FACULTY OF LAW
Lund University

Sara Andersson

Forget me not?
An exploration of the recent developments in case-law on the right to be forgotten

JURM02 Graduate Thesis

Graduate Thesis, Master of Laws program
30 Higher Education Credits

Supervisor: Eduardo Gill-Pedro

Semester of graduation: Period 1 Autumn Semester 2019

Contents

SUMMARY 1

SAMMANFATTNING 2

PREFACE 3

ABBREVIATIONS 4

1 INTRODUCTION 5

1.1 An introduction to the issue 5

1.2 Purpose and main thesis question 6

1.3 Sub-questions and disposition 6

1.4 Delimitations 7

1.5 Method and material 7

1.6 Terminology 10

What is a search engine and how does it work? 10

What is the processing of personal data? 10

What is personal data and who is a data subject? 10

Who is a Controller? 11

2 THE FOUNDING PRINCIPLES OF EU LAW 12

2.1 Introduction 12

2.2 What are the founding principles? 13

2.2.1 The founding principles are common to the member states 14

2.3 The EU is founded on respect for fundamental rights 15

2.3.1 The Charter can confer obligations to private parties, such as SEOs 16

2.4 The EU is founded on respect for rule of law and democracy 17

2.4.1 Democracy and freedom of expression 19

2.5 The legal structure of the EU 21

2.5.1 Opinion 2/13 and the autonomy of EU law 22

2.5.2 What are the implications of the autonomy of EU law for the member states? 23

2.5.3 The pluralism of the EU legal order 24

2.5.4 The CJEU on the relationship between member states constitutions and EU law 27

2.5.5 When the common EU denominator and a member states' constitutional obligations differ 28

2.6 Conclusion 30

3 THE RIGHT TO BE FORGOTTEN 32

3.1 Introduction 32

3.2 Historic background – Data protection in the EU 32

3.3 C-131/12 *Google Spain*: The CJEU established a right to be forgotten 34

3.3.1 The opinion of AG Jääskinen 34

3.3.2 The CJEU's legal assessment 36

3.3.3 The reactions that followed* Google Spain *37

3.3.4 Article 29 WP issued* Guidelines *40

3.4 The right to be forgotten codified in the GDPR 41

3.4.1 Article 17 of the GDPR: The right to erasure 42

3.4.2 Article 21 of the GDPR: The right to object 43

3.5 What rights and freedoms are especially triggered by a request to be 'forgotten'? 44

3.6 Article 7 and 8 of the Charter: The fundamental rights to privacy and protection of Personal Data 45

3.6.1 Interferences must be provided for by law and be necessary in a democratic society 47

3.7 Article 11 of the Charter: Freedom of expression and information 47

3.7.1 Freedom of expression and information and state interference 48

3.7.2 Access to information and search engines 49

3.7.3 Restrictions on freedom of expression and Information on the Internet 50

3.8 Conclusion 51

4 C-507/17 *GOOGLE CNIL* AND C-136/17 *GC AND OTHERS* 53

4.1 Introduction 53

4.2 C-507/17 *Google v. CNIL*: the territorial scope of the right to be forgotten 54

4.2.1 The opinion of AG Szpunar 54

4.2.2 The CJEU's legal assessment 55

4.2.3 Comments to the case 57

4.3 C-136/17 *GC and Others:* the processing of sensitive personal data 58

4.3.1 The opinion of AG Szpunar 59

4.3.2 The CJEU's legal assessment 60

4.4 Analysis of the cases 64

4.4.1 The EDPB issued Guidelines 64

4.4.2 Comments to the Case 64

4.4.3 Article 85 of the GDPR and SEOs 67

4.5 Conclusion 72

5 CONCLUSION 75

BIBLIOGRAPHY 79

TABLE OF CASES 84
Court of Justice of the European Union: 84
European Court of Human Rigts: 86
Opinions by Advocate Generals of the Court of Justice of the European Union: 87

TABLE OF LEGISLATION 88

Summary

This thesis has examined *the right to be forgotten* – the right to have personal data erased from the search index of a search engine operator (SEO) when requested. The right is fairly new, as it was first established in Case C-131/12 *Google Spain* on 13 May 2014 and was subsequently codified in Article 17 and 21 of the General Data Protection Regulation (GDPR) in 2016. As the right is, more or less, still in its infancy: when the Court of Justice of the European Union (CJEU) on 24 September 2019 published the two cases C-507/17 *Google CNIL* and C-136/17 *GC and others* which further outlined the scope of the right, the anticipation and interest was, to say the least, high.

The scope of this thesis is to explore the implications of the recent development in case law on the right to be forgotten, in the light of the EU's claim to be founded on values of democracy, rule of law, fundamental rights and pluralism; the founding principles of EU law, that must permeate all EU measures, both internally and externally. As shown, the role that the EU has given to SEOs as 'guardians' of both privacy and freedom of expression online may be problematic from the perspective of individual's right to access information and engage in democratic discourse. The complexity of the balancing of rights and freedoms triggered by a request to be forgotten is, in particular, the data subject's right to be forgotten, which is a fundamental part of the right to respect of privacy and human dignity, and the public's right to access information, guaranteed by freedom of expression and information. This is especially true in the context of search engines, which have revolutionized and facilitated access to, and dissemination of, the information in the online sphere. However, as search engines are private entities; how can we be sure that they strike the balance right between the two competing-yet-intertwined rights? And what are the implications for the founding principles if they fail the task?

Sammanfattning

Denna uppsats har undersökt 'rätten att bli glömd', dvs. fysiska personers rättighet att be en operatör till en sökmotor att inte visa sökträffar som innehåller personuppgifter på sin resultatlista efter en sökning på personens namn. Rätten att bli bortglömd är en relativt ny grundläggande rättighet i EU-rätten, då den först etablerades den 13e Maj 2014 i målet C-131/12 *Google Spain,* och blev sedan en del av EUs sekundärrätt i Artikel 17 och 21 i den allmänna dataskyddsförordningen (GDPR) när den antogs 2016. Då rätten att bli glömd fortfarande är relativt outforskad, var förväntningarna och intresset högt när EU domstolen den 24e September 2019 publicerade två nya mål som vidare utvecklade och beskrev rättigheten, C-507/17 *Google CNIL* och *C-136/17 GC and others*.

Syftet med denna uppsats har varit att undersöka konsekvenserna av dessa domar, och rätten att bli glömd, mot bakgrund av de grundläggande principer som EU bygger på; respekt för människans värdighet, demokrati, rättsstaten och respekt för de mänskliga rättigheterna. Dessa värden är gemensamma för alla EUs medlemsstater i ett samhälle som ska kännetecknas av mångfald, och ska genomsyra alla EUs åtaganden, både internt inom Unionen och externt i förhållande till andra icke-EU länder. Uppsatsen visar att EU har givit operatörer för sökmotorer ett stort ansvar att både skydda fysiska personer vid behandling av deras personuppgifter och samtidigt respektera människors yttrande- och informationsfrihet, då dessa är värden som måste balanseras för att bedöma om en person ska ha få rätt att bli glömd eller inte. Mot bakgrunden att EU värnar och bygger på ett samhälle där tillgång till information är en grundläggande rättighet, och respekt för demokrati, rättsstaten och respekt för de mänskliga rättigheterna, är det problematiskt att EU har gett en privat aktör ett så stort ansvar att säkerhetsställa att dessa värden tillförsäkras. Hur kan vi vara säkra på att sökmotorer hanterar förfrågningar om att bli bortglömd på ett korrekt sätt? Och vad blir konsekvenserna om de misslyckas, med tanke på hur viktiga sökmotorer är för personers möjlighet att snabbt och enkelt hitta information?

Preface

I would like to first and foremost express immense gratitude to my supervisor, Eduardo Gill-Pedro. Without your knowledge, guidance and support, there would be no thesis. Thank you.

