about the rules and options regarding the transmission and use of it and, currently, about control and decisional power of individuals over their own, personal information (Schünemann & Baumann, 2017:2). Since the new regulation is implemented throughout all European member states, the concept of Europeanization has been mentioned by Schünemann and Baumann. The former Directive 95 has established relatively high norms of data protection on a national level already, but the new GDPR will lead to a unification of data protection law on a European level rather than on a national level. As a result, two logics, or roots, have emerged over time that have created tension. The ‘economic’ logic which is concerned with the negative effects on individual privacy which led to the ‘constitutionalization of data protection as a fundamental right in Article 16 of the TFEU and Article 8 of the Charter of Fundamental Rights. It is concerned with the single market, which ignores privacy as a right (Jones, 2016:75) and protecting economic liberties rather than the individual’s security. In this case, the logic is
aiming to protect the economic benefit of data processing “as well as the satisfaction of interest of the public for the access to information” (Azurmendi in Schünemann & Baumann, 2017:25). On the other hand, the ‘security’ logic, and this entails the Right to be forgotten, is more concerned with ensuring the safety of citizens rather than protecting individual liberties and rights, focusing on the security of the individual rather than democracy (Ripoll Servent in Schünemann & Baumann, 2017:11).

Another broader concept is the idea of surveillance. Solove (2006:490) defines surveillance as “the watching, listening to, or recording of an individual’s activities’. Schneier argues that “we are living in the golden age of surveillance”, making the bargain every day to exchange our freedom for ‘free’ services (2015:4). Yet, privacy as a fundamental right is meant to protect us from state surveillance, but knowing how much data the state and every data processor hold about us has a rather intimidating effect. An interesting point Schneier (2015:125) makes is the very dominant misconception of privacy as a problem of having something to hide. Logically, if one is not doing anything wrong, then one does not have anything to hide. Privacy gives us the freedom of choice of how to present ourselves to the world and act appropriately in whatever setting we find ourselves, yet, surveillance strips us of our dignity. Considering that this is a very sensitive topic, I assume this to be directly or indirectly present in the data.

Another point I consider to be relevant is the idea of privacy uncertainty and the underlying problem of the privacy paradox. As mentioned earlier, technological advancements have enabled invisible processing of data, which makes it difficult for an individual to assess what information is gathered and to what degree this process was legitimate. Moreover, as Sobolewski et al. explained, more people are concerned about their privacy status online than people actually taking action to address their concerns (2017:211).

Consequently, one last assumption is concerned with the general need for sociality. Humans are “social animals” with the ultimate need to communicate with other people (Schneier, 2015:4; Acquisti, Brandimarte & Loewenstein, 2015:510). Digitization has provided the easiest and quickest means to communicate. The problem is that, in order to be social, individuals have to abandon to a certain extent their degree of privacy. This happens voluntarily in the pursuit of rewarding social lives but restrains the protection of personal data (Schünemann & Baumann, 2017:78). Additionally, the privacy risk for the people here can be either caused by a lack of knowledge on how to adjust privacy settings online or the “social cost of a reduced presence online” (Paparachissi and Gibson, 2011:83 in Trepte & Reinecke, 2011:83). It is the goal to find a balance between being social and simultaneously
protecting one’s personal information. Accordingly, concerns about people’s actual application of their new data protection rights will be discussed, but also the consequences online marketers draw from the enforcement of the regulation and particularly the Right to be forgotten.

4.3 Discourse analysis

In this section, I will elaborate on the theoretical concepts used in my thesis for the analysis of the empirical data collected. The study is approached from a qualitative social perspective rooted in Norman Fairclough’s approach on critical discourse analysis theory as the most appropriate tactic among social science discourse analysis literature. Moreover, this section will name a number of pre-determined categories and dimensions which are very likely to occur in the texts as overarching concepts and ideas concerning the protection of personal data and the Right to be forgotten in the GDPR.

Fairclough defines discourse as the following:

“I see discourses as ways of representing aspects of the world. Different discourses are different perspectives of the world associated with different relations people have to the world which in turn depends on their position in the world, their social and personal identities and the social relationships in which they stand to other people. Discourses not only represent the world as it is but also represent possible worlds which are different from the actual world.” (2003:124)

According to Fairclough (2003) and Jørgensen (2008), discourse can be “language or particular ways representing parts of the world” or a “particular way of talking about or understanding the world or part of it”. Thereby the authors refer to the active role of creating and changing the world, identities and social relations rather than a neutral reflection of our reality (Jørgensen, 2008:9,15). This is the reason why there is no consensus on defining discourse as such, but there are various suggestions, best applied individually by the researcher. A particular event in time can therefore be approached from many different perspectives or discourses which point to different courses of action (Jørgensen, 2008:18). The question arising from discourse analysis is how to differentiate between discourse and non-discourse, however, when taking Fairclough’s approach, this distinction is not necessary because he sees the discursive practice as just one dimension of the social in a dialectical relationship with other dimensions. A multi-perspectival approach shows how the social
world can be understood and constructed in various ways, proving that things can be different and open for social change. Jørgensen further explains that texts can never be understood in isolation but rather in relation to other texts and social context (2008:71). In my case, all textual sources underlie the bigger context of privacy, more precisely the Right to be forgotten, enshrined in the new data protection regulation in Europe.

4.4 Fairclough’s three-dimensional framework

This study is theoretically based on Fairclough’s three-dimensional framework to understand discourse as both constitutive and constituted, contributing to the “construction of social identities, social relations and systems of knowledge and meaning” (Jørgensen, 2008:68). Fairclough distinguishes between text, discursive practice and social practice as three levels of analysis (Fairclough, 1993:136).

On the textual level, analysis focuses on the linguistic features of the text to explore how discursive processes operate linguistically (Jørgensen, 2008:67). This is the most concrete level which gives meaning to experiences from a particular perspective. However, textual analysis, according to Jørgensen (ibid.) is not sufficient for discourse analysis as it does not “shed light on the links between texts and societal and cultural processes and structures”, which is why the interdisciplinary character of discourse analysis will advance this process.

The second stage involves the discursive practice, which includes the production and consumption of the text and is concerned with identifying discourses and intertextuality, meaning texts that draw on other, previous texts, for instance by citing them. Interdiscursivity and intertextuality are seen by Fairclough as both stability and instability, continuity and change, transforming the past, in terms of existing conventions or prior texts, into the present (Fairclough, 1993:137). Change is created by drawing on existing discourses in new ways. However, the possibilities are limited by power relations which determine the access of different actors to different discourses (Jørgensen, 2008:74). Power and relations of domination are created in society by social structures that form ideologies. “Ideologies are representations of aspects of the world which contribute to establishing and maintaining relations of power, dominations and exploitations” (Jørgensen, 2008:74), defined by a stable and coherent set of beliefs or values that have remained over time; however, it is the ideological discourses that contribute to the maintenance and transformation of power relations (Fairclough, 2003:218 in Wodak, 2008:9; Wodak, 2008:8). Ideology will only play
a minor part in this study, yet, I find it important to mention power relations in the context of privacy and data protection, since control and power over personal data are very relevant under the GDPR legislation.

