FACULTY OF LAW

Lund University

Kenny Chung

Eliminating Digital Footprints

An in-depth analysis of the Case C-131/12 Google Spain v. AEDP

JURM02 Graduate Thesis

Graduate Thesis, Master of Laws program

30 higher education credits

Supervisor: Marco Claudio Corradi

Semester of graduation: Fall semester 2017

CONTENTS

SUMMARY

The aim of this thesis has been to analyze the case of *Google Spain v. AEDP*, and the legal impacts of that particular case. One of the most important outcomes of the case was the establishment of the principle of the *right to be forgotten*. The definition of the principle *of the right to be forgotten* is to grant a data subject the right to have his or her personal information deleted and thus, making it inaccessible to a third-party. For a long time, there was a widespread uncertainty about the possibility of this. Because while you enable the protection of integrity for the data subject and protection of his or her personal data by removing content on the internet, you undoubtedly restrict a third-party from imparting information and the public to receive information. The core of the conflict is the clash between two fundamental rights in the Charter; namely the right to private life and protection of personal data versus the right to freedom of expression and information.

This conflict was seen in the case of *Google Spain v. AEDP*, where the Spanish citizen Mario Gonzalez requested Google to delist a news publication about him from their search engines. The Court ruled against Google and stated that there indeed existed a right to have your personal information deleted if certain requirements were fulfilled. In addition, the Court emphasized that the full and complete protection of the Data Protection Directive meant that there should be a broad interpretation of the territorial scope as well as the material definitions in the Directive. However, as the thesis concludes, many of the questions were answered rather insufficiently. Thus, leaving us with inconclusive arguments and unresolved conflicts. The thesis delves into these gray zones as well as circumstances that are entirely exempted from the principle.

Lastly, the thesis analyzes what impact the principle might have within the legal framework of the coming General Data Protection Regulation. The conclusion is that the provision containing the principle will further strengthen and reinforce the rights of the data subjects while at the same time consolidating the right to freedom of expression.

SAMMANFATTNING

Syftet med den här uppsatsen har varit att analysera rättsfallet *Google Spain v. AEDP*, och dess rättsliga inverkan. En av de viktigaste konsekvenserna från rättsfallet är upprättandet av principen *rätten att bli bortglömd* (på engelska: *the right to be* forgotten). Principen innebär att en personuppgiftsregistrerad ska ha rätten att få dennes personuppgifter raderade så att en tredjepart inte längre kan nå personuppgifterna. Under lång tid har det funnits en vidsträckt osäkerhet om möjligheten till denna princip. Anledningen är att skyddandet av en personuppgiftsregistrerads dataintegritet samtidigt kan hindra en tredjepart att dela med sig av informationen och för allmänheten att få tillgång till denna. Kärnan i konflikten ligger alltså mellan de två fundamentala rättigheterna i EU-stadgan; rätten till ett privatliv och skyddet av personuppgifter för individen gentemot rätten till yttrandefrihet och informationsfrihet.

Konflikten visade sig i rättsfallet *Google Spain v. AEDP* där den spanska medborgaren Mario Gonzalez begärde Google att ta bort en nyhetspublikation om honom från Googles sökmotorer. EU-domstolen dömde till Googles nackdel och slog fast att det finns en rätt att få sina personuppgifter raderade om särskilda rekvisit hade uppfyllts. Dessutom betonade EU-domstolen att ett fullgott skydd för de personuppgiftsregistrerade i Dataskyddsdirektivet innebär att de territoriella- och materiella definitionerna måste tolkas brett. Som framgår av uppsatsens slutsats lämnade dock EU-domstolen otillfredsställande svar till många av de ställda frågorna. Detta har vidare lett till gråzoner och olösta konflikter. Uppsatsen ämnar att fördjupa sig i några av dessa gråzoner såväl som situationer där principen om *rätten att bli bortglömd* är helt undantagen.

Slutligen ska uppsatsen analysera vilken/vilka rättsliga konsekvenser som principen möjligtvis kommer att ha inom den kommande ”Dataskyddsförordningen”. Slutsatsen är att principen kommer att fortsätta att stärka dataskyddet för personuppgiftsregistrerade samtidigt som den kommer att upprätthålla rätten till yttrandefrihet och informationsfrihet.

PREFACE

There is a particular moment when you feel that slight shift of change, that sudden realization that your scholarly years might just be coming to their end. For some people, that realization comes at the very end. Maybe at the day they finally hand over their thesis, or perhaps it is the day they defend their thesis with brilliant arguments and wordplay. They pat themselves on the back and look back with pride on what they have accomplished throughout the year.

For me it came at the very beginning, making this thesis a long journey full of procrastination and inhumane efforts to actually get words on paper. Never has it been more important to clean the room, make sure I ate properly and worked out regularly. But even then, rare moments of productivity prevailed, words actually appeared on paper and in the end: it finally got done.

However, this thesis would not have been made possible without the help of some critical people. Therefore I want to give my utmost gratitude to:

My thesis advisor Marco Claudio Corradi for taking time off his busy schedule to provide me with advice on this thesis. Björn, for his unrelenting support and fantastic proofreading skills. I am forever grateful for your feedback. My family, for being there and seeing it through with me until the end. Being able to come home once in a while to recharge my batteries really meant a lot.

Most of all I want to thank my fantastic girlfriend Elizabeth for encouraging and supporting me till the very end. Without you, the lonesome journey of writing an essay would have been lonelier still.

Five years of law school have finally come to its end and now it is time to pursue new exciting projects.

Norrköping, 30 december 2017

Kenny Chung

ABBREVIATIONS

CFREU	Charter of Fundamental Rights of the European Union
Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
DPD	Data Protection Directive
EC	European Community
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EU	European Union
GDPR	General Data Protection Regulation
Google Spain v. AEPD	Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González
Member States	Member States of the European Union
OECD	Organisation for Economic Co-operation and Development
TEU	Treaty European Union
TFEU	Treaty on the Functioning of the European Union
The Court	European Court of Justice
The Directive	Directive 95/46/EC
The Guidelines	The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of the Organisation for Economic Co-operation and Development

1 INTRODUCTION

1.1 Background

Ever since the birth of the Internet, our perception of receiving and imparting information has been revolutionized. Regardless of whether you upload photos on Facebook, share news articles on Twitter or simply message using WhatsApp; the amount of information growing at an ever-steady rate is unprecedented. With this comes the fact that you naturally leave a digital footprint every time you go on the internet, and unlike the human mind, the memory of the Internet is limitless. Thus, everything you ever do has the chance of being stored and recorded somewhere in the realm of the cyber world. For the average person, there might lie a comfort in knowing that the option to delete embarrassing photos or hastily written messages exists.

However, the fundamental question changes whenever a third party decides to share the personal information about you. Suddenly, your digital footprint is imprinted upon you and the rules for deleting that information changes. Here, lies a clash between two fundamental rights: the right to a private life and protection of personal data versus the right to freedom of expression and information. The removal of personal data from the internet means that another person's right to receive and publish that information gets restricted. The *Google Spain v. AEDP* ruling provided some clarity about the extent of *the right to be forgotten.* However, there are many issues still unresolved, and the challenges they pose will be present with the coming GDPR as well.

In our digital age, data protection rules will have an increasingly prominent role to play. While many people have welcomed a more precise position for the principle of *the right to be forgotten* that the case provided, countless other people have voiced concern of a stronger censorship being imposed and of history being rewritten, changing our perception of reality.

1.2 Purpose and research questions

The purpose of this thesis is to research the legal impacts on the data protection legal framework arising from the court case *Google Spain v AEPD*. Furthermore, I will provide clarification to how the coming GDPR might be interpreted in reference to the featured court case.

The following questions will be answered:

- What legal impacts did the court case *C 131/12 Google Spain v. AEDP* have on data protection in regards to existing data protection rules and fundamental rights?
- Which legal circumstances are exempted or lie outside the scope of the principle of *the right to be forgotten* based on the judgment of *Google Spain v. AEPD?*
- How will the new General Data Protection Regulation, with the basis of the court case and of the principle of *the right to be forgotten*, impact future data protection regulation?

1.3 Method and material

The research in this thesis is going to be conducted according to dogmatic legal methods. In this thesis, I plan to focus on EU legislation, case law, preambles, law commentaries, guidelines, preparatory work, legal articles, legal doctrine and general legal principles. The material above, will be used to understand how the legislation concerning data protection and, in particular, the principle of the *"right to be forgotten"* are applied to the European Union and the Member States.

A big challenge with writing about data protection and data privacy is its fast developing nature. The legislation concerning data protection and data privacy is very contemporary compared to that in other legal areas. Therefore,

some of the materials in this thesis will be written articles, blog posts, and other relevant news sources to understand the current legal standpoint better.

Within the area of the principle of the *right to be forgotten,* the case named *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* is the current precedent. Therefore, a comprehensive part of the thesis will be used to describe the case as well as critically examine the legal outcome and consequences with the judgment. Furthermore, the case in question will be analyzed through the lens of both Directive 95/46/EC, the Charter, and the GDPR. In some cases, there will also be mention of articles as well as court cases stemming from the ECHR. The close relationship between the Charter and the ECHR is shown in the following thesis, as both the Court and General Advocates often refer back to rulings made in the ECtHR. Furthermore, according to the explanations to the Charter the articles of 7, 8 and 11 (the articles most relevant for this thesis), correspond to their equivalent provisions in the ECHR.[1] As such, some case-law and articles from the ECHR will be necessary to analyze in order to make a well-reasoned legal thesis. The relationship between the Charter and the ECHR will be further elaborated on in the main text.

Lastly, for the reader to understand the underlying legal mechanisms of current data protection legislation I have provided an overview of the development of data protection legislation.

1.4 Delimitations

There are a lot of overlapping legal topics within the area of data protection. In order not to deviate from this thesis's focus on data protection and data privacy, those other legal topics have been chosen only out of necessity to understand the focus of this thesis. For example, the articles of 7, 8 and 11 in the Charter have their equivalence in the ECHR. These equivalent provisions

[1] Explanations relating to the charter of fundamental rights [2007], OJ C303/02, Article 8 and Article 9.

in the ECHR will only be briefly mentioned when needed to put perspective on the focus at hand. Furthermore, only such articles within Directive 95/46/EC and GDPR that have relevance to the principle and the case of *Google Spain v. AEDP* will be elaborated. The attention will mainly lie on Chapter II in Directive 95/46/EC and Chapter II and Chapter III in GDPR. This means that the case of *Google Spain v. AEDP* will be analysed from an EU perspective only. While the case, in question, is based on EU law as well as Spanish law, the thesis will only elaborate on the issues concerned with EU law. Furthermore, it is important to note that the principle of the *right to be forgotten* as well as the doctrine surrounding it differs a lot from U.S legislation. However, neither U.S legislation, nor U.S case law will be elaborated upon in this thesis.

Lastly, the thesis is written for an audience that already has a basic understanding of the fundamental workings and institutions in the EU. Therefore, the thesis will not delve deeper into these topics.