Secondly, and of equal importance, I want to say thank you to all my friends that have made my years in Lund more than I could have ever wished for – years that *I will never forget.*

Abbreviations

AG	Advocate General
Charter	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
Data Directive	Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Dir. 95/46/EC)
DPA	Data Protection Agency
ECHR	European Charter of Fundamental Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EU	European Union
GDPR	General Data Protection Regulation (Reg. (EU) 2016/679)
SEO	Search engine operator
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union

1 Introduction

1.1 An introduction to the issue

> "Reconciling the right to privacy and to the protection of personal data with the right to information and to freedom of expression in the internet era is one of the main challenges of our time."[1]

This quote is from the Advocate General Szpunar in his opinion on *GC and others*, one of the two cases published on 24 September 2019, which transformed the material and territorial scope of the *'right to be forgotten'* for search engines in EU law. The right to be forgotten gives a person whose data is being processed by a search engine a right to request that the data should be excluded from the search engine's index list that appears after a search on that data subject's name. In the first case, *Google CNIL*,[2] the CJEU determined the territorial scope of the right to be forgotten under EU law and ruled that, in principle, search engine operators (SEOs) are required to remove links from all version of the search engine in the EU, regardless of where in the Union a request has been made. In the second case, *GC and others*,[3] the Court held that SEOs are, in principle, prohibited from processing sensitive personal data, unless it can demonstrate reasons of substantial public interest that make the processing of it necessary for freedom of expression and information.

The EU is founded on the fundamental principles of respect for, *inter alia*, human dignity, freedom, democracy and respect for human rights.[4] These fundamental principles are common to the member states in a society where pluralism and justice prevail and are an expression of the pluralistic nature of the EU's legal structure. The pluralistic order of the EU legal system is one of the reasons why the right to be forgotten is a particularly special right for the EU to balance, as it permeates the very core of the founding principles of the EU; the fundamental right to data protection lies in the heart of human dignity and protection of privacy, and freedom of expression and information are vital cornerstones in a democratic and transparent society. As held by Hijke Hijmans; "[r]espect for privacy and data protection is part of a

---

[1] Opinion of Advocate General Szpunar delivered on 10 January 2019, C-136/17 *GC and Others*, EU:C:2019:14, para. 1.
[2] Case C-507/17 *Google v CNIL,* 24 September 2019, EU:C:2019:772
[3] Case C-136/17 *GC and others v CNIL*, 24 September 2019, EU:C:2019:773
[4] Treaty on the European Union (consolidated version) [2012] OJ C326/13, (TEU) Article 2.

European Union based on the values of democracy, the rule of law and fundamental rights".[5] If the balance between the fundamental rights and freedoms triggered by a request to be forgotten is not properly struck, it may trigger potentially serious implications for an individual's freedom of expression and information.

1.2 Purpose and main thesis question

This thesis aims to explore the implications of the right to be forgotten, from an internal EU perspective, in the light of the recent cases *Google CNIL* and *GC and others*, to analyse if the interpretation by the European Court of Justice appears to be compatible with the founding principles of the EU.

On those grounds, the main question of the thesis is the following:

- Is the right to be forgotten, in the light of the development of the recent case law, compatible with the founding principles of the EU?

1.3 Sub-questions and disposition

In order to assess the main question of this thesis, I will use the following sub-questions, which shall act as platforms providing the reader, and myself, with sufficient information to understand the implications of the recent case law. The sub-questions act as guidelines for the disposition of the thesis; where sub-question one is answered in chapter 2, sub-question two in chapter 3, and sub-question three in chapter 4. Each chapter will end with a concluding section where I explain the findings of the chapter, and why it is connected to the main question of the thesis. This leads us to the fifth and last chapter, titled '*Conclusion'*, where the main thesis question is answered.

The sub-questions are the following:

(1) What are the founding principles of the EU and why do they matter for fundamental rights?
(2) What is the 'right to be forgotten' and which rights and freedoms do it specifically trigger?
(3) How does the CJEU resonate in *Google CNIL* and *GC and others*, and what arguments paved the way to the outcomes of the judgments?

---

[5] Hijmans, H. (2016). *'The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU',* Springer International Publishing Switzerland 2016, p. 18.

1.4 Delimitations

The scope of this thesis is the legal impact of *Google CNIL* and *GC and others* on the founding principles of EU law from a purely EU internal perspective, leaving aside implications outside the EU and implications in relation to the ECHR. Moreover, this thesis focus on request of removal of information from search engines, and not requests to original publishers of information. The thesis does not explore information removed from SEOs due to different legal reasons, e.g. data that relates to children, or copyright, or that the information in itself is abusive or illegal. Furthermore, I have chosen to delimit the scope of this thesis to the rights of privacy and data protection, and freedom of expression and information. While the right to be forgotten triggers several other rights and freedoms as well, not the least the freedom to establish and conduct business and have implications on the internal market of the EU, this will be not be explored. Furthermore, the informational exchange in areas of EU law relating to the enforcement and judicial cooperation have been omitted.

Additionally, I have not explored the actual enforcement procedure that follows a request to be forgotten. This includes the enforcement of the member states, such as the 'one-stop-shop' mechanism and the national DPA's cooperation mechanism set out in the GDPR, and SEO's policies how to assess a request to be forgotten. For those interested, Google's transparency policy for the removal of personal data is available at: <<*https://transparencyreport.google.com/*>>.

1.5 Method and material

To answer my main thesis question, and the three sub-questions, I will use an EU legal dogmatic method. Characteristic for the EU legal order is to approach it using a teleological method, which focuses on a purpose-driven interpretation of the relevant legal rules. This method emanates from the concept of 'constitutional telos'; that all EU measures taken should further the goals and objectives of the Treaties and the EU.[6] The point of departure for this thesis has thus been to assess the relevant legal rules that the right to be forgotten triggers, both from the context it stems from; i.e. the background of data protection in the EU, why privacy and freedom of expression is important for democracy, rule of law and fundamental rights and due to the

[6] Hettne, J. (2011) *'EU-rättsliga tolkningsmetoder'*, in Eriksson Otken, I, Hettne, J. (eds) (2011) *'EU rättslig metod, Teori och Genomslag i Svensk Rättstillämpning,'* (2nd ed), Stockholm: Nordstedts Juridik AB, 2011, p. 158 – 159.

objectives it aims to foster; i.e. the free flow of personal data and respect for fundamental rights. The teleological method is used to interpret legislation to be consistent with the purpose that it aims to achieve, in order to prevent unwanted consequences of a literal interpretation and to fill in gaps to help further the objectives of the EU.[7]

This method is particularly important as the focus of this thesis is the *founding principles of EU law,* principles which by their nature are vague and hard to define, and therefore require interpretation to be applied. Due to the margin of interpretational that these principles allow, situations when they apply are susceptible to argumentation and interpretational discretion. This is beneficial as it allows the founding principles to provide a flexible framework suitable for a contemporary modern society,[8] which in the area of data protection is pivotal to keep the legislation up to date with the technological developments. Thus, this thesis has assessed the legal implications of Google CNIL and GC and others, and if they are compatible with the founding principles of EU law, I have focused on the founding principles and applied it in the particular situation of the right to be forgotten. To understand the values of democracy, rule of law, fundamental rights, and pluralism, I have examined, in particular, case-law where the CJEU has discussed and derived the purpose behind those values.[9] This concept has been described, e.g. in *Van Gend en Loos*, where the Court declared that the "spirit" or "general scheme" of the treaties must guide all provisions established therein.[10]

In the EU legal system, the binding instruments of law that this thesis has explored are the following sources: primary EU legislation, i.e. the Treaties and the Charter; the general principles of EU law, such as the ECHR;[11] secondary EU legislation, in particular, the GDPR and the Data Directive; jurisprudence by the CJEU, in particular, the three major cases on the 'right to be forgotten' *Google Spain, Google CNIL,* and *GC and others*.[12] Moreover, the non-binding, soft-law instruments of EU law have been: the *Explanations to the Charter*, while not binding positive EU law, nonetheless guides the interpretation of the Charter, as the CJEU cannot interpret its provisions in any way that conflicts with the explanations relating to it;[13] different types of