The third level of analysis is concerned with the social practice. This is the most abstract and most open to interpretation (Jørgensen, 2008:81). Here, I will try to explore the relationship between discursive practice and the broader social practice by addressing questions of social change on how things are or have been or representations of how things might, could or should be in one possible reality. The main aim is to unmask power relations and taken-for-granted understandings of reality with truth, exploring the ongoing discourses on data protection in an over-digitalized world and reveal social consequences.

The first two stages will strongly interact with each other but should be analyzed separately. However, the aim is to connect all three levels by going from a concrete textual analysis to a broader consideration of the discursive and social practice. Textual analysis will be conducted using the principles of qualitative content analysis.

4.5 Critical discourse analysis (CDA)

The aim of this study is to view the problem of data protection and the ongoing discussion about the Right to be forgotten through a critical lens. For Fairclough, “‘critical’ discourse analysis […] mean[s] discourse analysis which aims to systematically explore often opaque relationships of causality and determination between (a) discursive practices, events, and texts, and (b) wider social and cultural structures, relations and processes […] and to explore how the opacity of these relationships between discourse and society is itself a factor securing power and hegemony” (Fairclough, 1993:135). CDA sheds light on the linguistic-discursive dimension of social and cultural phenomena and processes (Jørgensen, 2008:64). Wodak (2008), Jørgensen (2008) and Fairclough (2003) agree on the fact that discourse constitutes the social world and is constituted by other social practices, that language is both determined by a social structure and contributes to stabilizing and changing that structure simultaneously, a form of action through which people can change the world. “Discourse not only reshapes social structures but also reflects them” (Jørgensen, 2008:64). The role of the analyst and researcher is to focus on the discourse itself rather than to find out what people really mean and the reality behind the discourse. It is not about finding out what is right or wrong, but working out what has been said and what the social consequences of different discursive representations are.
According to Fairclough (1993:137), his framework for CDA draws strongly on the concept of hegemony and further is associated with historical change as the primary focus of CDA. Further, the aim of CDA is to contribute to social change by taking the side of oppressed social groups as they aim for more equal power relations in the communication process and in society in general (Jørgensen, 2008:66). According to Jørgensen (2008), the focus lies on the discursive practices which construct representations of the world, social subjects and social relations including power relations and the role that these discursive practices play in furthering the interests of this particular social group, which is characterized by less control and less power. Revealing the social relations that involve unequal power relations is what makes CDA ‘critical’.
5. Methodology

In this chapter I will discuss the methodological choices made and explain why qualitative research is most suitable for my study. As a first step, I will briefly explain the choice for blogs as the only source, followed by a discussion of the benefits of using qualitative content analysis in combination with critical discourse analysis as a mixed methods approach. I will give a theoretical explanation of both methods and explain how I adapted the two to my own study. Providing a description of the applied sampling and coding procedures, as well as an overview of sampling criteria will complete the methodology. Moreover, I will briefly talk about ethical considerations and limitations of the study.

5.1 Data collection - Blogs as genre and Sampling

Since blog posts provide the foundation of this study and the only source of data for analysis, it is necessary to examine the potential of blog posts beforehand. Myers (2010:15) argues that blogs are “texts defined not so much by their form or content as by the kinds of uses to which they are put, and the ways these uses construct social identities and communities”. However, his research does not focus on identity or community, but rather as fact that, according to Myres (2010), blogs offer uncontrolled expression of opinion, which did not exist prior to the birth of blogging. This perception constitutes the foundation for selecting and analyzing blog posts and examining the current approaches and opinions towards the Right to be forgotten. Blogs differ significantly from traditional news media, as they provide an interactive space for bloggers and readers, no matter if they are opposing or agreeing with the expressed opinion.

The answer as to why choose blog post and not any other kind of contemporary news media is a simple one. There are various reasons why blog posts offer a convenient and thus valuable source for analysis. As Webb and Wang (2013:210) argue, the data blog posts provide is constantly available on the internet, allowing the researcher to download data almost instantaneously, with no investment of capital and no preparation or training for interviews. Furthermore, blogs are contemporary, providing fresh data and also allowing the researcher to analyze interactions between readers, including their responses to opinions. However, these are merely practical aspects, the main reason for choosing this genre lies in its functioning as a tool for the free expression of opinion.
The sampling procedure itself was based on a small scale (±30 textual sources, in this case blog posts) and purposeful or purposive sampling. Patton (2015:264, in Gentles, 2015:1778), and similarly Yin (2011; in Gentles. 2015:1778), provide this description of purposeful sampling: “The logic and power of purposeful sampling lie in selecting information-rich cases for in-depth study. Information-rich cases are those from which one can learn a great deal about issues of central importance to the purpose of the inquiry.” He introduced purposeful sampling as a “specifically qualitative approach to case selection” (ibid.). However, authors largely disagree on what defines purposive sampling; some, like Guba and Lincoln (1985; in Gentles, 2015:1779), argue that “all sampling is done with some purpose in mind” even if it is done by quantitative random sampling. In addition, I used snowball sampling, as intertextuality in the blog posts provides various connections to other bloggers and blog posts which promise to be highly relevant for the study. I consider this method as a part of purposive sampling like Merriam (2009; in Gentles, 2015:1778), but unlike Yin (2011; in Gentles, 2015:1778), who emphasizes the difference among the two.

Snowball sampling underlies the purpose of finding a valuable source on behalf of another relevant source, and even though not all sources found through this method were selected, the method helped identifying less valuable posts, although the relevance score was usually high here. Since it is up to the researcher to define purposive sampling in regard to his or her study, I see it as the most appropriate way of gathering information-rich data. Although convenience sampling sounds indeed very convenient, it may not lead me to the most valuable data sources I am aiming for.