1.5 Research position

The ruling of *Google Spain v. AEPD* in 2014 established a precedent on the data subject's right to delete their personal data called: *The right to be forgotten*. Within the area of data protection and data privacy, the principle is one of the most widely discussed topics, with articles, blog posts, and research papers being written about it. The outcome of the aforementioned case brought forth an array of public requests that had Google and other search engines delist personal information of individuals from their search engine indexes. However, in the aftermath of the case, there were still some unresolved issues.[2] Furthermore, the General Data Protection Regulation that will enter into force in May 2018 will consolidate the principle into law. It is still to be seen if that will clarify or further complicate the position of data erasure. Research papers, articles and blog posts within Europe as well as

[2] See 3.5.

abroad in the USA, which analyses and explains the topic at hand, are therefore essential contributions.

1.6 Outline

The first part of this thesis will introduce the different legal frameworks that have been in place concerning data protection and data privacy. The second part of this thesis will present the Court case of *Google Spain v. AEDP* with a particular focus on the principle of *the right to be forgotten*. To understand the logic and arguments behind the rulings, first, the Opinion of the Advocate General will be introduced followed by the actual judgment of the European Court of Justice, and lastly, an analysis between the different lines of reasoning of the aforementioned two will be provided. The third part will bring up topics of the consequences and remaining questions arising from the case as well as the instances where the principle of *the right to be forgotten* does not apply. Lastly, the thesis will bring up the upcoming EU-regulation: GDPR, and interpret how the relevant provisions will be implemented and what changes we might expect.

2 The History of Data Protection and Data Privacy

2.1 Introduction

The fast-paced development of society's use of data and information created the need of a new legislative framework governing the data protection and transmission within the EU. The introduction of the Lisbon Treaty brought a new narrative to data protection and the rules governing it. For example, Article 16 TFEU states a right for citizens of the EU to have their personal information protected with the European Parliament and the Council laying down rules that ensure the aforementioned data protection.[3] Article 39 TEU have a similar wording but concerns data processing of personal information by the Member States while dealing with foreign affairs.[4]

Meanwhile, certain data protection features have been established in the EU Charter and hence been given fundamental right status. Article 8 of the EU Charter concerns the protection of personal data for each individual within the EU.[5] The Article has been described as an innovative fundamental right as it introduces the protection of personal data as a fundamental right recognized within the EU. The usage of the phrase "personal data" differs from the previous international instruments and goes beyond the scope granted in the ECHR.[6] For example, whereas Article 8 in the ECHR acts as a right that protects personal data *within* the definition of the right to private life, Article 8 in the EU Charter concerning the protection of personal data is its own Article *separated* from Article 7, which depicts the right to private life.[7] While the Charter, otherwise, remains taciturn about the scope of

[3] Article 16 TFEU.
[4] Orla Lynskey, *The foundations of EU data protection law* (1st edn, Oxford 2015), at 18f.
[5] European Union, *Charter of Fundamental Rights of the European Union* [2012] OJ C 326/02, Article 8.
[6] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014), at 205 ff.
[7] See Article 7 and 8 in the Charter, Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014), at 205 ff.

definition in its Article 8, according to the commentaries and explanations of said article, it draws inspiration from: The Directive, Article 39 TEU as well as Article 8 of the ECHR.[8]

Lastly, it should be mentioned that insofar as the rights of the Charter correspond to the rights of ECHR the meaning and scope should be the same. In essence, this means that there should not be any gaps between the interpretation and meaning of the articles in the Charter and the articles in the ECHR.[9]

2.2 The OECD-guidelines and Convention 108

In 1980, the OECD came out with standard guidelines for data privacy and data protection. The legal framework got the official name: *the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of the Organisation for Economic Co-operation and Development* (hereafter referred to as *the Guidelines*).[10]The aim was to harmonize how data flow could cross borders, and also a response to the many emerging national laws on data protection data privacy (in Sweden, Germany, and France amongst others). The reasons being to reduce the legal obstacles and barriers to transborder data flow that might occur from different national legal frameworks.[11] The Guidelines contained the following objectives:

"(i) to achieve the acceptance of certain minimum standards of protection of personal privacy;
(ii) to reduce the differences between relevant domestic rules and practices in the Member States;

[8] EU Network of Independent Experts on Fundamental Rights, *Commentary of the Charter of Fundamental Rights of the European Union* (2006), at 90ff and *Explanations relating to the charter of fundamental rights* [2007], OJ C303/02, Article 8 – Protection of personal data.
[9] Article 52(3) of the Charter.
[10] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014), at 75.
[11] Orla Lynskey, *The foundations of EU data protection law* (1st edn, Oxford 2015), at 47.

(iii) to avoid undue interference with flows of personal data between Member countries; and (iv) to eliminate, to the extent possible, reasons which might induce the Member States to restrict transborder data flows"[12]

However, the Guidelines were not legally binding and the effectiveness was therefore limited.[13] Regardless, the Guidelines provided the beginning to a new legal framework of concerning data protection and data privacy. According to the Guidelines the data processing of countries would be subjected to eight principles in particular: the collection limitation principle, the data quality principle, the purpose specification principle, the use limitation principle, the security safeguards principle, the openness principle, the individual participation principle and the accountability principle.[14] In this context, it should be mentioned that the aforementioned principles have been implemented into the current legal framework of the Directive and the GDPR as well.[15]

Meanwhile, a debate had started within the Council of Europe on whether Article 8 in the ECHR and the *right to privacy* gave an adequate protection towards the new use of modern scientific and technological methods.[16] The debate concluded in two recommendations adopted by the Council of Europe's Committee of Ministers:

1) "*Recommendation 73 (22)* on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector."[17]
2) "*Recommendation 74 (29)* on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector."[18]

[12] OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Article 25, and Orla Lynskey, *The foundations of EU data protection law* (1st edn, Oxford 2015), at 47f.
[13] Ibid.
[14] See Articles 7-14 of the Guidelines, and Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014), at 80.
[15] See Article 6 in the Directive, and Article 5 GDPR.
[16] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014), at 83.
[17] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014), at 85.
[18] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014), at 86.

Furthermore, a thorough investigation of the Member States' advancement within the area of data protection in regards to their national legislation was conducted.[19] A project group named, *The Committee of Experts on Data Protection* (later renamed *the Project group on Data Protection*) started working on the Convention. This project was later known as *Convention 108*.[20] Convention 108 ensured data protection to be implemented into a legally binding international instrument. In addition, it linked data protection and data privacy to the right of privacy as stated in Article 8 ECHR.[21]

2.3 Data Protection Directive

As earlier mentioned, the importance of legislation concerning data protection and privacy started to gain recognition around Europe in the 1980s. The many Member States had already begun drafting their laws about data privacy and protection.[22] To avoid conflict between national laws across Europe, it became an inevitable topic for the EC as well. In the EC, debates and discussions regarding data protection were held in parallel to the developments happening within the OECD and the ECHR. The European Parliament adopted several resolutions within this period, but stressed the fact that there needed to be a directive from the Commission covering the entire EU.[23]

In 1990, the first key steps toward a directive from the Commission finally took place. Even though Convention 108 was already implemented, the Commission noted that the disparities between the Member States concerning data policies had not been reduced. The Commission feared that this could

[19] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014), at 86ff.
[20] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014), at 86ff.
[21] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014), at 88-89.
[22] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014), at 119ff.
[23] Ibid.

hinder the free flow of information between countries and thus, endanger the integration of the EC.[24] Nonetheless, the coming Directive would have similarities with the objectives of both Convention 108 and the OECD Guidelines.[25]

The two main objectives of the Directive would aim to: *"[…]protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy"*[26] and prohibiting the restrictions to *"[…]the free flow of personal data between Member States[…]."* [27] These objectives serve different purposes. Art. 1(1) aims to protect every person's right to privacy, which bears similarities to Article 8 in the ECHR and Convention 108 about protection of fundamental rights and freedoms.[28] Meanwhile, Article 1(2) concerning the free flow of personal data bears similarities to Convention 108 and the OECD Guidelines about establishing the internal market. This objective is more in conformity with the principles of the EU on free movement.[29]

However, as the nature of directives implies, the Articles within the Directive are only goals that the EU aims to achieve. How the Member States decide to implement them in their laws can differ widely. Furthermore, it explicitly states that the Member States can restrict the rights and obligations set out in the Directive should it be necessary to safeguard specific interests.[30]

[24] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014), at 125.
[25] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014), at 156.
[26] Directive 95/46/EC, Art. 1(1)
[27] Directive 95/46/EC, Art. 1(2)
[28] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014), at 133f.
[29] Ibid.
[30] Directive 95/46/EC, Art. 13.

3 Google Spain v. AEDP

3.1 Introduction

With the advancement of technology, individuals, companies, and organizations store more personal information online. There is no escape from the fact that you, as a user, constantly leave your digital footprints on the web. The stigmatizing effects of past crimes, embarrassing incidents, and past mistakes are recorded for all to see. As will be shown in this thesis, there are legal frameworks and legal precedents that protect rights and freedoms related to personal data. For example, the data subject has a right to, in certain instances, delete their personal data from the internet. The main questions, however, are how far this right extends and how useful its legal properties are in attaining this goal. While I argue that there need to be possibilities to delete your personal information from the web, an unlimited right to do so would cause censorship and infringe upon rights such as freedom of expression.[31]

As mentioned above, the current primary regulation governing data protection is the Data Protection Directive 95/46/EC. The Directive ordains that each Member State passes down national legislation deriving from the requirements stated therein and the paragraphs dictate when personal data may be processed.[32] While there are no explicit paragraphs that indicates that a data subject has the right to delete their personal information, it is however implied in specific paragraphs.[33] The Directive gives data subjects a right to access their data and if appropriate "[…] rectification, erasure or blocking of data […] which does not comply with the provisions."[34] Thus, there are ways in the existing Directive to delete personal information about yourself, and non-compliant companies may be judicially liable for overstepping

[31] Article 11 Charter and Article 10 ECHR.
[32] Michael L. Rustad; Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow (2015)*, 28 Harv. J. L. & Tech, at 359, Directive 95/46/EC.
[33] With the case of Google v. AEDP, the right to be forgotten became established fact. See further below.
[34] Directive 95/46/EC, Article 12 (c)

boundaries on the subject of processing of personal data.[35] The deletion of personal information is especially relevant should the personal data be inaccurate or incomplete.[36]

The following case *Google Spain v. AEPD* is an often-cited case regarding this principle and data subjects' right to have their personal information deleted.[37]

3.2 Background

On the 5th of March 2010, the Spanish resident Mario Costeja González lodged a complaint through the *Agencia Española de Protección de Datos* (hereafter AEPD) about articles published by the newspaper company *La Vanguardia Ediciones SL* (hereafter *La Vanguardia*). The published articles were about a real-estate auction related to attachment proceedings concerning González's recovery of social security debts.[38] In addition, González lodged a parallel complaint against *Google Spain and Google Inc.* for the fact that internet users were able to find the articles on Google's search engine by merely entering his name.[39] González requested that the newspaper *La Vanguardia* would remove or modify the articles so that a third party could no longer see his personal information. Furthermore, he requested that *Google Spain or Google Inc.* should be required to remove or hide personal data about him when entering his name in their search engine relating to the articles published by *La Vanguardia*.[40]