---

[7] Ibid, p. 168.
[8] Ibid. p. 62- 63.
[9] Ibid. p. 168 – 170.
[10] Case 26/62 *van Gend & Loos*, 5 February 1963, EU:C:1963:1, *(van Gend en Loos)* see page 13.
[11] TEU, Article 6(3).
[12] Hettne, J. (2011) p. 40; Case C-131/12 *Google Spain*, 13 May 2014, EU:C:2014:317 *(Google Spain)*
[13] TEU, Article 6(1); Article 52(7) of the Charter; Lenaerts, K. (2012). *'Exploring the Limits of the EU Charter of Fundamental Rights'*. European Constitutional Law Review, 8(3), pp. 375 – 403, p. 377.

soft-law instruments, such as official documents and reposts from both EU institutions as well as the Council of Europe, and the Guidelines that followed both *Google Spain*, and *Google CNIL* and *GC and others*, all of which guide member states to interpret EU legislation; Opinions of Advocate Generals, in particular, those to *Google CNIL* and *GC and others*; and lastly, legal doctrine have been applied to provide important critical thinking to the law and jurisprudence that exists, and consequently opinions of legal scholars to give a nuanced perspective, and to further the depth of understanding in the subject.[14] Moreover, as the two cases *Google CNIL* and *GC and others* were recently published, there has not been published many articles on the subject. Therefore, I have looked at other, more up-to-date sources of information, such as blog posts and articles written for newspapers.

As the perspective of this thesis is from the founding principles of EU law, and what the implications are for them in the context of the right to be forgotten, I want to define how they are interpreted in the scope of this thesis. The principles are both a part of positive EU legislation, the most important basis being Article 2 TEU, and an important source of teleological interpretation, as numerous secondary legislation must be interpreted in the light of the founding principles, especially in the light of a particular fundamental right or freedom.[15] This thesis does not claim that the Treaties of primary legislation; TEU, TFEU and the Charter constitute an 'EU constitution'. Such a claim is, not the least after the failed attempt in 2005 to adopt a formal constitution, the "EU Constitutional Treaty", not without controversy. However, with that said, the CJEU has several times, from early days of European Integration, referred to the existing EU Treaties as the "basic constitutional charter",[16] or the "constitutional framework", of the Union, and that the EU has a "constitutional structure".[17] The founding principles of the EU can thus be understood as "constitutional principles", as they form a "constitution" in the sense of *an overarching conception of principles of particular importance* that must permeate all measures taken, and all legislation adopted, by the EU, and its member states when implementing EU law.[18] Thus, as suggested by Armin von Bogdandy, without claiming that the Treaties are the constitution of the EU, it is helpful to view the founding principles of the EU as "constitutional", and deal with them

[14] Bogdandy, A. von (2009) *'Founding principles'* Chapter 1 in Bogdandy A. von and Bast, J. (eds), '*Principles of European constitutional law'* (2nd edn) Oxford: Hart Publishing, 2009, p. 18.
[15] Bogdandy, A. von (2009), p. 16.
[16] C 294/83 *Les verts,* 23 April 1986, EU:C:1986:166 *(Les Verts)* para. 23.
[17] Opinion 2/13 of the Court (Full Court) delivered on 18 December 2014, EU:C:2014:2454, (*Opinion 2/13*) paras. 158 and 165.
[18] Bogdandy, A. von (2009), p. 22.

accordingly, since they represent the "inviolable normative core that must be respected above all other values, rights or principles in the EU legal order".[19]

1.6 Terminology

What is a search engine and how does it work?

Generally, modern search engines function by allowing a computer robot, called a 'spider' or 'bot', crawl the web for content in the form of keywords or links, which are later indexed and made searchable by users. Search engines use an algorithm to ranks websites on their importance and index its list of results following a search accordingly.[20] Since search engines in themselves do not *create* information in the form of websites, but merely index information that already exists on the Internet, information which is not included in a search engine's result is still available on the internet (provided one knows the information's URL or how to find it without the help of the search engine) and links that are deleted from such results are not deleted from their original website.[21]

What is the processing of personal data?

Article 4(2) of the GDPR defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

What is personal data and who is a data subject?

Article 4(1) of the GDPR defines personal data as *any information relating to an identified or identifiable natural person*, which is called the *data subject*. The data subject can be any natural person "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".[22] Moreover, there are 'special categories' of data, i.e. *sensitive data*, that merit higher protection

---

[19] Ibid.
[20] Laidlaw, E. (2015). *'Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility.'* Cambridge: Cambridge University Press 2015, p. 173-174.
[21] Laidlaw, E. (2015) p. 172 and 174.
[22] GDPR, Article 4(1)

than other (non-special) personal data,[23] such as data revealing racial[24] or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, health or sex life. [25]

Who is a Controller?

The GDPR defines a 'controller' of personal data in Article 4(7) as any "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law". In *Google Spain*, the CJEU declared that search engines are considered 'controllers' in the respect of the processing of personal data carried when an internet user conducts a search on the basis of a data subject's name.[26]

---

[23] GDPR, Recital 53

[24] As pointed out in Recital 51 of the GDPR: "the use of the term 'racial origin' in the GDPR does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races."

[25] GDPR, Article 9(1); Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (consolidated version) [1995] OJ L 281, 23.11.1995, p. 31–50, Article 8(1), with the exception of data revealing genetic or biometric data, which was added to the GDPR.

[26] Case C-131/12 *Google Spain*, 13 May 2014, EU:C:2014:317, *(Google Spain)*

2 The founding principles of EU Law

2.1 Introduction

The first chapter of this thesis aims to explore the legal structure of the EU: both from the perspective of the founding principles of EU law, also called the 'grand structural plan' of the EU;[27] and from the perspective of the member states constitutions. The first section explains the values that the principles in Article 2 TEU encompass, and what type of commitments they conjure for the Union. This set us down the path to the second section, which describes the concept of the *autonomy of EU law,* and the 'constitutional pluralism' that exists within the EU legal structure, which requires that the interpretation of the founding principles of the EU must be ensured within the *framework of the structure and objectives of the EU* when acting inside the scope of EU law.[28] These two sections provide us with the necessary framework to understand the context that must guard EU secondary legislation that embodies fundamental rights, such as the GDPR, and help us understand the implications of the CJEU's reasoning in the cases which this thesis focuses on *Google CNIL* and *GC and others*.

This Chapter aims to "paint the broader picture" and takes us down the hierarchical ladder of EU law, starting at the very top – the founding principles of EU law. Before embarking on the process to outline the fundamental principles that govern all EU measures, it is necessary to clarify that while the EU possesses several *state-like features* typically not found in other intragovernmental institutions, such as, *inter alia* an autonomous legal order; rules addressed directly to sub-components of the member states; an internal set of fundamental rights, a 'bill of rights'; a territory and external borders; a concept of EU citizenship;[29] several important features are missing from concluding that the EU is a state. Some of those being that the EU leaves matters traditionally seen as "core elements of national sovereignty", such as

[27] Bogdandy, A. von (2009), p. 15.
[28] *Opinion 2/13*, para. 170.
[29] Rosas, A., & Armati, L. (2018). 'EU Constitutional law: an introduction' (Third edition). Hart Publishing, 2018, p. 14 – 16.

areas concerning national foreign policy, taxation, security and defence, immigration and penal law, still in the hands of the member states.[30]

2.2 What are the founding principles?

Article 2 TEU codifies the founding principle of the EU, and states the following:

> "The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity, and equality between women and men prevail."