Unlike quantitative research which requires large sample sizes in order to represent populations and draw statistically relevant estimates, qualitative research is used to acquire rich information for the purpose of understanding the depth, complexity, variation and context of a phenomenon which can be done with smaller sample sizes (Gentles, 2015:1782). However, as qualitative methods authors agree, it is hardly possible to determine a sufficient sample size in advance of the study, but rather determine the size according to data saturation (see Gentles, 2015:1782). In order to avoid claiming arbitrary saturation, I selected posts until the information started to overlap and finally new blog posts would not contribute new information to the data. Consequently, data saturation was reached. Data saturation is defined within general qualitative methods literature as “reaching the point of informational redundancy where additional data collection contributes little or nothing new to the study”, a repetition of the same event or story (Gentles, 2015:1781-1782). This is the saturation I am aiming for, unlike theoretical saturation whereby no additional data can be found (Glaser &
Gentles, 2015:1782), which emphasizes the difference to repetition of the same information or story. However, due to the immense number of available posts, theoretical saturation could most likely not be reached. The timing of the sampling procedure is described as ongoing since, other than a priori or initial sampling, where the researcher establishes sampling criteria before entering the field, the exploration of what is said in the blog posts cannot be determined before the researcher enters the field (Gentles, 2015:1784). Yet, a number of theoretical assumptions made beforehand by the researcher guide the sampling process, defining it to be a hybrid, or theoretically informed inductive analysis. The assumptions that were made are defined in the theoretical framework.

In total, I collected around 80 blog posts of which 16 different blog posts by different authors have been selected for analysis, according to the criteria above. The posts have been published on company blogs or business websites of law firms or marketing agencies. The authors are all experts in their field which are, broadly speaking, law, marketing, IT and reporting in the field of privacy. The posts were found on Google search inquiries with the main keywords being “The right to be forgotten”, “GDPR” and “The right to erasure” which have been complemented with “Human rights” or “Marketing” for a more detailed search. The posts have been found in Google’s general search engine as well as its news section. Some posts contained a number of links to other posts or articles on the same topic, which have been considered for selection, and which, in many cases, provided valuable information. Google search inquiries were mainly used to dive into the topic, whereas snowball sampling was used to dig deeper into the field. Moreover, a Google Alert helped informing about the latest news or posts on ‘GDPR’, ‘The Right to be Forgotten’ and ‘Max Schrems’. The latter is an Austrian data protection advocate who has been accusing Facebook of having opaque privacy terms for its users for nearly seven years.

5.2 Data selection criteria

This section will summarize the sampling strategy and procedure I applied in the study. To begin, a frame was set for the sampling that includes selection criteria. These criteria are (1) contemporary publishing, the posts should be published within the last year, meaning from 27th of April 2017 until 04th of April 2018, in order to avoid confusion with the old Right to be forgotten emerging from the 2014 Google Spain ruling, however, an entire exclusion of the former right will not be possible since the new one only emerged due to the old. Ultimately, setting a fixed end-date for sampling was key, as the closer the 25th of May
came, the more content was being produced, which is why the last day of collection was the 10th of April 2018. Even though the frame was set for one year, most posts, except for one, have been published within the last six months. (2) The name of the author should be known and also their identity in terms of their social role and profession, to draw on the relevance of the post and see the perspective from which this opinion derives. The selection of the authors of the blog posts is mainly based on their expertise within their own field which is strongly related to privacy and more specifically to the *Right to be forgotten* in order to establish a credible argumentation. Further, a number of authors, not only of the selected texts but also blog posts which could not be chosen, refer to authors whose texts have been chosen which shows a clear importance of their work to the overall debate. The main fields the authors engage in are IT, marketing, law and writing and reporting. (3) An opinion has to be expressed directly or indirectly on the *Right to be forgotten* in the context of the GDPR. (4) The blog site has to be credible to a certain extent, meaning unreliable sites or private, personal sites, providing vague or not very clear statements were not considered for analysis. (5) The posts have to be written in the English language and be publicly and freely accessible from everywhere in the world. The English language is of importance for the international context the GDPR is placed in, covering all 28 EU member states. In addition, quoting and placing the posts in relation to each other will be much more convenient this way. These criteria I set after collecting the first posts, due to aforementioned obstacles, such as other languages, difficulties in determining credibility of the posts as well as historical relationships and confusion with former legislative acts, which determined these criteria in order to not threaten the credibility of this study.

5.3 Data analysis – (critical) Discourse analysis and qualitative content analysis

Qualitative methods literature provides a rich argumentation on the benefits and constraints of both approaches. In practice, qualitative content analysis is a neutral method of analyzing texts and will serve CDA in this thesis making use of their complementary nature. Qualitative content analysis will be applied to serve the critical analysis of the privacy and *Right to be forgotten* discourse. Both methods combined allow not only the analysis and interpretation of the blog posts on a textual level, but also of the social phenomenon covered by them. Qualitative content analysis is used for the analysis of the texts from a CDA perspective.
CDA has been selected because it goes beyond the examination of texts themselves by linking text and society and viewing the text through a critical lens. Jørgensen argues (2008:9) explains, discourse is “a particular way of talking about or understanding the world or part of it” and creating and changing social relations, identities and the world.

Qualitative content analysis has been selected in order to examine, on a textual level, what the current opinions on the Right to be forgotten are. It is used to enhance an in-depth analysis looking to explore how values, ideologies or motivations appear in the texts. Discourse analysis requires a debate or a number of textual sources whereas CA can come from any textual source, making the combination of the two a very suitable method for this study. However, a crucial requirement for CA is that the coding procedure is sufficiently precise and that the categories are mutually exclusive. Drawing from these categories, the aim is to examine different discourses throughout the texts. One must be aware that from discourse analysis, one cannot draw absolute answers, and there will always be room for interpretation. Thus, discourse analysis allows the problem to be viewed comprehensively.

From an epistemological standpoint, CA takes meaning as reflecting reality, similar discourse analysis which sees meaning as fluid and reality depending on the use of interpretative methods (Banuta, 2015). When considering Fairclough’s views, different perspectives demonstrate that the social world can be constructed and understood in various ways, opening the possibility for social change. Consequently, the meaning of one sentence can differ among CA and discourse analysis. However, both methods mobilize external information about the context and the social environment during analysis in order to fully understand the meanings conveyed, with CA providing a general picture, mapping different themes throughout the posts and discourse analysis drawing on a more interpretative process. (Géring, 2015:19).

Since the aim of this study is to explore the current opinions on the Right to be forgotten in the wider picture, the combination of detailed textual content analysis and the broader discursive analysis promises to be fruitful in finding valuable conclusions on how the Right to be forgotten will influence data protection in the future, according to the authors.