As the case progressed, the first complaint lodged against *La Vanguardia* was dropped as the publication of González's personal information was legally

[35] Directive 95/46/EC, Article 23 and Michael L. Rustad; Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow (2015)*, 28 Harv. J. L. & Tech, at 361.
[36] Directive 95/47/EC, Article 12 (b).
[37] In regards to this thesis's theme, hereinafter only deletion will be addressed within Article 12 (b) in the Directive.
[38] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 14.
[39] Ibid.
[40] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 15.

justified. The second complaint against *Google Spain and Google Inc.*, however, proceeded and was brought before the Court.[41]

The questions asked to the Court were the following:

1) In regards to Article 4(1) of the Directive, how are the definition of *establishment* and "*use of equipment […] situated on the territory of the said Member State"*[42] supposed to be interpreted?[43]
2) In regards to Article 2 of the Directive, is Google processing personal data within the scope of the Directive and if so, is Google to be considered a data controller for personal data? If that is the case, is it possible to directly impose Google to delete personal information from its indexes even if personal data lawfully has been published by a third party?
3) In regards to the principle of *the right to be forgotten*, is it possible for the data subject with the basis of Article 12(b) and Article 14 (a) of the Directive to delete information about himself even if a third party has lawfully published it?[44]

In short, the first question concerned the *territorial scope* of the Directive. The second question was about the *material scope* of the Directive and the last question was in reference to the principle of *the right to be forgotten.*

3.3 The Opinion of the Advocate General

1.) The Advocate General began by stating that at the time the Directive was written, the considerations regarding the internet and online services were not considered. Therefore, the wording seems to be inconsistent and hard

[41] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 16-17.
[42] Article 4 (1) (c) Directive 95/46/EC.
[43] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 20 (1) a-b.
[44] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 20.

to apply to the present circumstances.[45] In this case, a literal interpretation of Article 4 (1) would exclude the application of Article 4 (1) (c) as Google has several establishments within the Member States. Moreover, the geographical location of the processing of personal information in regards to EU citizens by Google's EU subsidiaries is not made available to the public.[46] With this line of reasoning, the Advocate General proposes that the Court should take an approach related to the business model of search engines regarding matters of territorial applicability. In short, the national advertising that is done through Google's subsidiaries should be defined as an establishment within the meaning of Article 4 (1) (a).[47] The Advocate General further marks that the branch, as an economic operator must be considered a single unit. This single unit, however, still processes personal data within the context of a controller's establishment, if the subsidiary acts as a referencing service provider for the advertising market in the Member State.[48] The facts remain the same, regardless of whether the processing operations are situated in the Member States or in third countries.[49]

In summary, all subsidiaries that act as referencing service provider to the advertising markets (within the EU) that Google is in charge of are to be considered establishments that are processing personal data within the context of a controller's establishment.[50] As such, the national web domains of Google such as *google.se, google.es, google.fi* are to adopt the

[45] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 61.
[46] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para 61-62.
[47] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 64.
[48] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 66-67.
[49] Ibid.
[50] Directive 95/46/EC, Article 4(1)(a).

provisions in the Directive pursuant to the national regulations in that Member State.[51]

2.) On the second question, the Advocate General states that it seems quite clear that Google is indeed processing personal information. In short, this is due to Google requesting copies of web pages to be sent to Google that will be analyzed and indexed by Google's search engine function.[52] In the information that Google receives, there might be elements of personal data, which in turn, qualifies Google for processing personal data.[53]

However, the Advocate General reaches another conclusion on the question if Google is to be considered a controller as defined in the Directive. The Advocate General begins by writing that in theory; the concept of the controller could be stretched to an absurd extent. Strictly speaking, even ordinary internet users of the search engine could, in certain circumstances, be considered controllers of this personal information.[54] Thus, he applies the rule of proportionality in establishing if Google, as a search engine provider, qualifies for the role of a controller.[55] The Advocate General interprets that the function of the controller should also contain an element of *responsibility* for the processing of personal data. He means that there has to be an awareness on Google's part that the processed personal information is indeed personal information and that there exists an *intention* in processing said

[51] Directive 95/46/EC, Article 4 (1) (a).
[52] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 73.
[53] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 72.
[54] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para 81 and Article 29 Data Protection Working Party "*Opinion 1/2008 on data protection issues related to search engines"*, page 14 footnote 17.
[55] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para.79.

personal data.[56] To exemplify this, he points to the substantive provisions in Article 6 – 8 of the Directive, which he interprets as requiring the controller to be aware of the purpose of processing personal data.[57]

Hence, a search engine provider such as Google fails the requirements for being a controller. Google, the Advocate General argues, merely acts as a passive intermediary between the actual information provider and the internet user. The Advocate General also mentions the preamble where it is stated that the controller of messages in telecommunication or electronic mail is also the originator of the same messages.[58] Lastly, he makes an analogy to the exceptions of liability in the *e-commerce Directive 2000/31,* which concludes facts concludes that Google must not be liable for their activity.[59] In conclusion, the Advocate General follows the same line of reasoning as the Working Party, and states that the role of a search engine provider that Google has undertaken is not enough to be considered a controller.[60]

2. In the third question, regarding if Article 12 (b) and Article 14 (a) of the Directive constitutes the principle *right to be forgotten,* the General Advocate makes a literal interpretation of the Directive and examines both of the Articles separately.[61] The Advocate General first examines Article 12 (b) and notes that the Article gives a right to erasure *in particular* when the presented personal information is incorrect or inaccurate.[62] Neither the

[56] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 82.
[57] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 83.
[58] Directive 95/46/EC, Recital (47)
[59] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 85, 87 and 89.
[60] Article 29 Data Protection Working Party, *Opinion 1/2008 on data protection issues related to search engines*, page 14.
[61] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para.104.
[62] Ibid.

web pages from which the personal information originated nor Google's index has any such data, and thus he draws the conclusion that the personal information cannot be erased on these grounds.[63] Regarding Article 14 (a) of the Directive, the Advocate General notes that the data subject has to lodge a justified objection before the objection will be heeded. In other words, a balancing exercise between the data subject's interests and the controller and third parties' interests has to be conducted.[64] Since the legal ground for data processing relies on the legitimate interest of the controller, as stated in Article 6(f), the Advocate General notes that the data subject's subjective preference does not alone amount to an overriding legitimate interest that would constitute a justified objection.[65] Conclusively, the General Advocate states that Article 12 (b) and 14 (a) does not provide for a right to be forgotten.[66]

However, he continues by stating that said articles has to be read in the light of the relevant articles in the Charter, namely Article 7, Article 8, Article 11 and Article 16. By making comparisons, to both the ECHR as well as case-law from both the Court and the ECtHR, the Advocate General balances the right to private life against the right to freedom of expression.[67] In the end, he concludes that the internet search engine provider's right to freedom of expression should be given priority over the data subject's right to private life.[68] According to the Advocate

[63] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 105.
[64] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 106-108.
[65] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 108.
[66] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 111.
[67] Article 7 and 11 Charter, Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 128.
[68] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 136-137.

General, being able to search for information using search engines should be considered one of the most critical ways of exercising one's right to freedom of expression and information.[69] Furthermore, the personal information only appears when the internet user types in the data subject's full name in the search engine and, thus exercises his right.[70]

Lastly, he urges the Court not to conduct the balancing exercise of aforementioned conflicting interests on a case-by-case basis. To make a case-by-case assessment would, he argues, both give the internet search engine providers an unmanageable amount of requests from internet users and also move the decision-making process to the search engine providers. These factors would ultimately lead to inadequate legal protection for the data subjects.[71]

3.4 The Judgment

1) Regarding the first question, about the territorial scope of the Directive, the Court answered that although Google Search was handled by Google Inc., Google Spain was still considered a subsidiary to Google Inc. In addition to that, Google Spain has a separate legal personality through its promotion and advertising activity. Thus, it would be viewed as an *establishment* within the definition given in Article 4 (1)(a) in the Directive.[72]

   Furthermore, the Court pointed out the fact that the processing of personal data did not need to be carried out by the establishment but simply carried out in the context of the activities of the establishment according to Article

[69] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 131.
[70] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 130.
[71] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 133-134.
[72] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 46-49.

4 (1) (a).[73] By operating through an establishment in a Member State intended to profit in the advertising market, the connection between the controller and the establishment is enough to make the Directive applicable for Google.[74] Lastly, the Court stressed the fact that the Directive's purpose is the protection of the fundamental rights and freedoms of all individuals. Hence, the definition of the territorial scope in the Directive is meant to be interpreted broadly.[75] The broad interpretation is, in particular, essential for a controller residing in a third country, as that circumstance, should not stand in the way of ensuring natural persons their rights and freedoms.[76]

2) Regarding the second question, the material scope of the Directive, the Court began by defining the interpretation of processing of personal data as stated in Article 2 (b) of the Directive. In its role as an operator of a search engine, Google manages several functions such as retrieving, recording, organizing, collecting and storing personal data. Thus, Google is to be regarded as a processor of personal data.[77] This fact remains, regardless of the fact that other websites may have published the data, in which Google only acts as the intermediary.[78] Hence, the Court answered affirmatively on the question of whether Google would be considered a controller within the definition in the Directive. The reasoning was that Google, as a search engine operator, decides its own *purposes and means* of the processing of personal data it indexes.[79] Furthermore, the undertaking done by the search engine providers, in general, further

[73] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 52.
[74] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para. 55-56.
[75] Directive 95/46/EC, Recital (18-20) and Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 53-54.
[76] Directive 95/46/EC, Recital (20).
[77] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 28-29.
[78] Ibid.
[79] Directive 95/46/EC, Article 2(d) and Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 32-33.

disseminates the already published information by websites.[80] Since the activity by the search engine providers makes the information ubiquitous and facilitates access for internet users, the search engine providers have to comply with the Directive to ensure a full data protection for the data subjects.[81] To have search engine providers excluded from the definition of controller would go against the objective and the provisions of the Directive.[82]

The Court continued by raising the question regarding whether Google needed to delete information from its indexes even though a third party lawfully published it. Article 12 (b) of the Directive gives every data subject a right to delete information about himself or herself, if the data does not comply with the Directive.[83] The Court described the legal ground for processing the personal information of González to be 7 (f), where a balancing of rights and interests between the data subject and controller is required.[84] The Court went on to state that any internet user would have access to the personal information of Gonzalez by merely typing in his name. By indexing the personal information, Google greatly facilitated the accessibility of said personal information and made it ubiquitous.[85] The Court found that the fundamental rights and freedoms of Gonzalez, especially in regards to his privacy, were considered more important than the economic interests of Google and the public in attaining that information about Gonzalez.[86] The importance of the Directive being able to ensure an efficient and complete protection of individuals' fundamental rights and freedoms was emphasized once again