These values form part of, as declared by the CJEU in *Van Gend en Loos* as the "spirit" or "general scheme" of the Treaty,[31] which must guide all provisions established therein. They form the 'ideological' basis for the Union's objectives, outlined in Article 3 TEU, that are to, *inter alia*: "promote peace, its values and the well-being of its peoples"; "offer its citizens an area of freedom security and justice without internal frontiers"; "establish an internal market"; and in relations with the wider world "uphold and promote its values and interests and contribute to the protection of its citizen"; and have been referred to by the EU Commission as the "bedrock of our societies and common identity".[32] Respect for these values is thus a pivotal feature of the *raison d'être* of the Union, and following Article 49 TEU, a condition for a European State to apply to become a member of the Union. Correspondingly, in cases of "serious and persistent breach" by a member state of the values guaranteed in Article 2 TEU may trigger the 'nuclear option' embedded in Article 7 TEU, which leads to a suspension of certain of the rights deriving from the application of the Treaties to the member state in question.

The founding principles in Article 2 TEU, *i.e.* respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, have the normatively 'highest rank' in EU law. They are all supreme to norms of EU primary law, *i.e.* the Treaties and the Charter, as well as EU secondary law, since instrument of primary, and secondary law must be interpreted *in*

---

[30] Rosas, A., & Armati, L. (2018), p. 17 – 18.
[31] Case 26/62 *van Gend & Loos*, 5 February 1963, EU:C:1963:1, *(van Gend en Loos)* see page 13.
[32] European Commission, (2019) *'Communication from the Commission to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions: Strengthening the Rule of Law within the Union - A blueprint For Action'*, COM/2019/343 final, Brussels, 17 July 2019, p. 1.

the light of the founding principles. If any measure is considered contrary to the founding principles, such a measure is invalid.[33] The hierarchal order of placing the founding principles above primary law has been confirmed by the CJEU, e.g. *Kadi,* where the Court clarified that if a provision in the Treaties allows for derogation from EU primary legislation, "[t]hose provisions cannot [...] be understood to authorize any derogation from the principles of liberty, democracy and respect for human rights and fundamental freedoms enshrined in Article 6(1) EU [now 2 TEU] as a foundation of the Union."[34]

The hierarchical norm that the founding principles of the EU must guide all other EU actions and invalidates EU measures contrary to them is particularly visible in the case of fundamental rights vis-à-vis secondary legislation. This was the case in *Digital Rights Ireland*, where the Court declared a directive invalid for not complying with the fundamental rights to privacy and protection of personal data,[35] as well as in *Schrems*, where the Court declared a whole decision invalid after several provisions failed an assessment in the light of the Charter.[36]

2.2.1 The founding principles are common to the member states

As expressly mentioned in Article 2 TEU, the founding values of the EU are *common* to the member states. The connection between member states constitutions and the values enshrined in Article 2 TEU can be seen in, *inter alia,* Article 4(2) and Article 6(3) TEU: declaring that the Union is founded on a society in which pluralism prevails, that it shall respect member states' national identities, inherent in their fundamental and constitutional structures, and that fundamental rights are a result from the constitutional traditions common to the member states. Hence, member states' constitutional values are an integrated part of the founding principles of the EU, as the latter is founded on the former. While the founding values of the EU are common to the member states, they are not identical to those of one member state in particular. Instead, they represent a "common European denominator" composed of the different constitutions of all member states –meaning that even though the founding principles originate from the member states'

[33] Bogdandy, A. von (2009), p. 16.
[34] Joined cases C-402/05 P and C-415/05 P, *Kadi*, 3 September 2008, EU:C:2008:461, *(Kadi)* para. 303.
[35] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland,* 8 April 2014 ECLI:EU:C:2014:238.
[36] C-362/14 *Schrems* 6 October 2015 EU:C:2015:650.

constitutions, they may differ from values specific to one single member state.[37]

The scope of this thesis is the right to be forgotten vis-à-vis search engines, which especially triggers the fundamental rights to privacy and data protection, and freedom of expression. In contemporary modern society, search engines act as 'gatekeepers' for individuals who wish to seek, receive, or impart information, as content that is not listed high or shown at all in search engines' indexes is less likely to reach a large audience or to be seen at all. Search engines, therefore, act as important intermediaries between information and individuals, and are pivotal to create and maintain an "environment for pluralist public debate that is equally accessible and inclusive to all."[38] Thus, when information is removed from the result of a search engine, it interferes with the public's right of access to it. The interplay between those two rights is what is reconciled in *Google CNIL*, and, in particular, *GC and others*, where the CJEU struck a balance between those two rights.[39] The following section shall thus examine the founding principles of EU law, and their implications for fundamental rights.

2.3 The EU is founded on respect for fundamental rights

In the Lisbon Treaty, the principle of respect for fundamental rights can be found in Article 2 and 6 TEU. The importance of respect for fundamental rights has been highlighted several times by the Court, *inter alia*, in *Kadi*, where the Court stressed that even though certain provisions in the Treaties permit deviation to some extent from EU primary law, those provisions "may in no circumstances permit any challenge to the principles that form part of the very foundations of the Community legal order, one of which is the protection of fundamental rights".[40] In the EU legal system, there are two main sources of primary EU law that protects fundamental rights; one source being *unwritten,* the general principles of EU law, and the other being *written*, the Charter.[41] Oftentimes, the two sources overlap due to having the same

[37] Bogdandy, A. von (2009), p. 25.
[38] Committee of experts on the internet intermediaries, *"Final draft study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*", "Meeting report" MSI-NET (2017)06, Appendix 4, 6 October 2017, accessed 2019-12-28 from: https://rm.coe.int/msi-net-4th-meeting-18-19- september-2017/ p. 35 - 36.
[39] Case C-507/17 *Google CNIL,* 24 September 2019, EU:C:2019:772 *(Google CNIL)* para. 61.
[40] *Kadi*, para. 304.
[41] TEU, Article 6(3) and 6(1)

scope and field of application, and since the Charter, to a substantial part, was built on prior case-law on the general principles of EU law.[42]

2.3.1 The Charter can confer obligations to private parties, such as SEOs

Following Article 52(1) of the Charter, the Charter applies to the institutions, bodies, offices, and agencies of the EU, and member states when they are 'implementing EU law'.[43] Member states are acting inside the scope of EU law when they are either implementing[44] or derogating from it,[45] or when they are acting in a situation which falls within the *scope of application* of EU law. The idea is that "situations cannot exist which are covered in that way by European Union law without […] fundamental rights being applicable."[46] This is called the 'vertical' dimension. Due to the *special nature of EU law*, which we will assess in the second section of this chapter, some provisions of the Charter may be relied upon by individuals against other individuals. This dimension is called *horizontal direct effect*, or '*diagonal effect*', and was first recognised by the CJEU in *Defrenne* concerning non-discrimination on the basis of sex in work relations.[47] The reason why the Charter developed to include non-state actors to its addressees that some of the provisions in the Charter would not be *efficient* if they could not bind private parties,[48] such as the principle of non-discrimination on the grounds of age, which "is sufficient in itself to confer on individuals an individual right which they may invoke",[49] and the right to equal pay for men and women, which is "mandatory in nature".[50]

The situation in *Google CNIL* and *GC and others* concern the right to be forgotten and display a relationship between two private parties that lacks state interference. The individual whose data is being processed may on the basis of their fundamental rights of privacy and data protection, enshrined in

[42] Explanations Relating to the Charter of Fundamental Rights, [2007] OJ C303/2, *Explanation on Article 51 of the Charter* and the case-law cited therein.
[43] Charter of Fundamental Rights of the European Union [2012] OJ C326/02, Article 51(1).
[44] Case 5/88 *Wachauf* [1989] ECR 2609.
[45] Case C 260/89 *ERT* EU:C:1991:254.
[46] Case C-617/10 *Åklagaren v Åkerberg Fransson,* 26 February 2013 *(Åkerberg Fransson)* EU:C:2012:340, para. 21
[47] Case 43/75 *Defrenne*, 8 April 1976 *(Defrenne)* EU:C:1976:56
[48] Frantziou, E. (2015). *'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality'*, European Law Journal, Vol. 21, No. 5, September 2015, pp. 657-679, p. 660.
[49]Charter, Article 21; C-176/12 *Association de médiation sociale* 15 January 2014, EU:C:2014:2 para. 47.
[50] Charter, Article 23; *Defrenne*, para. 39.