5.3.1 Coding

The coding process was done in two main coding cycles for qualitative content analysis. The coding process helped in ensuring not only sufficient qualitative data, but enough quality data, regardless of the amount of posts (Saldaña, 2008:15). Descriptive
coding was applied as a first cycle process in order to get an overview of topics throughout the posts. Descriptive coding summarizes in a small phrase or single word, mainly a noun, the topic of the passage of text (Saldaña, 2008:70). In some cases, this method was complemented with in vivo coding, which as a code refers to a word or phrase from the actual language found in the data. The in vivo codes “can provide a crucial check on whether you have grasped what is significant” to the participant, in this case the blog post author, and may help “crystallize and condense meanings” and “help us to preserve participants’ meanings of their views and actions” (Charmaz, 2006:55-57; in Saldaña, 2008:75-76). As Saldaña (2008:76) encourages the researcher to use more than one coding method in order to not be limited in terms of the perspective on the data, a perspective that can contribute to a more conceptual and theoretical view of the phenomenon. In addition, in the first coding cycle, value coding was applied in order to grasp a blogger’s worldview and values. “Values Coding is the application of codes onto qualitative data that reflect a participant’s values, attitudes, and beliefs, representing his or her perspectives or worldview” (ibid.). According to Gubrium & Holstein (2009:70, in Saldaña, 2008:92) values are shaped by the individual’s specific biography and historic period of existence, depending on the identity of the blogger, his or her values can differ. However, it is up to the researcher own values to code what is being said in all possible ways.

At the second cycle of coding, focus coding was applied in order to grasp the most frequent or significant first cycle codes to examine and determine which initial code makes the most analytic sense (Saldaña, 2008:155). Additionally, theoretical coding helped to determine the main category, that “appears to have the greatest explanatory relevance” for the phenomenon under study, and link all subcategories systematically to the main (Corbin & Strauss, 2008:104; in Saldaña, 2008:163). Hereby I could determine the main theme of the research and connect all other factors explored in the first cycle coding to it. As Saldaña (2008:166) emphasizes, the main category is not necessarily determined by frequency but rather by quality, as specific in vivo codes may appear rather rarely, there can be a summative power that determines a main category.

5.4 Ethical considerations and limitations

In terms of ethics, the study did not contravene ethical guidance to do harm (Ess at al., 2002:8). All blog posts are publicly available and it is the authors’ choice to provide their names, professions and further information. Due to public availability, there is no need to
provide letters of consent or to confirm anonymity, as it would be necessary in interviews or surveys for instance. Furthermore, no private or sensitive issues are being examined in this study which could cause potential threats to the people being studied. Ironically, the selected data sources are also just part of the digital footprint we leave on the internet, however, the post and personal information were assumingly published knowingly and on purpose, with awareness of potential privacy threats. Floridi made an interesting point:

“My” in “my information” is not the same as “my” in “my car” but rather the same as “my” as in “my body” or “my feelings”; it expresses a sense of constitutive belonging, not of external ownership, a sense in which my body, my feelings, and my information are part of me but are not my (legal) possessions. (2005: 195, in Ess et al., 2011:44)

Putting it as ‘we are our information’, the fact that the authors of the blog posts deliberately published their information online, allows me to use that information in my research without asking for consent of each one of them.

Although there are no ethical concerns, there surely are certainly other limitations to the research. This thesis was designed as exploratory research, as it is based on a very limited number of data sources, further also only belonging to one genre. Advancing the research onto more and also different genres could lead to findings of academic and professional texts which could contribute rich and credible information. Last, conducting this research as an individual project limits the study to the individual analyst relying on her own judgements and interpretation. Further research by several analysts therefore would allow procurement of more reliable results.

5.5 Researcher’s position and role

Taking an objective stance towards a topic is particularly difficult for a researcher who is part of the culture or problem under study, like myself. Although I am not a law student or expert, I engage in digital marketing and targeted advertising and therefore gather specific knowledge on data collection and protection, which is also why this topic is of particular personal interest. However, I will use this research to expand my knowledge on the matter and explore different opinions and facets of the new legislation. Therefore, it is fruitful for to distance myself and view myself as an anthropologist who is exploring a “foreign universe of meaning” (Jørgensen, 2008:28-29). Since CDA does not lead to an absolute answer of the
research question or to a solution of the problem, it is more about finding out how privacy is understood in contemporary Europe and how the *Right to be forgotten* presses for a redefinition or re-shaping of privacy. As Baym (2015:25) noted, technology changes humanity, and therefore technological change leads to different societal worldviews on problems like privacy. I will attempt in exploring the discourse around privacy and the *Right to be forgotten* from an objective perspective and in an exploratory way, rather than trying to give facts or a clear explanation.
6. Presentation and analysis of results

“If the product is free, you’re the product.”

This chapter’s aim is to provide a mere answer to research question one and two. The first research question tries to identify the main issues at stake regarding the Right to be forgotten according to a textual analysis of the blog posts. The second research question aims at exploring how the Right to be forgotten contributes to (re-)shaping data protection and privacy discourse in the future according to the opinions expressed in the posts. Beforehand, a brief analysis of the authors’ identities in terms of their roles is provided to enhance the understanding of the context.

Critical discourse analysis allows us to see a problem from a bird’s eye view to gain a comprehensive understanding by exposing the hidden. Based on Norman Fairclough’s CDA framework (2003), the first research question is aligned with the textual and discursive dimensions and it intends to identify linguistic elements in the texts that express the authors’ opinions and attitudes towards the Right to be forgotten. The second research question is located within societal analysis and focuses on explanations of the findings in the broader social context.

In order to understand the context in which the authors’ arguments develop, it is important to identify different actors. Broadly speaking, there are three kinds of actor groups within the discussion: individuals, organizations and legislative institutions. Individuals are the data subjects, that the GDPR, and more specifically the Right to be forgotten, apply to, empower and safeguard. Organizations are the data controllers and processors, like Google or Facebook, which largely run their businesses by processing personal data. It has to be recognized that by organizations, not only businesses that are deeply engaged in online marketing but also non-profit or public organizations as well as state owned corporations process personal data. However, depending on the character of each, the processing is more or a less a risk to privacy. Hospitals for instance gather vast amounts of data through patient records which are not used for profit making but for research, medical progress and therapy. Even though these kinds of organizations will also have to become more transparent and GDPR compliant, they are significantly less under pressure than platforms like Facebook and Google which are exclusively online. Interestingly, almost all blog posts refer to these companies, as they are the two most dominant data controllers and processors in the world. The legislative actors are policy makers and law professionals with the legislative knowledge and expertise.
6.1 RTBF - Unidentifiable threat or silver lining? – A textual analysis

Blog posts, unlike academic articles or newspapers, typically allow for a very broad usage of language. Colloquialism, slang and all sorts of linguistic elements can be used to express a certain attitude or opinion. The data shows, that most of the selected posts make use of such features; some, however, are written in a rather plain and neutral language. The following part will give an overview on the issues at stake according to the authors and how they are expressed in the texts.