[80] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 36.
[81] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 34, 38.
[82] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para. 34.
[83] Directive 95/46/EC, Article 12 (b).
[84] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 73-74.
[85] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 80.
[86] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 81.

as being central to the Directive. The fact that the publisher was not residing within the EU did not matter.[87]

3) The third question was about the extent of which data subjects may have their information deleted. In this case, the newspaper lawfully published Mr. Gonzalez's personal information, which Google later listed in their search engine. The Court had to answer the question if deletion of personal data was generally to be considered lawful for the reasons that the data subject may face prejudice.[88] One of the main points that the Court brought up was, whether the personal information could be deleted, if the processing did not comply with the Directive as stated in Article 12(b).[89] The Court argued that not only inaccurate information could be erased but also personal information that was inadequate, irrelevant or excessive as stated in Article 6 (1) (c) to (e).[90]

Furthermore, as previously stated, the legality of the processing has to be supported by Article 7 in the Directive. The processing of personal information as done by Google is legitimized on the legal ground stated in Article 7(f) in the Directive. Hence, the balance of interests between the data subject, and the public (including the controller and the third party) has to be weighed against each other. In this particular case, the publication had taken place 16 years earlier, and the sensitivity of the personal information at hand (attachment proceedings for the recovery of social security debts) was deemed more important than the economic interests of Google and the public's right to attain that information.[91] The judgment was a combination of aforementioned factors of being

[87] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 84-87.
[88] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 90.
[89] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 92.
[90] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 94.
[91] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 98.

irrelevant/inadequate, and infringing on the private life of the data subject. The conclusion being that Gonzalez's personal information should be deleted from Google's search engines regardless of whether it caused the data subject prejudice.[92]

However, the Court also stressed the fact that a more public figure may have had a different outcome as the public may have had a more justified reason to access the information about said public figure.[93]

3.5 Analysis of the Opinion of the General Advocate and the Judgement

The opinion of the Advocate General and the ruling from the Court has many dissenting points between the recommendations of the former and the actual turnout. In the following, I will address those different lines of reasoning.

In reference to the first question, both the Advocate General and the Court agrees that Google Spain counts as a subsidiary to Google Inc. with a legal personality. The act of promoting and selling advertising space in a national market is enough to amount to being a controller processing personal data in the context of the activities of the establishment.

In the second question, the Advocate General and the Court agree inasmuch, that Google in its role as a search engine provider does handle the activity of processing personal information. However, the Advocate General and the Court disagree in regards to whether Google should be considered a controller in its role as a search engine provider. The Advocate General mentions that the search engine's sole purpose is to replicate and reproduce personal information from the original provider, thus, only allocating information to be more accessible. Ultimately, Google leaves the content unaltered. Herein,

[92] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 96, 98.
[93] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 97.

the General Advocate claims the rule of proportionality and therefore excludes search engines as being controllers. This view is not shared by the Court, which states that the search engine provider is indeed processing personal data and with that deciding by itself the purposes and means of that very data. [94] Furthermore, the objective of the Directive is to protect natural people's right to privacy concerning the processing of their data.[95] By this line of reasoning, the Court instead makes a teleological approach that prioritizes the complete protection of the data subjects.

As far as my thesis goes, the Court's approach is the correct one. Although the rule of proportionality ought to be implemented, setting the threshold of inclusion too low would make the Directive ineffective in its objective to protect the affected data subjects. This consideration is particularly important when considering that search engines are a significant part of how internet users navigate the web as well as how they find and receive information.

Furthermore, there are two inconsistencies brought up by the Advocate General that are worth mentioning. The Advocate General states that the Directive was drafted in a way that would cover new developments. In the same paragraph, however, he mentions that following a teleological and literal approach of the Directive would not be optimal as the emergence of the internet was a new phenomenon. It might be true that the phenomenon of the internet was unforeseen but from my standpoint, the argument does not suffice to limit the scope of interpretation of the Directive. The nature of the Directive (and legal frameworks in general) is to be applied within an area of constant new developments. Thus, the Directive would have had, as the Advocate General himself mentioned, to take on possible future developments regardless of the extent of them.

[94] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 33. Compare with Article 2 (d) Directive 95/46/EC.
[95] Directive 95/46/EC, Article 1(1) and Article 7 and 8 of the Charter.

The Advocate General also makes a comparison of how making a search engine provider take upon the responsibilities of a controller would equal to making an internet user, owning an electronic device, a controller as well. According to him, processing the personal data in a random manner should not fall within the definition of a controller that determines the *purposes and means* of said information. The same way that an internet user should not be considered a controller simply for downloading a case-file from the internet containing personal information.[96]

In this context, it is important to note that the Directive aims to ensure an efficient and complete protection to data subjects.[97] If an internet-user or a company is, processing personal information related to the data subjects they should not be exempted from the responsibility of that of a controller unless it is mentioned in the Directive.[98] Naturally, as mentioned, there ought to be a reasonable threshold for the application of the Directive. Therefore, it is important to highlight the influence that a search engine provider have. Not only do search engine providers manage an enormous amount of data but they also facilitate data access for internet-users around the world. Neither an internet user nor a third-party news-publishing website could never manage information in the same manner. That being the case, when we consider the difference in capacity between search engine providers and internet users, the comparison the Advocate General makes between the two aforementioned of potentially being controllers, is really underestimating the influence of search engine providers.[99] Exempting search engine providers from the Directive would make it a lot less effective and setting the threshold too high.

[96] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2013] ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para 81.
[97] Article 1 (1) and Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317 para 53.
[98] For example Article 3(2) states that people processing personal information purely for private or household activity should be exempted from the Directive.
[99] See 3.1.2, footnote 50.

With that said, the Court does not comment on the rule of proportionality whatsoever in its judgment. In my opinion, this seems a bit lacking as the Advocate General correctly points out that the Court has chosen the rule of proportionality over the literal and maximalist approach in prior cases.[100] The omitted explanation concerning the application of the rule of proportionality, unfortunately, leaves the legal status regarding the scope of the definition of controllers unknown. Giant search engine providers, such as Google, are considerably easy to recognize and enforce responsibility on for complying with the Directive. However, the legal status concerning other smaller websites that likewise replicates and reproduces information remains unclear. The primary question would be whether a smaller website would be equally responsible regardless of the usage and exposure of the personal information.

Following above-mentioned line of reasoning, would a personal blog, for example, be given the same amount of responsibility? This question was brought up in the case of *Bodil v. Åklagarkammaren i Jönköping.* In the case, Bodil Lindqvist had set up a website on her personal computer which contained personal information about herself and 18 other colleagues.[101] The consent of the colleagues for publishing their personal information was not obtained.[102] One of the questions referred to the Court, concerned whether Bodil Lindqvist's processing of personal information would fall within the scope of Article 3(2) second indentation.[103] The Article states that processing of personal information solely done in private or in the context of household activities are exempted from the Directive.[104] The Court pointed to the preamble and stated that the activities carried out had to be exclusively personal or domestic.[105] Therefore, the publication on the internet that made

[100] Case C-101/01 *Bodil Lindqvist v. Åklagarkammaren i Jönköping* [2003], ECLI:EU:C:2003:596, para. 68.
[101] Case C-101/01 *Bodil Lindqvist v. Åklagarkammaren i Jönköping* [2003], ECLI:EU:C:2003:596, para. 13.
[102] Case C-101/01 *Bodil Lindqvist v. Åklagarkammaren i Jönköping* [2003], ECLI:EU:C:2003:596, para. 14.
[103] Article 3(2) second indentation of the Directive 95/46/EC.
[104] Case C-101/01 *Bodil Lindqvist v. Åklagarkammaren i Jönköping* [2003], ECLI:EU:C:2003:596, para. 29.
[105] Directive 95/46/EC, Recital (12).

the data accessible to a broader public could not be considered to fall within the scope of Article 3(2) second indentation.[106] In the context of personal blogs, publicly accessible content would infer that even smaller websites would fall outside the scope of Article 3(2). In spite of that, these days platforms like Facebook and Instagram provide the user with the option to restrict the accessibility to only include your friends and family. The following question would, therefore, be if a limited online access could be considered to fall within the scope of Article 3 (2)?[107]

The last question concerned the principle of the *right to be forgotten*. Although, the Advocate General argued that there did not exist such a right, the Court went ahead and granted data subjects the right to erase their data based on Article 12 (b) and 14 (a) of the Directive. For Article 12 (b) the Advocate General pointed out that the erasure of the personal data, *particularly,* concerns information that is incorrect or inaccurate. By arguing that the information was neither incorrect or inaccurate, he concludes that Article 12 (b) should not grant the data subject a right to delete his or her data.[108] However, in my opinion, this analysis is insufficient. The wording of the Article reads "erasure […] of data […] of which does not comply with the provisions of this Directive, *in particular* […]."[109] The interpretation of the Article should not exclude other given circumstances in which processing of personal data does not comply with the Directive; even if *particular* attention should be put on personal information being inaccurate or incomplete. As the Court noted, the list in Article 12(b) is not exhaustive.[110] In the judgment, the Court examined Article 6(1) (c) to (e) as well and stated that incompatibility

[106] Case C-101/01 *Bodil Lindqvist v. Åklagarkammaren i Jönköping* [2003], ECLI:EU:C:2003:596, para. 46-47.
[107] Claire Bessant, *The application of Directive 95/46/EC and the Data Protection Act 1998 when an individual posts photographs of other individuals online* [2015], 4.2 The Interpretation of Article 3(2) in Lindqvist and subsequently.
[108] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 105.
[109] Directive 95/46/EC, Article 12 (b)
[110] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para. 70.

with Directive could be a result of being inadequate, irrelevant or excessive.[111]

The Advocate General further discusses Article 14(a) and its requisites, eventually dismissing the application of Article 14(a) as granting a right to erase personal information.[112] According to the Court, Article 14 (a) should be included in the same balancing act as Article 12(b) and can therefore be more specific in finding compelling interests for the data subject's particular situation.[113]

Apart from aforementioned factors, the Court simply states that the circumstances in the current case grant the data subject a right to erase his data as stated in Article 12 (b) and Article 14 (a). Neither the reach of Article 12 (b), nor that of Article 14 (a), is explained further. The omission of said explanation, therefore, leads to my conclusion that both of the articles are given a broad interpretation. This interpretation is partly seen in the Court's judgment where both non-compliance with Article 6 (1) (c) to (e) and non-compliance with Article 7 (f) fits within the scope of Article 12 (b) and Article 14 (a).[114] However, in my opinion, this still leaves questions about the interpretation of the articles. For example, does Article 12 (b) grant a right to delete personal information for all non-compliant processing, no matter how small? Are there situations where the data subject's justified objection grants erasure in Article 14 (a) but not in Article 12 (b)?