the Charter and secondary legislation in the GDPR, request a SEO to remove data from their search result, which then has an obligation to assess that claim. It is a clear example of where provisions of the Charter are capable of producing a direct horizontal effect, as the Court stated that ”the data subject may, in light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public [by search engines]”.[51] The reasoning by the Court to declaring those provisions binding for private parties was due to the significant effect SEOs can have on the fundamental rights to privacy and protection of personal data, as the search results give a more or less detailed profile of the data subject. As the online sphere is mostly governed by private parties,[52] the data subject's fundamental rights would thus not be sufficiently protected if the Charter could not create obligations for non-state actors.[53]

2.4 The EU is founded on respect for rule of law and democracy

As the EU is not a state,[54] it does not have the legitimacy requirements of a state and lacks the reciprocal relationship with individuals that are required of a democracy.[55] The EU does not claim the coercive authority of the individuals inside the territory of the member states, instead, the EU claims authority over the member states and obliged them to ensure the full application of EU law and their sincere cooperation.[56] The founding principle of democracy is meant to be abstract and to provide guidance, and it has therefore not been subject to a EU wide definition.[57] While member states claim of legitimacy vis-à-vis individuals in their jurisdiction is based on the "democratic process through national law is made", the Union's claim of authority over its member states based on *their respect of the founding principles;* democracy, rule of law and fundamental rights. This conclusion is supported by the fact that member states constitutional court declared that they will reject the claim of authority that follows from the primacy of EU law if the Union does not respect fundamental rights, which was one of the reasons why the Union incorporated a fundamental rights framework.[58]

---

[51] *Google Spain*, para. 99.

[52] Leczykiewicz, D. (2020) *'Judical Development of EU Fundamental Rights Law in the Digital Era: A Fresh Look at the Concept of 'General Principles',* in U. Bernitz, X. Groussot et. al, (eds) *General Principles of EU law and the EU Digital Order*, Kluwer Law International, 2020. p. 66.

[53] *Google Spain*, para. 38.

[54] See section 2.1.

[55] Gill-Pedro, E. (2019) 'EU law, fundamental rights and national democracy.' New York: Routledge, Taylor & Francis Group 2019, p. 98-99.

[56] Ibid. p. 100; TEU Article 4(3).

[57] Eriksson Otken, E, Hettne, J (2011) p. 76 – 77.

[58] Case 11/70 *Internationale Handelsgesellschaft*, 17 December 1970, EU:C:1970:114

The EU's claim to be founded on the shared objective to respect fundamental rights, democracy and the rule of law necessitates that those principles must underpin all internal and external measures taken by the EU.[59] A pivotal prerequisite to respecting democracy is to promote freedom of expression, opinion, assembly and association, both online and offline.[60] As noted by the United Nations in a report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression:

> "States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other."[61]

Consequently, both freedom of expression and rights of privacy sometimes are referred to as opposite rights, which must be balanced in *inter alia* the context of the right to be forgotten, they must be juxtaposed in order to create a favourable environment for democracy.[62] So, the EU's claim to be a Union founded on respect for democratic principles, preconditions that it respects rests on fundamental rights "as conditions that generate and maintain the democratic debate", [63] *inter alia* freedom of expression and rights to privacy and data protection. Without a framework guaranteeing respect for fundamental rights, individuals cannot engage in the democratic process.[64]

As stated by Hielke Hijmans, democracy for EU citizens requires that the EU, as a society, ensures its citizens the full exercise of their fundamental rights under the rule of law, so that they may freely participate in democratic discourse.[65] This premise is declared in Article 10(3) TEU, which guarantees that "[e]very citizen shall have the right to participate in the democratic life of the Union". Both the Preamble and Article 1 TEU echoes similar ambitions, holding that the Treaty aims to strengthen "the process of creating

---

[59] Council of the European Union, (2012) *EU Strategic Framework and Action Plan on Human Rights and Democracy*, Luxembourg, 25 June 2012 11855/12, p. 1; TEU, Article 2; and Article 13.
[60] Council of the European Union, (2012) *EU Strategic Framework and Action Plan on Human Rights and Democracy*, Luxembourg, p. 2.
[61] United Nations Human Rights Council, '*Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*', Frank La Rue, A/HRC/23/40, 17 April 2013, para. 79.
[62] Ivanova Y. (2020) *'Can EU Data Protection Legislation Help to Counter "Fake News" and Other Threats to Democracy?'* In Katsikas S., Zorkadis V. (eds) *'E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age. e-Democracy 2019.'* Communications in Computer and Information Science, vol 1111. Springer, Cham. p. 222.
[63] Gill-Pedro, E. (2019) p. 57.
[64] Ibid. p. 49.
[65] Hijmans, H. (2016), p. 24.

an ever closer union among the peoples of Europe, in which decisions are taken as closely as possible to the citizen". These provisions aim to foster a Union which respects democratic principles by, *inter alia,* enhance procedures for openness, and transparency, which are key factors for democracy and respect for fundamental values.[66] Openness and transparency are core elements of the democratic life in the Union and have been enshrined, *inter alia*, in the right of access to documents in Article 42 of the Charter, which according to Article 15(3) of the TFEU applies to documents of institutions, bodies, and agencies generally, regardless of their form. The principle of transparency contributes to ensuring democracy by enabling "citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system", which importance has been emphasized by the CJEU several times in case law.[67]

The fostering of transparency and openness to ensure democracy in the EU has resulted in a regulation on public access to EU documents, Reg. No 1049/2001, which purpose is "to give the fullest possible effect to the right of public access to documents".[68] The principles of transparency and openness, and privacy may sometimes interfere with each other, as seen in e.g. Article 4(1)(b) of Regulation No 1049/2001, which provides for an exception to "access to documents where disclosure would undermine the protection of privacy and the integrity of the individual," especially concerning the protection of personal data. The collision of these rights, enshrined in EU secondary legislation, was the focal point in *Bavarian Lager*, where the Court emphasized that one does not have primacy over the other, but instead that both should be simultaneously ensured.[69]

2.4.1 Democracy and freedom of expression

The link between the founding principles of the EU of democracy and freedom of expression and information has been confirmed several times by the CJEU, e.g. in *Tele2* from 2016, where the Court expressly declared that the freedom "constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU,

[66] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, *OJ L 145, 31.5.2001, p. 43–48,* Recital 2.

[67] For e.g. Joined Cases C-39/05 P and C-52/05 P, Sweden and Turco v. Council, 1 July 2008, ECLI:EU:C:2008:374 para. 45; Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen*, 9 November 2010, EU:C:2010:662, *(Volker und Schecke)* para. 68.

[68] Reg. 1049/2001, Recital 4.