Interestingly, two authors use fairly strong metaphors and analogies to describe the Right to be forgotten, which show a negative connotation. Ellen Tannam (IT security) sees a “deluge of requests” that companies and organizations will have to cope with. A ‘deluge’ usually is something one drowns in, if one is not quick enough or lacks the right resources to safeguard themselves. Christopher Knight (Law) used Disney’s Lion King as an analogy by foreseeing an “approaching dust-cloud of a migrating horde of right to be forgotten litigating wildebeest” by which “like Mufasa, you be crushed underneath an unexpected flurry of developments”. This is the most imaginary linguistic element among all of the texts and it shows very clearly how Knight feels about the upcoming legislative changes. Like Tannam, he also foresees an ‘unknown something’ that looks rather threatening and that, in its appearance and consequences, is very unpredictable from his standpoint a safe distance away.

Moreover, throughout all texts, the authors use modal verbs like “might” or “could” or use expressions as “almost certainly” or “most likely”. Modal verbs are used to express a certain degree of uncertainty. Since these linguistic elements can be found in each text in different ways, a general skepticism and confusion about the Right to be forgotten become apparent throughout the texts. As justification, authors from every of the four fields (Tozer, Green, Fleischer, Hammett, Zylstra and Knight) name the vagueness within the formulation of the legislation text. Expressions such as “muddy waters”, “vagueness” and “confusing aspects” clarify this point. The legislation text, but also the title of the right are causing confusion. According to the GDPR text, the right is firstly called the “Right to Erasure” and only secondly the “Right to be forgotten” (article 17). However, erasure seems to be, for a number of authors like Edwards (Law) and Green (IT), no option in the digital world. Bob Edwards partly titled his post “The right to (almost) be forgotten” referring to data rather being made inaccessible or “quarantined” than actually erased. Daphne Keller (Privacy expert at Stanford University) mentioned the effect that deletion has on the data. The
phenomenon is called Streisand effect and denotes that the attempt to hide information only
draws more attention to it. This is very like to be a common side effect of the application of
the Right to be forgotten.

These textual features are used to express the authors uncertainty about the GDPR in
general and their skepticism about its future influences on privacy and data protection. They
create an imaginary, unidentifiable threat, that concerns society as a whole, including
individuals, businesses as well as democratic values such as fundamental rights, perpetuating
the idea that democracy may be at risk.

Nigel Tozer (IT and marketing director) refers to a “horror story about zombie data”
with businesses finding “it super scary with one of the main challenges being unstructured
data”. For him, there is nothing unknown, but he sees the problem most businesses have:
unstructured data and no expertise in data storage, that will make compliance difficult. He
uses the metaphor a “silver bullet” as protection from evil, referring to effective software
that organizes large data sets. Similar to Tozer, Duncan Hendy, a marketing strategist, speaks
of “a dark cloud of data despair”, however, he sees the GDPR as a “silver lining” and a “boon
for data-addicted marketers”, stressing a more optimistic view on the new legislation.
Similar to Hendy, McDermott (marketing consultant) refers to the Right to be forgotten as
“a carrot on the stick – or perhaps the stick” leading to better practices among businesses.
Further, many authors use adjectives that create a very imaginative impression. Examples
are “a ghostly chill”, “ugly head” or “shivers down the spine” that every reader, experts as
well as non-experts, can relate to, contributing to the expected threatening effects of the new
legislation. Regarding the aforementioned part, these authors agree on the possible threat
arising from the GDPR, but they provide suggestions on how to cope with the unknown and
to overcome potential risks and burdens.

In addition, the term “balance” is used in most of the text. In most cases, it is used in
the context of balancing the Right to be forgotten with the fundamental Right of Freedom of
Expression, as the former is likely to be seen by many authors as undermining the latter. Due
to the permanent mentioning of the term ‘balance’, it becomes clear that the majority of
authors agree on the fact that two fundamental rights, the Right to Privacy and Freedom of
Expression are colliding and will have to be balanced to maintain democratic values.
Moreover, various authors speak of the “digital age” (Freya – writer on privacy) or “digital
society” (Oghia, 2018 – independent researcher and consultant working in the internet
government ecosystem). The word ‘digital’, theoretically, does not make sense in
combination with age or society as these are abstract concepts that do not have any physical
connection to technology. However, both together create a notion of naturalization, and by applying the concept of digitalization onto society and time, an impression of taken-for-grantedness is constructed. Our everyday life revolves around digital technology with devices which are so deeply embedded in it, that it becomes natural to live in a digitalized world.

Another aspect is that the authors (Kaye, Tannam and McDermott) divide data subjects or individuals into two groups. One constitutes “average” people and the other “advocate-type” people. The latter refers to persons like Max Schrems who have knowledge and expertise within the field of data protection and who are trying to bring forward more sustainable legislation, fighting for the protection of individual privacy by prosecuting data giants, like Facebook in his case. Average people are persons without any specific knowledge; the everyday user. One issue here is being raised by Freya when she questions: “How many people actually care enough”? This indicates that not only a lack of knowledge but also of general interest and motivation could influence the implementation of the new law. As mentioned above, the privacy paradox is not just a theoretical concept but also reality regarding the future application of the Right to be forgotten. According to the authors, most people will be concerned about their privacy but few will have the knowledge and motivation to actually change their settings. Privacy uncertainty, as mentioned above, is accompanied by the human need for sociality. The digital world has made communication so simple and convenient that the majority of people are very unlikely to give up their multifaceted social lives online for the sake of their own privacy. Moreover, since technology is deeply rooted in daily life, it becomes difficult to control one’s own data sharing, which raises uncertainty for people in determining what kind and how much data they are sharing at the moment. With the new consent requirement, the privacy terms may become more transparent, but as Freya argued before, it is not clear how many people will actually take responsibility for their own security or blindly trust the online platforms.

One interesting feature is that a number of texts contain links to other texts. This turned out to be positive during data collection and has a logical reason. The authors refer to each other mostly because they agree on something the other author wrote or because they would like to stress specific arguments. Links in blog posts can easily be created as a hyperlink referring directly to the other source, or by direct citations; however, a hyperlink was always included. This feature is called intertextuality. Fairclough (1993) argues that intertextuality can either contribute to the reproduction of, or the challenge to the established status quo. This means that meaning in one text can only be understood in relation to another text and
the context in which it was produced. It can also be used to open up the discussion by bringing other voices into the text (Fairclough, 1992:276). In these cases, intertextuality indeed serves to open up space for other opinions, but mainly in order to strengthen the author’s own argument, referring to experts in the same or different field that hold a similar view.