Regarding Article 7 (f), the Court and the Advocate General both discuss the balancing of opposing rights.[115] The Advocate General argues that the

[111] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para.92.
[112] Case C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [2013] ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para 106-108.
[113] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para. 76.
[114] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 98.
[115] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para. 74.

public's interest and right to receive information as established in Article 11 in the Charter should be prioritized before the individual's right to private life and data protection in Article 7 and Article 8 in the Charter. However, the Court states that data subject's fundamental right to private life, as a general rule, overrides the economic interests of the controller and the public's interest to access and receive the information. In other words, the Court's conclusion was that there exists a legal presumption that the privacy of the data subject overrides both the controller's and the public's interest to receive information in Article 7(f) in the Directive.

However, as far as my research goes, this judgment of valuing the data subject's right to privacy to such extent is unprecedented in the Court's cases. This case is the first one where the Court declares that there exists a *general rule* in where the fundamental rights of the data subject override the controller's economic interests as well as the public's right to impart information.[116] The Advocate General, as a result of his reasoning, does not indulge in a discussion stemming from that fact but instead regards the two opposing fundamental rights as even.[117]

Lastly, as explained by the Court, the articles in the Directive must be seen in the light of the fundamental rights.[118] In addition, the Court expressed that the data subject's rights as a general rule override the economic interests of the controller as well as the public's right to gain access and receive the personal information. However, the ruling lacked an in-depth explanation on the role of the fundamental rights in reference to the articles in the Directive. Furthermore, in my opinion, the Court does not sufficiently elaborate on how the balance of interest between the two opposing rights should be constructed. This is quite problematic, because, as the Advocate General mentioned in his

[116] For example: See Case C-468/10 *ASNEF* [2011] ECLI:EU:C:2011:777, para. 40.
[117] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2013] ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para.128.
[118] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para. 68 and Case C-465/00 Österreichischer Rundfunk [2003] ECLI:EU:C:2003:294, para. 68.

opinion, to grant data subjects the right to erase personal information from search engine providers would lead to two significant results:

1) The search engine provider would be given the obligation to manage deletion requests from internet users.
2) The matter of deleting personal information would be managed exclusively between the data subject and the search engine provider thus, decentralizing the decision-making obligation to a private party.[119]

By omitting a proper explanation of how the balancing should be done, the Court essentially leaves the decision-making about when to delist personal information to search engine operators, whom will have to second-guess the intentions of the Court.[120] It has further been argued that the lack of elaboration on how to balance the two fundamental rights will ultimately devalue the right that was less discussed; namely the legitimate interests of the public and the controller as stated in Article 11 of the Charter.[121]

[119] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2013] ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen, para. 133-134.
[120] Eleni Frantziou, *"Further Developments in the Right to be Forgotten: The European Court of Justice's Judgement in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos" (2014),* page 770.
[121] Ibid.

4 After Google Spain v. AEPD

4.1 Introduction

After the judgment, Google launched an online form, which gave Europeans the possibility to remove links related to them from the search engine. Specific criteria such as the personal information being *irrelevant* and *outdated* are required in the online form.[122] Following this, Google received requests from citizens all around Europe to have their links removed from Google search engines in the EU.[123] However, while the links might have gotten removed from the search engines in the EU, the search results related to those search terms are still up on the U.S version of Google, and the original publisher's website in question.[124]

With aforementioned information, there remain a few questions concerning the conclusion of the court case of *Google Spain v. AEDP*. It is clear that the personal information in question was not removed in its entirety from the Internet, but merely delisted on Google's search engines. The following instances still provide means for the public to access Mario González personal information:

1) While the search engine operator had to remove any search results based on Mario González's name, the article about Mario González would still be available on the publisher's website.[125]
2) As mentioned above, Google only removed the links to the personal information based on González's name from the search engines in the

[122] Google sets up 'right to be forgotten' form after EU ruling, (BBC, 30 May 2014), http://www.bbc.com/news/technology-27631001.
[123] *Google Is Having Trouble Determining The Legitimacy Of Europe's 91,000 'Right To Be Forgotten Requests*, (Business Insider, 1 August 2014), http://www.businessinsider.com/google-is-having-trouble-determining-the-legitimacy-of-europes-91000-right-to-be-forgotten-requests-2014-8
[124] Ibid.
[125] Article 29 Data Protection Working Party "Guidelines on the implementation of the Court of Justice of the European Union Judgement on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12", page 2 point 4.

EU. It is still possible to search for the original article with González's name on the U.S. version of Google.[126]

With the exceptions mentioned above in place, it is clear that the principle of the right to be forgotten does not apply in all kinds of circumstances. For example, González's side did not proceed with the case of having the publisher *La Vanguardia* take down the article, as it had been published upon the order of the Ministry of Labour and Social Affairs to give maximum publicity to the auction.[127] One may hypothesize what would have happened if the news article had not been under Spanish legislation and hence been required to be published.[128] While the same articles in the Directive would have applied, it is not certain the outcome would have been the same. A daily newspaper and a search engine are in many ways different, and the assessment of the possibility to delete information has to be done in accordance.[129]

The following pages will highlight the material differences between a news-publishing website and a search engine by analyzing the following criteria: *journalistic purposes, level of exposure, and the data subject's recognition in public*. These criteria bear particular importance, as they were mentioned by the Court in *Google Spain v. AEDP* as requisites distinguishing a search engine provider from a news-publishing website and thus, potentially falling outside the scope of *the right to be forgotten*.[130]

---

[126] *Google Is Having Trouble Determining The Legitimacy Of Europe's 91,000 'Right To Be Forgotten Requests,* (Business Insider, 1 August 2014), http://www.businessinsider.com/google-is-having-trouble-determining-the-legitimacy-of-europes-91000-right-to-be-forgotten-requests-2014-8

[127] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 16.

[128] Ibid.

[129] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 86.

[130] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 81-88.

4.2 Journalistic purposes

Article 9 states an exemption of the Directive from "[…] processing of personal data carried out *solely for journalistic purposes* […]."[131] The applicability of the principles in the Directive, if at all, should be determined in a restrictive manner.[132] To judge if the journalistic expression should be exempted, one has to weigh it against the fundamental rights of individuals as laid down in Article 10 ECHR.[133] Because the Directive came into force earlier than the Charter, no referring was made to the latter but instead to the ECHR. However, Article 11 of the Charter states the same thing as Article 10 in the ECHR and according to Article 52(3) of the Charter, the interpretation and meaning should correspond to the articles in the ECHR.[134] While this means that processing of personal data expressed through journalistic purposes can be exempted from the principles in the Directive, there is a need to analyze the content of Article 9 as well as understand what the expression of processing of personal data *solely for journalistic purposes* means.

In the preliminary ruling of *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, the Supreme Administrative Court of Finland referred questions regarding the scope of journalistic practices in Article 9 in the Charter to the Court. The case was about *Markkinapörssi*, transferring personal data containing individuals' tax information to the company *Satamedia* for them to disseminate the information through a text-messaging system.[135] In the case, the Court described the objective of Article 9 in the Directive as to reconcile the fundamental rights of protection of privacy and freedom of expression.[136] Therefore, journalistic activities must be interpreted broadly but not more than necessary for the protection of

[131] Directive 95/46/EC, Article 9.
[132] Directive 95/46/EC. Recital (17).
[133] Directive 95/46/EC, Recital (37).
[134] Article 52(3) of the Charter.
[135] Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECLI:EU:C:2008:727, para 29.
[136] Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECLI:EU:C:2008:727, para 55.

privacy.[137] The Court went on to summarise the content of Article 9 in regards to the processing of personal data *solely for journalistic purposes* like this:

> "[…] data from documents which are in the public domain under national legislation, may be classified as 'journalistic activities' if their object is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They are not limited to media undertakings and may be undertaken for profit-making purposes."[138]

While traditional newspapers, such as *La Vanguardia*, certainly falls under the scope, the Court also opened up for an interpretation with undertakings in other media, particularly referring to the internet.[139] With the internet comes a range of different ways to express and process personal information through social media, blogs and internet forums, etc. Furthermore, the Court clarified that the definition of *solely journalistic purposes* did not preclude an action taken for profit-making purposes as that might often be the result of professional journalistic activity.[140]

However, with the definition mentioned above, there is no difference between a news-article about American politics written in the *New York Times* or an off-handed comment on *Facebook* about Donald Trump's haircut. The question, I hence ask, is whether the journalistic activity should have a certain *quality* to itself. This issue was further elaborated on in the Opinion of *Advocate General Kokott*. As described in the Opinion, the processing of personal information for journalistic purposes is the act of "imparting information and ideas on matters of public interest."[141] The Advocate General further explained the type of communication and the subject-matter that must

---

[137] Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECLI:EU:C:2008:727 para 56.
[138] Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECLI:EU:C:2008:727, para 61.
[139] Directive 95/46/EC, Article 9. Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECLI:EU:C:2008:727, para 60.
[140] Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECLI:EU:C:2008:727, para 58.
[141] Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECLI:EU:C:2008:266, Opinion of Advocate General Kokott, para 106.

be taken into consideration when deciding whether the content is of public interest.[142] The definition of public interest relates to public debate, and matters such as public hearings, the transparency of political life, the conduct of politicians and so on; are all matters of public interests the Advocate General argued.[143] Nonetheless, issues about an individual's private life satisfying only certain readers in the public were not regarded as such. An important factor for deciding whether the content could be seen as being public interest or not have to do with whether the subject has legitimate expectations to have his or her private life respected.[144]

The Advocate General concludes, by stating that it is not possible to ascertain which topics will be considered matters of public interests in advance, and that it is not up to the authorities to determine such issues as that could amount to censorship.[145] With this explanation, a written article in *New York Times* would fall within the scope of Article 9 in the Directive while the latter comment would not.