[69] C-28/08 P *Bavarian Lager*, 29 June 2010, EU:C:2010:378, *(Bavarian Lager)* para. 56.

the Union is founded."[70] Freedom of expression and information has furthermore been described, in *Bavarian Lager*, as "one of the fundamental pillars of a democratic society".[71] The technological developments of the 21st century have resulted in the fact that access to, and participation on, the Internet, has become "[…] an integral part of our democratic life, and facilitation of this democratic potential critically relies on a governance structure supportive of free speech".[72] Therefore, the freedom must be fully applied on the Internet, and state obligations to ensure that the right is protected of expression equally exist online as well as offline.[73] Freedom of expression and information applies not only to the actual content of the information expressed but also to the means of transmission or reception used to express oneself.[74] The ECtHR has several times recognised the importance of freedom of expression on the internet, due to "the substantial contribution made by Internet archives to preserving and making available news and information. Such archives constitute an important source for education and historical research, particularly as they are readily accessible to the public and are generally free".[75]

Rights of privacy and data protection and freedom of expression and information are, together, vital components that must coexist to create an environment where people feel free to engage in a democratic society. The values can be seen as 'two sides of the same coin', as individuals cannot exercise their freedom of expression and information if they are not guaranteed a sufficient level of privacy, and the internet must be safe for citizens to use as a tool to express and inform themselves, to ensure them the possibility to participate in democratic debate.[76] A solid privacy and data protection regime are needed to create a safe environment on the internet, to ensure that the internet is a safe and allows individuals to express themselves freely, participate in discussion and exchange opinions which are different from those held at an official level.[77] If privacy and data protection is not upheld, it could create a "chilling effect on individuals' participation in democratic society."[78] Thus, when the EU claims to be founded on

---

[70] Joined cases C-203/15 and C-698/15, *Tele2 Sverige AB*, 21 December 2016, EU:C:2016:970 *(Tele2 Sverige)* para. 93.
[71] *Bavarian Lager*, para. 18.
[72] Laidlaw, E. (2015), p. 231.
[73] See e.g. *Editorial Board of Pravoye Delo and Shtekel v. Ukraine,* 5 May 2011, no. 33014/05 CE:ECHR:2011:0505JUD003301405.
[74] *Ahmet Yldrim v. Turkey*, 18 December 2012, No. 3111/10 CE:ECHR:2012:1218JUD000311110, para 50.
[75] *M.L and W.W v. Germany*, 28 June 2018, nos. 60798/10 and 65599/10, CE:ECHR:2018:0628JUD006079810, para. 90 and case-law cited therein.
[76] Hijmans, H (2016) p. 24.
[77] C-340/00P, *Cwik v Commission,* 13 December 2001, ECLI:EU:C:2001:701, para. 22.
[78] Hijmans, H. (2016) p. 24.

democracy, it entails a coexistence of data protection and privacy and freedom of expression and information to ensure that the EU is a sphere where citizens are free to express themselves.

2.5 The legal structure of the EU

As expressly mentioned in Article 2 TEU, the founding values of the EU are *common* to the member states – not identical. Therefore, they may differ from values specific to that of one single member state.[79] Even so, member states have an obligation to comply with the level set on an EU level, due to the autonomy of EU law, and the specific obligations that are conferred to the member states because of it. Hence, even though the protection of those were inspired by the constitutional traditions common to the member states, it has always been its own part of EU law which must be ensured within the framework of the structure and objectives of the community.[80] Member states are therefore guaranteed protection of fundamental rights when acting inside the scope of EU law, but not as interpreted by their constitution, or by the ECHR, but as independent, self-standing, "EU fundamental rights".[81] This fact has been the cause of a dispute that can be traced back to the very beginning of EU integration when the Court developed the principles of direct effect and primacy of EU law. As ruled in *Costa v. Enel*:

> "[…] the law stemming from the Treaty, an independent source of law, could not, because of its special and original nature, be overridden by domestic legal provisions, however framed, without being deprived of its character as Community [EU] law and without the legal basis of the Community [EU] itself being called into question."[82]

The 'special and original nature' of EU law is dependent on cooperation by the member states since they have chosen, by becoming members to the Union, to limit "their sovereign rights, albeit within limited fields",[83] and confer it to the Union. Many of the 'specific characteristics of EU law'[84] can be traced back to the CJEU's endeavour to guarantee the full effectiveness of EU law and compliance by the member states, such as the autonomy of EU law,[85] and the principles of direct effect[86] and primacy of EU law.[87] Following

---

[79] Bogdandy, A. von (2009) p. 25.
[80] Case 11/70 *Internationale Handelsgesellschaft*, para. 3
[81] Gill-Pedro, E & Groussot, X. (2017) 'The Duty of Mutual Trust in EU Law and the Duty to Secure Human Rights: Can the EU's Accession to the ECHR Ease the Tension?', Nordic Journal of Human Rights, 35:3, 258-274, p. 260.
[82] Case 6/64 *Costa v. Enel*, 15 July 1964, EU:C:1964:66 p. 594.
[83] Ibid, p. 593
[84] *Opinion 2/13*, para. 166
[85] Case 6/64 *Costa v. Enel*
[86] Case 26/62*Van Gend en Loos*
[87] Case 6/64 *Costa v. Enel*

Article 19(1) TEU, which gives "concrete expression to the value of the rule of law",[88] the CJEU has an obligation to ensure that the interpretation and application of the Treaties is observed, and member states have an obligation to provide remedies to ensure effective legal protection in fields covered by EU law.

Due to the full effectiveness of EU law, even though the member states enjoy a certain margin of manoeuvre when implementing EU law, such margin must nevertheless be applied by the authorities and courts of the member states in a way that respects the EU set balance between the rights and interests involved, in conformity with the principle of proportionality.[89] The obligation for member states to ensure the full effectiveness of EU law can be seen *Google Spain*, where the Court held that the data subject may, on the basis of his or hers fundamental rights stemming from the Charter request a private search engine operator (SEO) to remove his or her personal information from the list of the SEO's results,[90] leaving it to the member states to enforce the obligation.[91] The principle of rule of law may thus be *one* of the many reasons to the Court's stringent interpretation of the effectiveness of EU law and member states obligation to ensure it, as an irregular application of EU legislation would undermine rule of law and consequently, democracy and fundamental rights, without which the Unions claim of authority over member states sovereignty will not be respected.

2.5.1 Opinion 2/13 and the autonomy of EU law

Google CNIL and *GC and others* concern the application of the right to be forgotten, which consists of a balance between the fundamental rights to privacy and data protection, and the public's access to information as guaranteed by freedom of expression and information. This section aims to explain, from the point of view of the EU, why it is important that member states comply with EU law, and the implications that stem from respecting the autonomy of EU law for the member states, vis-à-vis their constitutional obligations. The specific nature of the EU legal structure is explained by the CJEU in its review of a draft agreement proposed in respect of the Union's possible accession to the ECHR, *Opinion 2/13.* The context of the Opinion is that the EU has committed, following Article 6(2) TEU, to accede to the ECHR provided that such accession does not affect the Union's competence

[88] Case C-619/18 *Commission v Poland*, 24 June 2019, EU:C:2019:531, para. 47 and case-law cited therein.
[89] Case C-101/01 *Lindqvist*, 6 November 2003, EU:C:2003:596, para. 84-85 and 87.
[90] *Google Spain*, para. 97 – 98.
[91] Leczykiewicz,D. (2020) p. 79.

as defined by the Treaties. Something that is, according to the Court in *Opinion 2/13*, not possible, due to the specific legal structure of EU law.[92]

As pointed out in section 2.2, the strict internal hierarchy of EU law requires all measures taken by the EU, internally and externally, to comply with the founding principles of EU law. In conjunction with these values, "must be added the specific characteristics arising from the very nature of EU law", i.e. that it stems from an independent source of law, the Treaties, and is at the same time independent from and supreme to, all national provisions of its member states.[93] These specific characteristics have "given rise to a structured network of principles, rules and mutually interdependent legal relations", and created a bond between the Union and its member state, and between member states, in an endeavour to foster European integration and create an "ever closer union".[94] This complex 'structured network' is what the Court refers to as the legal structure of the EU.

The legal structure of the EU rests of the fundamental premise that all member states recognize and trust that they share "a set of common values on which the EU is founded, as stated in Article 2 TEU", a premise that both implies, and justifies, mutual trust between the member states. And "at the *heart* of that legal structure" lies respect for fundamental rights, as enshrined by the Charter.[95] As the Court in *Les Verts* emphasized, the EU is "based on the rule of law, inasmuch as neither its Member States nor its institutions can avoid a review of the question whether the measures adopted by them are in conformity with the basic constitutional charter, the Treaty."[96] The claim that the EU is founded on rule of law, means that "all public powers always act within the constraints set out by law, in accordance with the values of democracy and fundamental rights, and under the control of independent and impartial courts."[97] Consequently, the autonomy of EU law requires that the interpretation of the values encompassed in the founding principles of the EU rights is ensured within the framework of the structure and objectives of the EU, both in relation to member states national laws, and international law such as the ECHR.[98]

2.5.2 What are the implications of the autonomy

[92] *Opinion 2/13*, paras. 160-162 and 164.
[93] Ibid, para. 166
[94] TEU, Article 1; Charter, Preamble.
[95] *Opinion 2/13* para. 168.
[96] Case 294/83 *Les Verts,* para. 23.
[97] European Commission, (2019), COM(2019) 343 final, p. 1
[98] *Opinion 2/13*, para. 170.

of EU law for the member states?