Lastly, one text is worth mentioning that particularly stood out. It was written by Trevor Zylstra (Marketing) and is based on an interview he conducted with himself. The ironic, or even sarcastic undertone he uses to constitute this dialogue aims at explaining but also critiquing the legislation text, although the language and irony is written for ordinary people to easily understand and critically evaluate. However, by using slang and colloquialism he suggests that his reader should not take it too seriously, since the law has not been implemented yet, underlining the general confusion.

Interestingly, when comparing the texts with the social role of the authors, it already stands out that there are two sides of opinion. Marketers, like McDermott and Hendy, have good hope for businesses when facing the Right to be forgotten challenge. On the other side, writers or lawyers, like Tannam or Knight, have a dystopian perspective on the impact of the GDPR that, in its full extent, will only be visible when it is enforced. However, these authors only represent their personal stance based on their expertise within their field. Marketers will only be able to take on one perspective, that of a data-driven advertiser who has no choice but to adjust his work and behavior according to the new laws in order to maintain his or her profession. Therefore, it becomes clear that they will look for possibilities, chances and remedies. Philosophers like lawyers or reporters are taking the GDPR to another level by relating it to democratic values and fundamental human rights, regarding the security of our society. Both logics are now becoming present within the authors’ perspectives and debates. Marketers are profit and market oriented and will therefore always prioritize the liberties of the free market over individual security, as lawyers and writers would.

6.2 The social perspective

The regulation sets forth stricter rules and broadens the understanding of personal data, territorial scope and the definitions of data controllers and processors. However, there are a number of concerns raised by the authors that affect not only the EU but also the world as a whole. With regard to Fairclough’s three step model for discourse analysis, the discursive practice and the social practice are merged in this chapter.
The most prevalent concern throughout the data refers to the problem of balance. Law experts and writers especially contribute to the discussion by arguing that the Right to be forgotten poses a significant threat to the Right to Freedom of Expression and Information. However, it needs to be considered that, according to the authors, the Right to Privacy as well constitutes a fundamental human right. The problem to solve is that, in order to ensure both rights at the same time, a balance will have to be found between the two. Regarding the ‘economic’ and ‘security’ logic referred to in the theoretical framework, the balance has to be found between safety and liberty. The question that underlines the authors’ arguments is, what is more important: individual privacy and safety or individual liberty and by that also the liberty of the free market. A critical standpoint towards this dichotomy is necessary as it is arguable that the liberty of the free market is equally, or even more important than the liberty of an individual, but both are fundamental for democracy. This will be a question that will have to be applied to each Right to be forgotten case individually and cannot be answered per se, however, this is an essential part of the overall debate on the Right to be forgotten.

One aspect that has been emphasized by David Kaye (Law), United Nations Special Rapporteur for the Freedom of Expression, is that due to the restrictions towards the Right to Information and Freedom of Expression, “creative endeavors” will be limited. The production of creative content will be restricted in a way that comes tremendously close to censorship. With a limited right to Freedom of Expression, areas like journalism will suffer extensively. The internet functions as a global archive for journalists to seek information to perform reporting in the way they do now. Especially with the extraordinary technological progress that took place with the advent of digitalization, the new Right to be forgotten is likely to undermine the achievements made within media development. Setting the Right to be forgotten and censorship equally may be a bit far-fetched; however, the possibility exists and with that also the threat towards democracy and liberalism.

Democracy, even as one of the greatest values in western society, is not a self-evident concept in every country in the world. Oghia, similar to Jones before, gives the examples of Turkey and Russia as countries that could possibly make use of the Right to be forgotten in a rather detrimental way concerning the protection of personal data. Turkey for instance, according to Oghia, is already drafting similar legislative texts but is very likely to disregard freedoms that have been recognized by the CJEU. Russia is already making use of erasing information rather than deindexing and more importantly, does this for ordinary persons as well as public figures. The concept of forgetting is much more dominant in these countries
and disregards multiple individual freedoms and public interest. Wiping out one’s digital past may sound at first glance very tempting to someone with former convictions, but politicians or important public figures who are of major interest to the population will have to be exempted from this in order to establish balance and democratic values like free journalism. Westin’s concept of secrecy comes into play here. As Schneier (2015) also noted, if you are not doing anything wrong, you have nothing to hide. Consequently, he argues, one should consider before the fact that if one does not want past convictions known, one should not commit them in the first place. Yet, this clean slate concept allows for the creation of one’s identity in the most perfect way and has only become possible by technological progress and new legislative forms. In some cases, like Google Spain, old social security debts caused the forced sale of properties for Costeja which were linked to his name on Google search. Costeja is neither a public figure nor has he convicted major crimes, which legitimizes the Right to be forgotten ruling in his case. Further the data was outdated and no longer true, but it still related to his name which could have impacted his job applications or house rentals, for example. Returning to the discussion of Russia and Turkey, there are many countries in the world with governments that will make use of the Right to be forgotten in negative ways. This will raise the level of the discussion about the Right to be forgotten from a Eurocentric point of view to a global level. Europe has the world’s highest privacy principles, setting fairly high standards that challenge the adaption to the GDPR for other, non-European governments. This constitutes a challenge to upholding democratic values and the fundamental human rights which apply globally and for which not only Europe carries responsibility but every state, every business and every person in the world.

However, both, Right to Privacy and Freedom of Expression are fundamental rights which democracies are built on and which allow us to live in peace. However, the risk of different countries applying the new right in their own interpretation and for their own purposes is evidence for different hegemonic structures between society and government in those countries compared to those in Europe, where the security of the individual and the upholding of fundamental human rights are fundamental convictions and given the utmost priority. With these values at risk, public resentment becomes a potential consequence.

Yet, it is no secret that data flows cross international borders. Safe Harbor is meant to protect such data flows at least between Europe and the US. But there still are cases like the Snowden revelations or the very recent Cambridge Analytica scenario where the flow of data is illegal and the current regime data protection is showing loopholes and grey zones. In addition, so-called ‘fake news’ spread rapidly and misinformation poses another threat to
journalism, just as inaccessible information does. The problem is already recognized globally already, but implementation and interpretation of the legal frameworks will differ in different parts of the world.

Regarding illegal data processing and data flows, neither of the blog posts mentioned literally the concept of surveillance. Although the literature suggested that surveillance plays a major role within the privacy discourse, it was not directly of importance to the authors. Schneier argues that ‘we’ tolerate electronic surveillance because it is hidden and less obvious than real-life surveillance would be. Even though the concept of surveillance is not explicitly mentioned by the authors of the blog posts, it constitutes an important part or assumption for the understanding of the digital world and constant data gathering by online platforms as part of the digitalization process. The authors are aware that the technological devices we permanently use constantly gather and process data and that this data is stored and used in an unknown space for an unknown purpose, which evokes the underlying impression of electronic surveillance by platforms, businesses and the state. The tools and rights offered by the GDPR, such as giving one’s consent or being able to access and change one’s digital footprint are, to an extent, only tools that make supervision acceptable and that provide only the appearance of control for the individual. Yet, it lies within the individual’s responsibility to be aware of one’s rights and apply them when in doubt or when illegitimate data processing takes place.