4.3 Level of exposure and public life

In the case of *Google Spain v. AEDP*, the Court pointed out that personal information that initially had been lawfully processed might become, as time passes, incompatible with Article 6(1) (c) to (e) in the Directive. If that is the case, it would be a legitimate reason to delete one's personal information pursuant to Article 12 (b) and Article 14 (a).[146] These circumstances; the significant intrusion of his privacy and the personal information being published 16 years earlier were reasons enough for the data subject to have

[142] Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECLI:EU:C:2008:266, Opinion of Advocate General Kokott, para. 72.
[143] Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECLI:EU:C:2008:266, Opinion of Advocate General Kokott, para. 73.
[144] Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECLI:EU:C:2008:266, Opinion of Advocate General Kokott, para. 74.
[145] Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008] ECLI:EU:C:2008:266, Opinion of Advocate General Kokott, para 78.
[146] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 93-94.

his search result deleted from Google.[147] The information was just not considered sufficiently relevant to the public when comparing the news value of the personal information to the intrusion of privacy that Mario Gonzalez would be subjected to.[148]

While the relevance of Gonzalez's personal information was the same regardless of it being on Google or in a daily newspaper; it is important to note the difference in exposure between being on a third-party news-publishing website and on international display. The assessment criteria undertaken for a national daily newspaper and a global search engine has to be different.[149] According to the Opinion of Advocate General Jääskinen and the cited case *Volker und Markus Schecke and Eifert*, the Articles 7 and 8 in the Charter apply to any information that is related to an identifiable individual.[150] Therefore, by making the personal information about Mr. Gonzalez significantly more accessible on the search engine, the intrusion of his privacy was also higher.[151]

Referring to the fundamental rights of Article 7 and Article 8 in the Charter, the Court stated that as a rule of thumb these fundamental rights override both the economic interests of Google and the public's interest in partaking that information in regards to Article 11.[152] However, the outcome is ultimately dependent on the actual personal information being processed. For example:

---

[147] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 98.
[148] Article 29 Data Protection Working Party "Guidelines on the implementation of the Court of Justice of the European Union Judgement on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12", page 15.
[149] Article 29 Data Protection Working Party "Guidelines on the implementation of the Court of Justice of the European Union Judgement on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12", page 6 point 7.
[150] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, Opinion of Advocate General Jääskinen, para 117 and Case C-92/09 and C-93/09 *Volker und Markus Schecke und Hartmut Eifert v. Land Hessen* [2010] ECLI:EU:C:2010:662, para 52.
[151] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 87.
[152] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 97.

The nature of the personal information, the sensitivity of the issue for the data subject's private life, and how great of an interest it is to the public to know about the information, all are important deciding factors.[153] The last criterion is of particular interest as it relates to the public life of certain data subjects, whose privacy may consequently be allowed to be infringed to a more considerable extent.

As the Court does not further elaborate on above-mentioned criterion, it is not possible to define exactly what public life the data subject must lead in order for the public to have access to his or her personal information.[154] However, a few legal sources may be able to spread light on this issue. The *Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe* describes a public figure as someone holding public office and using public resources.[155] However, the definition extends even further to people that merely play a role in public life. These people can partake in the economic, the political, and the social or any other public arena.[156] If these people are considered to be playing a public role; information about private details of their lives may be of public interest.[157] In the case of *von Hannover v. Germany (no.2),* the ECtHR argued that a clear distinction had to be made between public figures and private individuals. ECtHR continued stating that the same level of protection of privacy could not be ascertained to a public figure contributing to the public debate or in their exercise of official functions.[158]

The interesting part of unraveling the definition of public life is that it seems to have some relation to the description of how the expression of journalistic

[153] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 81.
[154] Article 29 Data Protection Working Party "Guidelines on the implementation of the Court of Justice of the European Union Judgement on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12", page 11.
[155] Resolution 1165 (1198), Art. 7.
[156] Resolution 1165 (1198), Art. 7.
[157] Resolution 1165 (1198), Art. 9.
[158] *Von Hannover v. Germany (No.2)* App no. 40660/08 and 60641/08, para 110.

purposes should be interpreted.[159] In essence, according to my research, newsworthy articles that impart information of public interest either are exempted from the Directive, pursuant Article 9 in the Directive, or override the privacy of the data subject in Article 7 (f) in the Directive. In spite of that, it is essential to clarify that there may be a discrepancy to how the definition of matters of public interest may be interpreted in Article 9 as opposed to Article 7(f) in the Directive as the context of assessment is different. While the requisites for Article 9 depend on the public outreach and specific qualities of the journalistic activity, Article 7(f) has to be assessed from a fundamental rights perspective. A published newspaper article that falls outside the Directive in regards to Article 9 may, on the other hand, be infringing on privacy in reference to Article 7(f) when instead published by a search engine.

Notwithstanding the aforementioned facts, it may still be impermissible to reproduce information about the data subject beyond that initial publication. Even if that means that it has reached the public sphere. According to the case of *Aleksey Ovchinnikov*:

> "In certain circumstances a restriction on reproducing information that has already entered the public domain may be justified, for example to prevent further airing of the details of an individual's private life which do not come within the scope of any political or public debate on a matter of general importance"[160]

The citation is corresponding to the earlier discussion of how debates that only interest a particular audience should not be regarded as matters of public interest.[161] In the context of *Google Spain v. AEPD*, the reproduction of Mr. Gonzalez's personal information featured on the Google search engine could have potentially been restricted by invoking his fundamental rights to data

[159] See 4.2.
[160] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2013] ECLI:EU:C:2013:424, Opinion of Advocate General Jässkinen, para 127 and *Aleksey Ovchinnikov v. Russia* App no. 24061/04 (ECHR, 16 December 2010), para 50.
[161] See 4.3.1.

privacy. The arguments would have been that the information, displayed on the daily newspaper *La Vanguardia,* was not a matter of public interest beyond the initial publication. While the publication in the Spanish newspaper regarding Mr. Gonzalez's attachment proceedings served a purpose in that they tried to gather as many bidders as possible, the interest of the public may have been limited to the period when the bidding was still on-going.[162] Following this line of reasoning, there would be legitimate reasons not to spread his personal information beyond the initial publication.

4.4 Territorial scope

As mentioned above, Mario Costeja González's personal information continues to be delisted on the search engine platforms residing within the EU. In addition, the accessibility for residents in the EU are restricted.[163] This condition is prevalent regardless of which country's Google search engine provider is used.[164] An example of said situation, would be that an internet user using the Google search engine in Sweden would not be able to access delisted personal information on any search engine, within or outside of the EU.

However, it has been pointed out and made evident that the personal information in question will still be available for an Internet user not residing within the EU on one of Google's many search engines outside of the EU.[165] The same is possible if EU citizens manage to make it seem as though they are doing their search outside of the EU, by hiding their geographical location

[162] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 16.
[163] Peter Fleischer, '*Adapting our approach to the European right to be forgotten'* (Google blog, 4 March 2016), https://blog.google/topics/google-europe/adapting-our-approach-to-european-rig/
[164] Ibid.
[165] Ibid.

from Google (through proxy services for example).[166] This situation naturally puts the effectiveness of the principle of the right to be forgotten into question.

Some countries, among them France, have required that Google apply the principle of the *right to be forgotten* as ruled in the decision from *Google Spain v. AEPD*, not only for search engines within the EU, but also outside of the EU. In other words, these countries have required Google to delist the information on all their search engine-related platforms. As of this moment, the court proceedings regarding the territorial scope of the principle are still underway.[167] The outcome of the case will most certainly affect international companies' interaction with data protection within the EU.

As of now, Google has requested a preliminary ruling from the Court, asking for clarification about the territorial scope of the delisting. The first question is if the delisting involves all the domain names used by Google, regardless of whether the search of the requester's name is conducted outside the territorial scope of the Directive. If that is not the case, the second question delves into the issue whether the delisting should be limited to the Member State from which the request was made and, if so, the delisting should be made on all the domain names for all of the Member States bound by the Directive. The third question asks if the delisting should be done by blocking searches from IP-addresses deemed to be located within one of the Member States regardless of which Google domain name is used.[168]

As the case is in the middle of its process, there is no way of knowing the result of the preliminary ruling. However, it may be possible to get a hint by analyzing the current legal standpoint. In the case of *Google Spain v. AEPD*, on the topic of whether the Directive was applicable under Article 4 (1) (a),

---

[166] Alex Hern, *'Google takes right to be forgotten battle to France's highest court'* (The Guardian, 19 May 2016), https://www.theguardian.com/technology/2016/may/19/google-right-to-be-forgotten-fight-france-highest-court

[167] Ibid.

[168] Case C-507/17 *Request for a preliminary ruling from the Conseil d'État (France) lodged on 21 August 2017 — Google Inc. v Commission nationale de l'informatique et des libertés (CNIL).*

Google argued that Google Spain was merely providing advertising support to Google Inc., hence not partaking in any processing activity done by Google Inc.[169] However, among other things, the Court argued that it was not necessary for the actual processing to be done by the establishment itself, namely Google Spain. It was enough that it was done in the context of the processing activities by the establishment.[170] Furthermore, an essential purpose of the Directive is the use of non-restrictive personal processing activity pursued by the Directive.[171] The Court underlined the fact that the main processing activities of a company being carried out in a state outside the EU, should not be a factor which renders the Directive inapplicable. Otherwise, it would have been ineffectual and easy to circumvent.[172]

This conclusion is shared by the Opinion of the Working Party, which states that there are still circumstances under which the Directive will be applicable even if the controller is a non-European Economic Area-based controller. However, the establishment of the controller has to be exercising real and effective actions in the processing activity in regards to the controller. Furthermore, these establishments can be local offices, subsidiaries with legal personality, etc. The requirements that the processing operations have to be carried out in the context of the activities of the establishment, implies that the actions have to have relevance to the processing activity *per se*. For example: Whether the establishment has user-relations or is involved in advertising to inhabitants of the Member State are two implications that the processing operations are in context with the activities of the establishment.[173]

[169] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para. 51.
[170] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para. 52.
[171] Case C-324/09 *L'Oréal and Others* [2011] ECLI:EU:C:2011:474 para. 62-63.
[172] Directive 95/46/EC, Recitals (19-20) and Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para. 53-54.
[173] Article 29 Data Protection Working Party "*Opinion 1/2008 on data protection issues related to search engines"*, page 9-10.

These legal findings seem to point in a direction where Google will eventually have to universally apply the rules of the Directive to their search engines.

5 General Data Protection Regulation

5.1 Introduction

On the 15th of December 2015, the EU Parliament and Council agreed to the final version of the GDPR. The final version was later adopted, and the date set for enforcement is on the 25th of May 2018.[174]

The implementation of the GDPR succeeds the Directive and is meant to be universally and directly applicable in the Member States.[175] There are several new functions in the GDPR, but most importantly, the GDPR aims to harmonize data privacy laws within the EU, which will naturally bring enormous changes for companies and private citizens alike.[176] The primary purpose of the GDPR is to continue to reinforce data protection and privacy for all EU citizens. Furthermore, in order to make sure that the Member States comply with the new regulation; administrative fines, amongst other things, will be introduced. These penalties could go up to 20 000 000 EUR or 4 % of total worldwide annual turnover for non-compliance and infringements on the data subject's rights, whichever is deemed to be the highest amount.[177]

The GDPR will also consolidate the principle of *the right to be forgotten.* While the principle was already considered controversial prior to the implementation of the GDPR, the consolidation of the right to be forgotten has drawn further criticism from practitioners and private citizens alike.[178] The criticism is multifaceted, but a great deal of concern lies in the fact that companies may feel forced to comply with an erasure request so as not to risk

[174] *GDPR Timeline of Events*, http://www.eugdpr.org/gdpr-timeline.html
[175] Julian Wagner; Alecander Benecke, *"National Legislation within the Framework of the GDPR"* (2016), page 359.
[176] *GDPR Portal: Site Overview*, http://www.eugdpr.org/eugdpr.org.html
[177] Article 83 (5) (b).
[178] Daphne Keller, *The new, worse 'right to be forgotten'* (Politico, 27 January 2016), https://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/

being subjected to the high administrative fines. In turn, this situation would lead to companies erasing personal information upon request without much consideration and thus, result in a higher degree of unwanted censorship.[179][180] In the new Article 17 GDPR, individuals will likewise be able to request that their data be taken down and deleted from those responsible for processing the data.[181] The circumstances, under which the principle is applicable, are established in Article 17 (1) (a-f) GDPR.