The protection of fundamental rights in the member states is composed of a "complex web of intersecting jurisdictions where domestic, Union, and European Convention rights concur, as well as sometimes compete, with one another".[99] Thus, when the Court in *Opinion 2/13* claims the interpretational authority of fundamental rights when member states act inside the scope of EU law, this entails several implications for the level of protection for fundamental rights inside the territory of the Union and hence, inside the territory of the member states. In cases as *Google CNIL* and *GC and others*, concerning the fundamental rights to privacy and data protection and freedom of expression and information; even though the balance struck between those interests are not identical to those of one single member state, it represent a level set by the EU, "common European denominator",[100] which is, in line with Opinion 2/13, a balance that only the CJEU has authority to strike in the light of the legal structure of the EU. This is due to the autonomy of EU law, as interpreted by the CJEU. As pointed by Eleanor Spaventa, once the scope of EU law is triggered, the CJEU "[…] gains the hermeneutic monopoly over striking the balance between competing rights and interests", which "in turn, means that individuals are no longer protected by their domestic (constitutional) fundamental rights *and* that, lacking accession, they are also no longer protected by the ECHR".[101] Similarly, "when the EU decides to legislate […] it not only relocates the assessment of fundamental rights compliance from the national to the European courts […] but it also subtracts, at least in theory, that same assessment from the scrutiny of the ECtHR".[102] In the example of Data protection, the very *rationale* behind taking EU measures in the area was to harmonise and create an equivalent level of protection of the fundamental rights and freedoms of natural persons throughout the EU: and with that comes the 'hermeneutic monopoly' of reconciling the competing rights and interests in the area of law.[103]

2.5.3 The pluralism of the EU legal order

Even though the EU has the 'hermeneutic monopoly' to decide the 'common European denominator', as a Union which according to Article 2 TEU is a

[99] Spaventa, E. (2011) *'The horizontal application of fundamental rights as general principles of Union Law.'*, in A constitutional order of states : essays in honour of Alan Dashwood. Oxford: Hart Publishing, pp. 199-218, p. 199 (Introduction).
[100] Bogdandy, A. von (2009), p. 25.
[101] Spaventa, E. (2015) *'a Very Fearful Court: The Protection of Fundamental Rights in the European Union after Opinion 2/13'*, Maastricht Journal of European and Comparative Law, 22(1), pp. 35- 56, p. 40.
[102] Ibid.
[103] GDPR, Recital 10.

society in which pluralism prevails, it must respect diversity and member states' constitutions. Traces of this pluralistic concept of constitutional legal orders can be seen in the Treaties, for e.g. in Article 2, Article 4(2) and Article 6(3) TEU, which declares that the Union is founded on a society in which *pluralism* prevails, that it shall respect member states national identities, inherent in their fundamental and constitutional structures, and that fundamental rights are a result from the constitutional traditions common to the member states. Hence, as the Treaties express that the EU is a society built upon pluralism as one of the fundamental principles,[104] pluralism is a value that like all other fundamental principles of EU law, must be ensured in all external and internal measures taken by the EU.

Pluralism of the EU legal system is also visible in the Charter, in particular, in Article 52(4) and Article 53, the former concerning the scope, and the latter the limits to the Charter. Article 52(4) of the Charter states that "[i]n so far as this Charter recognises fundamental rights as they result from the constitutional traditions common to the Member States, those rights shall be interpreted in harmony with those traditions", and Article 53, holds that "[n]othing in this Charter shall be interpreted as restricting or adversely affecting human rights and fundamental freedoms as recognised […] by the Member States' constitutions."

Moreover, the fact that the EU and its member states all share a common ground of respect for the values enshrined in Article 2 TEU, none of which are able to exist without the protection of fundamental rights, allows for cooperation in the field of fundamental rights. As stated by Spaventa, "[i]t is this (alleged) common basis that is at the heart of the mutual trust (so dear to the Court) between Member States in relation to judicial co-operation […]".[105] So, when the EU aims to create an equivalent level of protection of the fundamental rights and freedoms triggered by the processing of personal data, it must respect the national peculiarities and differences that occur between member states' constitutions, as the goal is not to create an equal, but an *equivalent* level of protection in all member states. This dualism can be perceived in for e.g. Article 85, or Article 9(2)(g) of the GDPR, which allows for national exceptions and derogations from the regulation on the ground of freedom of expression and public interest respectively, to '*customize'* the regulation more towards their national preferences, albeit *within the limits offered by the EU*. This will be further explored in the last Chapter.

[104] TEU, Article 2.
[105] Spaventa, E. (2015) p. 43.

The idea is that the member states constitution and the EU framework can and should co-exist with one another, since the former guarantees the respect for the latter, preventing situations where the two might come in conflict.[106] This is possible since the EU legal order is founded on the fundamental values common to the member states, and "[b]y anchoring the constitutional foundations of the European Union in the constitutional principles common to the Member States", the EU avoids creating conflicts with member states constitutions.[107] That being so, as history tells us,[108] dissimilarities between the EU legal system and member states may occur, and consequently also a question of how extensive the EU's obligation to respect member states national identity and respect pluralism, is. In order to ensure that Union respects member states national identities and constitutional peculiarities and the "authentic interpretation of the national constitutions" are respected by the Court, the EU and the member states should engage in 'constitutional dialogue' in the sphere of fundamental rights. One way for the parties to participate in constitutional dialogue is via preliminary rulings.[109]

There are departing views on how extensive the Union's obligation to respect a single member state's constitutional peculiarities. On the one hand, Leonard Besselink suggests that constitutional pluralism requires a rather wider-ranging obligation for the EU to ensure that the member states constitutional values are respected. In his view, the EU is obliged to respect not only those constitutional values that are *common* to the Member States but also those which are particular to one single Member State.[110] His view is in contrast with Koen Lenaerts, who argue that Article 53 of the Charter should not be interpreted as a rule of conflict between member states constitutions and EU law, but a rule which strengthens pluralism of EU law, as it ensures that EU measures can never replace, restrict or adversely affect fundamental rights as incorporated in member states constitutions.[111]

However, in this context, one must recall for e.g. *Commission v Poland*, where the Court emphasized that the Union "entrusts the responsibility for

---

[106] Opinion of Advocate General Poiares Maduro delivered on 21 May 2008, C-127/07 *Société Arcelor Atlantique et Lorraine and Others v Premier ministre, Ministre de l'Écologie et du Développement durable and Ministre de l'Économie, des Finances et de l'Industrie,* EU:C:2008:292, paras. 16 – 17.
[107] Ibid.
[108] See in particular Melloni and Taricco I and II, presented below in section 2.5.5
[109] Opinion of Advocate General Poiares Maduro delivered on 21 May 2008, C-127/07 *Société Arcelor Atlantique et Lorraine and Others v Premier ministre, Ministre de l'Écologie et du Développement durable and Ministre de l'Économie, des Finances et de l'Industrie,* para. 17.
[110] Besselink, L. F. M. (2014). '*The parameters of constitutional conflict after Melloni.'* European Current Law, 2014(10), p. 1185.
[111] Lenaerts, K. (2012). Exploring the Limits of the EU Charter of Fundamental Rights. European Constitutional Law Review, 8(3), pp 375-403, p. 398 – 399.

ensuring the full application of EU law in all Member States and judicial protection of the rights of individuals under that law to national courts and tribunals and to the Court of Justice".[112] While the Treaties and the Charter 'safeguard' member states constitutional values,[113] member states still have a great responsibility to ensure the full application of EU law, since the EU has a great responsibility to ensure the full application of EU law as a Union based on the rule of law. If member states were able to interpret EU fundamental rights in the light of their national constitutions, the outcome would vary significantly depending on which member state performed the assessment. This would deprive EU law of a consistent application, and thus, would be contrary to the fundamental principles which the EU is founded upon, and in particular, be contrary to the understanding of the EU as a society based on the rule of law.[114]

2.5.4 The CJEU on the relationship between member states constitutions and EU law

The EU framework on data processing aims to harmonise member states data protection legislation to ensure a free flow of personal data and a high level of respect for fundamental rights and freedom, and balances rights of individuals against other legitimate interests, such as the public and controllers.[115] So, while the GDPR allows for some national discretion, as in the already mentioned Article 85 and 9(2)(g), the provisions in the GDPR are meant to represent a 'common European denominator' and not provide much leeway for member states to divert.[116] At the same time, the EU is a Union where pluralism and respect for member states constitutional values must be recognised in the field of fundamental rights.