Yet, the new European regulation will have an impact on data protection, but its actual consequences and effects depend on the people’s perception and application of it. As mentioned earlier, the privacy paradox is not a theoretical concept but an actual phenomenon. According to the authors, the Right to be forgotten shifts the power over personal data towards the end user by requiring consent to be given voluntarily and knowingly and by having the right to demand from a data controller all data held on them and the right to have it erased or better, deindexed. However, the near future will show if individuals will use their new legal possibilities in order to change their privacy status and if the GDPR will contribute to overcoming the privacy paradox or if low awareness or lack of interest or general care will remain dominant.

Speaking of power, even though individuals gain more power and control over their personal data, it is now up to the businesses to make legal decisions regarding these requests. However, control means not only power, but knowledge, and with the knowledge Facebook and Co. have about us, the hegemonic relations are rather unequal here, letting the new right be more of a facade to legitimate data processing. Those unequal power structures do not
agree with Westin’s normative theory which seeks for balance, questioning the prevalent ideology of privacy. Epistemologically, ideology has to do with falseness, according to Marx as quoted by Sevignani (2012:605) which points to the fragility of ideological values and a receptivity for change.

Furthermore, balancing the two rights discussed above is now to the responsibility of companies which will face the challenge of making the ‘right’ decisions. Legal consultation will be necessary for these steps to be taken, as well as the, probably minor, but still relevant, fact that emotional empathy could have an influence on decision making. This will be a huge burden to carry as well as a major responsibility. Moreover, a big responsibility will also be the organization of data sets within the companies. Unstructured data will be the most daunting task to take on since requests have to be handled with undue delay, meaning a company will have to know where which data is stored and how to delete it completely, including from all processors as well. Backups will pose a major problem here because, even though they are often necessary for bringing back lost data, that data will now be in multiple copies, haunting businesses. Several authors were mentioning preexisting or beta versions of software that will help businesses to structure as well as anonymize data. As McDermott mentioned, prevention will be more important than compliance.

Regarding data storage, as expected that online marketing will be affected tremendously, with the right data structuring systems, data-driven marketing, according to several authors, will in fact be reanimated. Marketers see a huge opportunity as the customer experience becomes paramount now. Not all the data that is being gathered is also being used, meaning that only with useful and legitimately processed data, will it be possible for marketers to better meet the needs of only interested customers. “Data-driven marketing is not dead” Hendy explained, because data mapping software will be the remedy making structuring and anonymization possible.

However, whether the legislative framework of the regulation will actually affect all these aspects in the foreseen ways will depend on the individuals and their perceptions and usage of the legislation. It has been argued that it will be sometime after the enforcement of the regulation that individuals will start to take action. This is due to the fact that most ‘average’ people are not aware of the change, its new possibilities and threats. Referring back to the privacy paradox, many people would like more privacy but lack the knowledge on how to get there or lack the motivation. With the attention drawn to individual privacy, the privacy discourse now opens new perspectives towards a discussion that arose in 2014,
when the *Right to be forgotten* discourse first came to live, and that grows and shapes a *Right to be forgotten* discourse.

### 6.3 Discussion

When referring back to normative privacy theory by Westin, the GDPR shows the organic structure of privacy, adapting to timely developments and requirements. The authors have shown that there is an overall agreement that the prevalent legislation in the EU and the world concerning data protection is not sufficient anymore due to technological change and the digitalization process. Current lawsuits are evidence for the problem which has become a reality. The cases around Max Schrems and Facebook, where a young Austrian privacy advocate is suing Facebook for providing inadequate and opaque data protection policies, or the very recent Facebook and Cambridge Analytica case, where the personal data of more than 71 million people was ‘leaked’ from the social media platform for the development of “political propaganda campaigns” in the UK and the US (Hern & Bowcott, 2018: www.theguardian.com).

The EU is making a big step by implementing the GDPR with the *Right to be forgotten* which constitutes a challenge for courts as well as businesses, whose overall aim is to make the ‘right’ decisions and practice compliance. However, the expected negative consequences mentioned above will be balanced with positive effects concerning marketing strategies and, more importantly, the increased attention to individual privacy. Prior to this ruling, Europe already had high privacy standards compared to other parts of the world, where fundamental rights are not explicitly protected to the same degree. The GDPR is already reaching out to other states like Russia, whose public figures appear to be very keen on editing their digital footprint, however, it should be the first aim of every state to protect the fundamental human rights which allow us to live in peace and where these values are not protected, public resentment and suffrage are a probable reality, as argued by Jones earlier. Therefore, it is the priority of new legislative changes such as the implementation of the GDPR to protect these values and ensure the continuation of peaceful democracy.

It is arguable that the shift towards the user in regard to control over personal data will turn out to be positive overall, but it is certain that ‘we are our information’ and therefore deserve the power and the knowledge on how to handle our data and privacy. On the other hand, people have a tendency to perfection; leading a perfect life with no flaws and no past convictions, and therefore the aiming for a ‘clean slate’ is an issue that has to be controlled by weighing the *Right to be forgotten* against the Right to Information. This means public
figures and important persons whose lives are of public interest would need to be exempted in order to ensure democratic values like free journalism and the Right to Know. The GDPR takes this issue into account, but other governments will hold different views. However, the necessity of evaluating each request separately, constitutes an enormous burden for businesses and smaller businesses without the necessary financial resources are very likely to suffer especially.

Moreover, even with the knowledge and legal rights to efficiently protect their privacy, it is very likely, according to Freya, that people will not care enough to take necessary steps for the protection of their data, as it could lead to isolation from their social group on online platforms and its informational streams. As noted earlier, humans are social animals in need of communication with other humans. The younger generations in particular happily share information wherever possible to fulfill their urgent need to socialize, blindly trusting those platforms by taking for granted that their terms and conditions will be in favor of their safety. Long and complicated documents explaining the terms of the individual sites are a deterrent for the users which is why they accept them without understanding. The platforms adapted their business models accordingly evoking the impression to provide free services but in reality, personal data has become the prime currency online. In the recent court hearing of Facebook CEO and the Cambridge Analytica case, Mark Zuckerberg played confused when questioned by congresswoman Eshoo if he was willing to change Facebook’s business model in the interest of protecting individual privacy. “Congresswoman, I am not sure what this means” (Dillet, 2018), he said, indicating that it is certainly not an option since data-driven advertisement is how Facebook operates and makes its profit. Moreover, the point was raised, that if Facebook was to change its business model for the sake of data protection, Facebook will become liable to pay costs for its users. This brings us back to paying for services with data or with money, and with taking all the blog posts into account, the overall perception implies that people would be more likely choose their personal data over money, proving the fact that personal data is indeed the online currency to of the digital age.