5.2 The Right to be Forgotten

Article 17 Right to erasure ('right to be forgotten')[182]

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

[179] Jeffrey Rosen, *The Right to Be* Forgotten (2011-2012), page 90. Daphne Keller, *The new, worse 'right to be forgotten'* (Politico, 27 January 2016), https://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/

[180] Note that the administrative fines described in above article were based on old information. Nevertheless, he considered them as being 'ruinous monetary sanctions'.

[181] Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014), at 246.

[182] GDPR, Article 17.

5.2.1 Article 17 (1) (a) GDPR

Article 17 (1) (a) GDPR concerns the situation when the information of the data subject no longer is relevant, according to the purposes for which the personal data originally were being processed. This situation is also mentioned in Article 5(b) in the Directive where the controller has to state the purpose of the personal data processing.[183] According to the Court in *Google v. Spain*, the Directive grants the right for the data subject to have his or her data deleted should the personal data no longer be relevant. The right to erasure of personal information is applicable even if the personal information concerned might initially have been relevant to process.[184] To ascertain the effectivity of data protection for the data subjects, there is a proposal from the European Commission to *reverse the burden of proof* where it will be the responsibility of the data controller to prove that the information is still relevant for the stated purposes and, thus, should not be deleted. [185]

5.2.2 Article 17 (1) (b) GDPR

Article 17 (1) (b) GDPR concerns the data subject's consent as a legal ground for the processing of personal data.[186] While this means that the data subject has agreed to let the controller process his or her personal information, a withdrawal of the consent means that the legal ground for processing the personal data disappears. Hence, the personal information has to be erased upon request from the data subject.[187]

The equivalent Article of processing based on the data subject's consent can be found in Article 7 (a) in the Directive. The conditions of a valid consent are that it has to be "[…] freely given, specific, informed and [an]

[183] GDPR, Article 17 (1) (a), Article 5 (b).
[184] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 93-94.
[185] European Commission, *Factsheet on the "Right to be Forgotten" ruling (C-131/12)*, page 3.
[186] See Article 7 (a) GDPR.
[187] Article 17 (1) (b) GDPR.

unambiguous indication of the data subject's wishes […]."[188] While the definition of consent seems to be mainly the same in the new Regulation as in the Directive, the conditions for consent in the new Regulation has been strengthened.[189] In addition to the definition of consent above, there are further conditions for the data subject's consent to be valid as stated in Article 7 GDPR. For example, the controller should be able to prove that the consent has been given.[190] Furthermore, the request for consent should be distinguishable from other matters and presented in a clear and easily accessible form.[191] Lastly, withdrawing one's consent should be as easy as to give the consent in the first place.[192] The Article has been added to prevent long unintelligible terms and conditions from the requesting party.[193]

5.2.3 Article 17 (1) (c) GDPR

Article 17 (1) (c) GDPR gives the data subject a right to object to the further processing of his/her personal information.[194] This Article, in turn, refers to Article 21(1), which states that the data subject can object to processing that is not necessary for the legitimate interest of the controller or a third party based on the legal grounds of Article 6 (d) and Article 6 (f) GDPR. Article 21 (1) has its equivalence in Article 14 (a) in the Directive which is based on the processing of personal data done according to the controller's interests.[195] If there are no overriding interests based on Article 6 (d) or Article 6 (f) GDPR, the processing shall cease. My interpretation is that Article 17 (1) (c) together with Article 21 (1) means that any initial processing, as well as further processing, should immediately discontinue.

---

[188] Article 4 (11) GDPR and Directive 95/46/EC, Article 2(h).
[189] *GDPR Key Changes* - "Consent", https://www.eugdpr.org/key-changes.html. Compare Article 4 (11) GDPR and Directive 95/46/EC, Article 2 (h).
[190] Article 7 (1) GDPR.
[191] Article 7 (2) GDPR.
[192] Article 7 (3) GDPR.
[193] *GDPR Key Changes* - "Consent", https://www.eugdpr.org/key-changes.html.
[194] Article 17 (1) (c) GDPR.
[195] Article 21 (1) GDPR and Directive 95/46/EC Article 14 (a). Just like the previous Article in the Directive, the Article in GDPR refers to the legal processing grounds dealing with the controller's or third party's legitimate interests.

Article 17 (1) (c) also refers to Article 21 (2) which deals with situations when data processing is done for direct marketing purposes. Unlike Article 21 (1) there is no need to override a legitimate interest from the controller or a third party, a simple objection from the data subject is enough.[196] When the data subject has objected to data processing pursuant to direct marketing purposes, such processing of personal data has to cease.[197] In reference to processing done for direct marketing purposes, the data subject receives a particular reliable data protection.[198]

5.2.4 Article 17 (d) to (f) GDPR

Article 17 GDPR introduces a few more legal grounds on which it will be possible for the data subject to erase their personal data. Article 17 (d) and (e) GDPR both have to do with the lawfulness of the processing. If it is unlawful or not in compliance with Union or Member State law the data subject has a right to oblige the controller to the erasure of such personal data.[199] Article 17 (f) GDPR concerns the protection of privacy regarding children's personal information. Where personal information regarding children has been collected in relation to the offer of information society services, the data subject, namely the child in question has a right to have it erased. As is evident by the preamble, a child might not be able to realize the risks of having his or her personal information processed.[200]

As far as my research goes, the sole purpose of Article 17(f) seems to be to strengthen a child's right of erasure. Article 17 (f) refers to Article 8 (1) that, in turn, makes the distinction between processing of personal data in relation to the offer of information society services for children over the age of 16 vis-á-vis under the age of 16.[201] In both cases, the consent is the legal ground upon which the processing of personal information will be made legal.

[196] Article 21 (2) GDPR.
[197] Article 21 (3) GDPR.
[198] Compare Article 21(1) with Article 21(2).
[199] Article 17 (d) and (e) GDPR.
[200] Recital (66) GDPR.
[201] Article 8 GDPR.

Although, for children under the age of 16, the consent has to be given or authorized by the parent (holder of parental responsibility). These findings effectually mean that the legal ground for erasure could have been based on Article 17(1) (b), withdrawing consent, instead of having its legal ground in Article 17 (1) (f). For the situation in where a child under the age of 16 has given the consent and where the parents have not been consulted, this would constitute unlawful processing, and the legal ground of Article 17 (d) could be applied to said erasure of personal data. As far as my thesis goes, these legal findings seem to indicate the lawmakers' intention of especially emphasizing the data protection of children.

5.2.5 Article 17 (2) GDPR

The intention of Article 17 (2) GDPR is to strengthen the rights of the data subjects to have their personal information erased.[202] The section in Article 17 (2) urges the controller, which has been requested to delete the personal information, to also inform other controllers to delete any replications, copies or links to said personal data. The obligation to do such, depends on the technical measures and the technology available within reason.[203] This Article did not previously exist in the Directive, and the lawmakers imposes an extended responsibility on the controller to ensure that the data subject's privacy is being adequately protected. However, there are also concerns about the passage being redundant as Article 13 (2) (b) already urges controllers to inform the data subject about erasure requests.[204] Nonetheless, Article 17 (2) seems to put the burden on the controllers to contact each other, instead of having the data subject needing to do the same.

[202] Recital (66) GDPR.
[203] Article 17 (2) GDPR.
[204] European Digital Rights, *Key aspects of the proposed General Data Regulation explained*, page 6.

5.2.6 Article 17 (3) GDPR

The last passage in the Article deals with situations that are exempted from the right to erasure, and which specifies the particular circumstances where *public interest* overrides the data subject's right to erasure.[205] While the situations listed in 17 (3) (b) to (e) states exemptions to specific cases, such as in the area of public health, scientific, historical, archiving and so on, the most compelling exemption is stated in Article 17 (3) (a). The passage in question, concerns exercising the right of freedom of expression and information. As previously noted, this fundamental right conflicted with the right to be forgotten. By providing a separate Article for the principle of freedom of expression, the lawmakers want to highlight the importance of the balance between data privacy and freedom of expression.

Lastly, according to case law, the provisions of the Directive have to be seen in the light of the fundamental rights enshrined in the Charter.[206] Although the GDPR has yet to be implemented, the Court has stated that the Charter embodies general principles of law that must be ensured.[207] Therefore, there should not be any doubt that the GDPR will also follow the same interpretation as the previous Directive.

5.3 Territorial Scope and Freedom of Expression and Information

In addition to Article 17, there are a few Articles in the GDPR that should be mentioned, and which, together with the *right to be forgotten* fortifies the data subject's complete protection.

[205] European Commission, *Factsheet on the "Right to be Forgotten*" ruling (C-131/12), page 4.
[206] Case C-465/00 Österreichischer Rundfunk [2003] ECLI:EU:C:2003:294, para. 68.
[207] Case C-465/00 Österreichischer Rundfunk [2003] ECLI:EU:C:2003:294, para. 68.

5.3.1 Article 3 GDPR – Territorial Scope

The territorial scope of the new Regulation has been changed in order for there not to be any doubt as to whether the Regulation's rules apply. If a non-EU company or search engine offers goods or services to EU-citizens, the laws of the GDPR will be applicable. The rules will apply regardless of where the processing activity is being undertaken.[208] The rewording of the Article seems, amongst other things, to refer to the situation that arose in the case of *Google Spain v. AEDP*.[209] When determining if the controller or processor is offering services to data subjects in EU, there are some deciding factors involved including the use of language, currency, mentioning of customers or users in EU, which may clarify if the controller or processor has to abide by the Regulation.[210]

5.3.2 Article 85 GDPR – Processing and freedom of expression and information

This new Article obliges the Member States to reconcile the protection of personal data with the right of freedom of expression and information.[211] In contrast to above-mentioned articles, this Article presents the Member States with an administrative task of implementing sufficient protection for the right of freedom of expression and information.[212] Member States shall, therefore, establish national legal frameworks that specifically empower the freedom of expression and information, including such processing of information that is carried out for journalistic, artistic, academic or literary expressions.[213]

According to the European Commission, the Article aims to reinforce the freedom of expression and to strike the right balance between the fundamental

[208] Article 3 (2) GDPR, European Commission, *Factsheet on the "Right to be Forgotten*" ruling (C-131/12), page 2.
[209] Ibid.
[210] Recital (23) GDPR.
[211] Article 85 GDPR.
[212] Julian Wagner; Alexander Benecke, *"National Legislation within the Framework of the GDPR"* (2016), page 356.
[213] Article 85 GDPR.

opposing rights as ruled in the case *Google Spain v. AEDP*.[214] This addition eliminates the uncertainty under the previous Directive where personal data protection could be implied to be regarded as more important than freedom of expression, information, and media.[215]

[214] Article 3 (2) GDPR, European Commission, *Factsheet on the "Right to be Forgotten*" ruling (C-131/12), page 4.
[215] Ibid.