Taking Taylor et al.’s approach to privacy, that emphasizes the protection of the group, the Right to be forgotten appears rather inadequate because it grants its power only to an individual. Taylor et al.’s logic makes sense in the context of big data where one individual is not the focus anymore but patterns of consumer behavior for instance determine data processing strategies. The idea that an individual can only be protected if the group it belongs to is protected makes more sense in this context, but as noted earlier, the group itself would need to be classified beforehand which constitutes an almost impossible task. Therefore, it
would be too complex to construct a legislative text for the protection of groups, however, the protection of the individual through the *Right to be forgotten* appears insufficient and inadequate in a world of cloud storage and big data. The authors of the blog post did not mention the idea of group privacy in any way but they indicated the problem of big data and the insufficiency of the GDPR and its *Right to be forgotten*. Possibly, since the publication of Taylor et al.’s work was in 2017, the concept is fairly new and has not received much attention yet. Therefore, it provides an interesting approach to privacy that would contribute to the debate and raise new ideas on consequences, effects and suggestions for further research, legislative prospects and compliance.

Moreover, the current concept of data protection is mainly based on informational self-determination meaning individuals decide what data they share, which goes along with normative theory. This allows them to have the power to determine how much privacy they want in their online interactions; however, this non-political approach evokes the assumption that data protection could fall in the responsibilities of self-regulating data processing economies.

Regarding the discourse on privacy and data protection, it becomes clear that discourse is a very flexible concept that can change according to the given circumstances. As Fairclough noted, discourse is the way people see the world and their reality. Due to the significant change in legislation in Europe and the technological advancements that have created our digital world, also the discourse on data protection changes. As Baym noted, technology changes humanity, and therefore technological change leads to different societal worldviews on problems like privacy.

When privacy seemed to be a very general and rather assumed concept and condition, it is now being a lot more critically evaluated by privacy advocates who are raising awareness and warning the public. The assumption that individual privacy is being taken care of by the platforms in the interest of the user has been shaken-up and becoming increasingly questionable. The reality behind these platforms is becoming clearer and this may be frightening for individuals and businesses who now have to reveal what they were trying to hide in their long and complex terms and conditions documents, providing more transparency to the people. However, privacy advocates like Max Schrems alone cannot push forward the debate and therefore the privacy discourse. As a number of blogs have suggested, the media will also need to contribute to raise awareness among society in order for the legislation to be effective and for change to happen.
7. Conclusion

This thesis first sets forth the theoretical background on privacy, the current situation and the upcoming changes in Europe, giving a short summary of what changes the new regulation implies. The theoretical framework is based on Norman Fairclough’s three-dimensional model of discourse analysis as a CDA requirement; the analysis and findings were viewed through a critical lens. After establishing the theoretical premises; the analysis was based on a selection of 16 different blog posts on the Right to be forgotten, aiming to identify discursive and societal implications and understanding the online discourse on privacy and data protection.

Though the GDPR aims at balancing legal frameworks within European borders, it remains to be seen in practice, after the 25th May this year, how this provision is interpreted and applied. As Viktor Mayer-Schönberger noted the GDPR is “two-faced”; “it imposes costs but also structure” (The Economist, 2018) and its tentacles reach far beyond European borders. It will be seen in the near future if the policy makers had this implication in mind, but the GDPR is certainly an attempt to adapt a legal framework to reality and to harmonize the understanding of data protection for both the public and private sector, as it will influence data processing of private businesses as well as public administrations. In this context, the discourse on privacy should be reassessed from the perspective of the impending change that will affect the everyday lives of individuals and businesses. The new Right to be forgotten is, in fact, not so much about forgetting but about editing one’s digital history. The human trait to compare oneself to others as well as the tendency to aim for perfection are characteristics that cannot simply be overcome since it is deeply rooted in our cultural and social habits. The new law is enhancing this perception and enables individuals to a maximally flawless online presence. On the other side, it can be argues that the GDPR was indeed, successful in enhancing individual privacy rights.

This research has been conducted to contribute to the comprehensive understanding of this new legislative act that is fast arriving and its consequences on society, businesses and the broader privacy discourse. However, apart from the limitations mentioned earlier, the time and extent of this thesis were both very limited. Especially as we move closer to the enforcement of the regulation there will be a lot more content being produced in all sorts of genres that would provide interesting grounds for further research from many different perspectives. Especially following up on the Cambridge Analytica lawsuit, the Brexit issue and GDPR for UK citizens as well as taking into account the realization of the Right to be forgotten and its application by the people.
8. References


Sloot, B. van der, Floridi, L., & Taylor, L. (2017). Group Privacy: Philosophical Studies Series 126 (1st 2017). DE: Springer Verlag. Retrieved from http://uu.summon.serialssolutions.com/2.0.0/link/0/eLyHCXMwtrR1LS8Mw-GOPiyD4sseEgeB1TNpka9KDhvkbItLpgcvo48UBtqO2fr7_d10SR0v8OAlaZImhH7-p98r3AKDxulv4AJRMiRekhokeGRcPLmce8xhCWVBFl88cUbHz3zycz-tyjbbd-_Ah77ETSPsf1YywDeLYgc-4xHAEg8Bhv8sWiWfvyV1mm9_AiozafykxeU-J6VVldZnrzMiZ6NLzN6zLFeImVtIBUWm0bvwXip69-mKIQLQyh_ltcNZa6E8jRUzosSRWnrxUrl4LINIYNOIfZkKctkVL8qPceSkUDS2-CM2V9tNfDgv8Il5-Ga1LV-zJQ5Q_G5PZrejV41T1eAeYSh0Ddet3yWGZSLMcviXLBG-7XLfijSedgb2ptOpNhExsSXbj56qQFYJrlB3fWNVZjv9tlf1PDqAh0kPY01k3uhUSPoLdErLdCrLHCuDZz-8f-mapxUepFD1n8-Aj0BFplopT6Ca4DENITTykwGycKNOEHc3wmZP6TBGX52rXS-ffCedwkJ9DKI4W4hEZRFAPVhqn (accessed 23rd April 2018).


Blog Posts