6 ANALYSIS & CONCLUSION

In the case of *Google Spain v. AEPD,* the Spanish citizen Mario Costeja González requested Google to erase search results about him stemming from a newspaper publishing two articles about his attachment proceedings for the sake of covering social security debt. The Court assessed several different questions: The matter concerning the principle of a right to be forgotten, the responsibility of a search engine provider and the territorial scope of the Data Protection Directive.

The core question of the case concerned the problematic balancing exercise between fundamental rights within the Charter. The Court responded to the question from a legal standpoint where it gave priority of the data subjects' right to privacy and protection of personal data over the controller's and the public's legitimate interests to impart and receive information. Throughout the case, the objective of the Directive to ascertain a full and complete protection for the data subjects was emphasized. Furthermore, this reasoning meant that the territorial scope of the Directive included controllers, which were outside of the Member States, but had establishments within the Member States. Search engine providers such as Google, were considered to have the responsibilities and liabilities of a controller as defined within the Directive.

While the judgment finally laid to rest questions about the principle of the *right to be forgotten,* there was also criticism of how the judgment lacked depth and only vaguely explained its assessments. For example, the territorial scope of the principle *right to be forgotten*, and its implications for different domain names as well as geographical locations were left untouched. These matters have left Google pursuing the question of whether the Directive would be universally applicable for the delisting of information on all their search engines. This issue could have been resolved, had the Court given

more explicit guidance. Furthermore, the balancing exercise between two opposing fundamental rights was only superficially explained.

As the Advocate General foresaw, the aftermath of the verdict saw Google take on the responsibility to erase personal information from its search engines. With the vague explanation of how the balancing exercise should be conducted, Google has been given insufficient tools to handle requests for delisting personal information. Furthermore, because the delisting will be done in private it may further undermine the representation of the fundamental rights. The establishment of a general rule, that data subject's privacy overrides the freedom of expression, might leave the latter in a disfavoured position, since the Court did not clearly define how to balance the conflicting fundamental rights. One possible outcome is that the precedence for individuals' rights to private life and data protection may limit the right to expression and information, and in practice, further censor published information. Lastly, there still exists questions regarding the extent of the definition of *controller*. While Google was ascribed the responsibilities and liabilities of a controller, the Court did not mention if the same would be applicable for other internet-based entities.

Nonetheless, as explained in this paper, the principle of the *right to be forgotten* does not apply in every circumstance where processing of personal data is involved. There are some possibilities where the principle of *the right to be forgotten*, based on Article 12 (b) and Article 14 (a) of the Directive, would be exempted or overridden based on several factors. The factors presented in this thesis include: If the processing of personal data was submitted for journalistic purposes, the level of exposure and relevance that the information has, and lastly whether the data subject lived a public life. While the first one is an exception to the Directive in regards to the processing of personal data, the latter ones depend on the requisites in each individual case.

When it comes to the GDPR, there are no doubts that the new regulation will have a significant impact on data regulation procedures henceforth. The harmonization of the data protection regulations means that the same rules will bind countries within the EU. To ascertain that non-EU companies offering services or goods to EU citizens (e.g., Google) will have to apply the provisions of the GDPR; Article 3, has been rewritten. The new Article intends to enact certainty about the applicability of the GDPR regardless of the geographical area of the processing. This change is aimed to reinforce the effectiveness of the data protection for individuals, not least when it comes to the *right to be forgotten*. Right now, it is too early to hypothesize how the Court will interpret the principle of *the right to be forgotten* in its consolidated form. Nonetheless, there will be a more significant responsibility for the controller processing personal data, by, for example, needing to contact other controllers.

As far as the criticism goes, not only the principle of the *right to be forgotten* will be consolidated in the GDPR, but this extends to the right to freedom of expression as well. In addition to that, Article 85 aims to strengthen the processing of personal information in different media undertakings by urging the Member States to establish national legal frameworks protecting the freedom of expression. It is yet uncertain, by what means, will these provisions prove the criticism unfounded by assuring companies, and controllers alike, from precipitously deleting data subject's information.

In summary, as has been explained in this thesis, the legal area of data protection is developing fast, and there will undoubtedly, be a continuation of the debate concerning the application of the legal frameworks and principles. This research paper aimed to provide an insight into the principle of *the right to be forgotten* leading up to the GDPR. However, it remains to be seen how the Court intends to apply and interpret the articles in the upcoming GDPR. Hopefully, the Court will manage to strike the right balance between the two opposing fundamental rights.

Bibliography

Electronic Sources

European Commission, *Factsheet on the "Right to be Forgotten" ruling (C-131/12)*, *http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf*, [accessed 30 November 2017].

GDPR Key Changes, https://www.eugdpr.org/key-changes.html, [accessed 1 December 2017].

GDPR Timeline of Events, http://www.eugdpr.org/gdpr-timeline.html, [accessed 30 August 2017].

GDPR Portal: Site Overview, http://www.eugdpr.org/eugdpr.org.html, [accessed 30 August 2017].

EU legislation, opinions and recommendations

Article 29 Data Protection Working Party, *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12* [2014], 14/EN WP 225, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf, [accessed on 10 November 2017].

Article 29 Data Protection Working Party, *Opinion 1/2008 on data protection issues related to search engines*, 00737/EN WP 148,

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf, [accessed 21 November 2017].

Consolidated version of the Treaty on the Functioning of the European Union [2012], OJ C326/01.

Directive 95/46/EC of the European Parliament and of the Council in the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995], OJ L 281/1.

Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular, electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000], OJ L 178/1.

EU Network of Independent Experts on Fundamental Rights, *Commentary of the Charter of Fundamental Rights of the European Union* [2006] http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf, [accessed 31 August 2017].

European Digital Rights, *Key aspects of the proposed General Data Protection Regulation explained*, https://edri.org/files/GDPR-key-issues-explained.pdf, [accessed 30 December 2017].

Explanations relating to the charter of fundamental rights [2007], OJ C303/02, Article 8 – Protection of personal data.

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016], OJ L119/1

Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the right to privacy, Text adopted by the Assembly on 26 June 1998 (24th Sitting), http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16641&lang%20=en, [accessed 10 November 2017].

The European Union, *Charter of Fundamental Rights of the European Union* [2012] OJ C 326/02, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT, [accessed 1 September 2017].

Online Journals

Claire Bessant, *The application of Directive 95/46/EC and the Data Protection Act 1998 when an individual posts photographs of other individuals online* (2015), European Journal of Law and Technology [Online], Vol 6, No. 2, http://ejlt.org/article/view/390/570, [accessed 30 December 2017].

Eleni Frantziou, *Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12" (2014), Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*, Human Rights Law Review, Volume 14, Issue 4, Pages 761–777, https://doi.org/10.1093/hrlr/ngu033, [accessed 16 November 2017].

Jeffrey Rosen, *The Right to Be Forgotten* (2011-2012), 64 Stan. L. Rev. Online 88., http://heinonline.org.ludwig.lub.lu.se/HOL/Page?handle=hein.journals/slro64&div=17&start_page=88&collection=journals&set_as_cursor=0&men_tab=srchresults, [accessed 30 Devember 2017].

Julian Wagner; Alexander Benecke, *National Legislation within the Framework of the GDPR* (2016), 2 Eur. Data Prot. L. Rev. 353., http://heinonline.org.ludwig.lub.lu.se/HOL/Page?handle=hein.journals/edpl

2&div=60&start_page=353&collection=journals&set_as_cursor=2&men_tab=srchresults, [accessed 30 December 2017].

Michael L. Rustad; Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow (2015),* 28 Harv. J. L. & Tech. 349, 418. http://heinonline.org.ludwig.lub.lu.se/HOL/Page?handle=hein.journals/hjlt28&div=14&start_page=349&collection=journals&set_as_cursor=0&men_tab=srchresults [accessed 19 September 2017].

Other legislation

Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, http://www.refworld.org/docid/3ae6b3b04.html [accessed 3 January 2018].

OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, (updated: 2013), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [accessed 2 September 2017].

Websites

Alex Hern, *Google takes right to be forgotten battle to France's highest court*, (The Guardian, 19 May 2016), https://www.theguardian.com/technology/2016/may/19/google-right-to-be-forgotten-fight-france-highest-court, accessed 28 October 2017.

Agence France Presse, *Google Is Having Trouble Determining The Legitimacy Of Europe's 91,000 'Right To Be Forgotten Requests*, (Business Insider, 1 August 2014), http://www.businessinsider.com/google-is-having-

trouble-determining-the-legitimacy-of-europes-91000-right-to-be-forgotten-requests-2014-8 , accessed 12 October 2017.

BBC, *Google sets up 'right to be forgotten' form after EU ruling*, (BBC, 30 May 2014), http://www.bbc.com/news/technology-27631001, [accessed 12 October 2017].

Daphne Keller, *The new, worse 'right to be forgotten'* (Politico, 27 January 2016), https://www.politico.eu/article/right-to-be-forgotten-google-defense-data-protection-privacy/, [accessed 30 December 2017].

Peter Fleischer, *Adapting our approach to the European right to be forgotten*, (Google blog, 4 March 2016), https://blog.google/topics/google-europe/adapting-our-approach-to-european-rig/, [accessed 28 October 2017].

Literature

Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (1st edn, Springer 2014)

Orla Lynskey, *The foundations of EU data protection law* (1st edn, Oxford 2015)

Table of Cases

EU Cases

Case C-465/00 *Österreichischer Rundfunk and Others,* 20 May 2003, ECLI:EU:C:2003:294.

Case C-101/01 *Bodil Lindqvist v. Åklagarkammaren i Jönköping,* 6 November 2003, ECLI:EU:C:2003:596.

Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy,* 16 December 2008, ECLI:EU:C:2008:727.

Case C-73/07 *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy,* 8 May 2008, ECLI:EU:C:2008:266, Opinion of Advocate General Kokott.

Case C-92/09 and C-93/09 *Volker und Markus Schecke und Hartmut Eifert v. Land Hessen,* 9 November 2010, ECLI:EU:C:2010:662.

Case C-324/09 *L'Oréal and Others*, 12 July 2011, ECLI:EU:C:2011:474.

Case C-468/10 *ASNEF,* 24 November 2011, ECLI:EU:C:2011:777.

Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* 25 June 2013, ECLI:EU:C:2013:424, Opinion of Advocate General Jääskinen.

Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* 13 May 2014, ECLI:EU:C:2014:317.

Case C-507/17 *Request for a preliminary ruling from the Conseil d'État (France) lodged on 21 August 2017 — Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, Application (OJ).

ECHR Cases

Aleksey Ovchinnikov v. Russia App no. 24061/04 (ECHR, 16 December 2010)

Von Hannover v. Germany (No.2) App no. 40660/08 and 60641/08 (ECHR, 7 February 2012)