As the right to be forgotten is, in principle, a reconciliation of the data subject's rights to privacy and data protection and the public's access of information,[117] the balance between those two represents the balance as determined on an EU level, which may be different than that of one single member state, as that the EU's legal system is founded on respect for constitutional pluralism. To shed some light on the legal area in question, we

[112] *Commission v. Poland,* para. 47 and case-law cited therein.
[113] See e.g. TEU, Article 2, Article 4(2) and 6(3) TEU; Charter, Article 52(4) and 53
[114] Opinion of Mr Advocate General Poiares Maduro delivered on 21 May 2008. *Société Arcelor Atlantique et Lorraine and Others v Premier ministre, Ministre de l'Écologie et du Développement durable and Ministre de l'Économie, des Finances et de l'Industrie,* para. 16
[115] GDPR, Recital 10.
[116] Bussche, A. von dem., & Voigt, P. (2017). p. 219
[117] See e.g. *Google Spain; GC and others.*

will look at case law where the CJEU and member states have had a different level of protection for fundamental rights.

2.5.5 When the common EU denominator and a member states' constitutional obligations differ

Melloni from 2013 is a striking example of a situation where a member state offered a more extensive constitutional protection for fundamental rights than the EU framework.[118] In the case, the Spanish Constitutional Court (SCC) asked the CJEU if it was possible to interpret Article 53 of the Charter as allowing a member state to provide a more extensive level of protection for a fundamental right than the one enshrined in EU law to avoid a conflict with its constitutional obligations, an interpretation that was firmly rejected by the CJEU. The Court's legal reasoning for rejecting the interpretation was that such an interpretation would undermine the primacy and effectiveness of EU law, which demands that national provisions that are contrary to EU law or EU objectives must be set aside by member states.[119] Such an act would not only be contrary to the primacy of EU law but also undermine the whole EU legal order, as the primacy of EU law is "an essential feature of the EU legal order" which demands that "rules of national law, even of constitutional order, cannot be allowed to undermine the effectiveness of EU law on the territory of that State".[120] With that said, the Court emphasized it did not deprive the member states of the possibility to apply their national constitutional level of fundamental rights every situation falling inside the scope of EU law, "provided that the level of protection provided for by the Charter, as interpreted by the Court, and the primacy, unity and effectiveness of EU law are not thereby compromised".[121]

The ruling left narrow possibilities for member states to provide more extensive protection for its citizens than the level set on by the EU. The case has therefore been described as a 'wake-up call' for member states in the area of fundamental rights[122] since its implications are that all situations falling into the ambit of EU law must respect the full effectiveness of EU law, even

---

[118] C-399/11 *Melloni*, 26 February 2013, ECLI:EU:C:2013:107.
[119] *Melloni*, para. 59.
[120] Ibid.
[121] *Melloni*, para. 60.
[122] Fransse, V. *'Melloni as a Wake-up Call – Setting Limits to Higher national Standards of Fundamental Rights' Protection'*, posted on 10 March 2014, accessed 2020-01-29 from: https://europeanlawblog.eu/2014/03/10/melloni-as-a-wake-up-call-setting-limits-to-higher-national-standards-of-fundamental-rights-protection/

if it lowers the fundamental rights protection for citizens in one member state. The Court's interpretation of the relationship between the level of fundamental rights guaranteed by the Charter and member states constitutions and constitutional pluralism is in line with how Koen Lenaerts argued that Article 53 of the Charter should be interpreted: that the Union's level can differ from that of a single member state.[123] The stringent obligation for member states to ensure the full effectiveness of EU law, even if it meant lowering the protection of fundamental rights in the territory of one single member state was affirmed in *Taricco I*.[124] In *Taricco I*, the Italian Constitutional Court (ICC) found itself in a situation where their constitutional obligations and their EU obligations were incompatible. Instead of addressing the domestic situation in Italy, the CJEU stressed that since statutes of limitations were not protected by EU fundamental rights, and there was no conflict between the Italian constitution and EU law.[125] By the time *Tarico I* had been adjudicated, there were already two new, similar cases pending before the Italian courts. The ICC, thus, once again, turned to the CJEU, this time emphasizing the practical effect of *Tarico I*; that the Italian courts were forced to either disapply with its constitution or provisions of EU law.

In its response, the CJEU maintained that the situation in hand did not, in principle, infringe the legality principle.[126] However, as VAT offences concerned the financial interests of the Union, which fall within an area of *shared competence* which had not been subject to harmonization, the Court declared that member states remain free to categorize statutes of limitations as falling inside the scope of the legality principle. Thus, Italy could protect statutes of limitations in their constitutional protections of the legality principle and did not need to lower the protection of their fundamental rights, even though letting those accused of VAT fraud go unpunished was not an efficient way to protect the financial interest of the Union. That being so, the Court stressed that it will be a matter of assessment by the Italian courts whether it is necessary to apply the national statute of limitations to ensure the accused individual's fundamental rights, or if it can be disapplied without undermining it. *Taricco II* thus clarified, in conformity with *Åkerberg Fransson* and *Melloni,* that member states remain free to apply national standards of protection of fundamental rights, provided that the level of protection provided for by the Charter, as interpreted by the Court, and the primacy, unity, and effectiveness of EU law were not compromised.[127]

---

[123] Lenaerts, K (2012) p. 398 – 399.
[124] Case C-105/14 *Taricco I,* 8 September 2015, ECLI:EU:C:2015:555.
[125] Ibid, paras 54 - 58.
[126] Case C-42/17 *M.A.S and M.B.* 5 December 2017, EU:C:2017:936 *(Taricco II)* para. 42; *Taricco I* para. 57 and case-law of the cited therein.
[127] *Taricco II*, para. 42 - 47.

After *Melloni* and *Taricco I,* the CJEU was seen adopting a more lenient approach to member states obligation to ensure the effectiveness of EU law in *Taricco II.* This leniency continued in the subsequent *Aranyosi and Căldăraru*,[128] where the Court recognised that member states are required, "save in exceptional circumstances, to consider all the other Member States to be complying with EU law and particularly with the fundamental rights recognised by EU law".[129] However, situations may arise where they fail to do so. If the judicial authority of the executing member state possesses "evidence of a real risk of inhuman or degrading treatment" in the issuing member state, it has an obligation to assess that risk before extraditing an individual,[130] as EU secondary legislation may never "have the effect of modifying the obligations to respect fundamental rights".[131] Thus, in *Aranyosi and Căldăraru*, the Court assured that the effectiveness of EU law cannot lead to an infringement of fundamental rights and that the issuing state has a responsibility to assess certain situations to ensure that individuals fundamental rights are not infringed.[132] Similarly, in *CK*, the CJEU ensured that member states responsibility to comply with harmonized EU legislation may never take away a state's responsibility to respect fundamental rights.[133]

2.6 Conclusion

This chapter of the thesis aimed to answer the question of what the founding principles of the EU are, and why they matter for fundamental rights. As explained in section 2.2, following Article 2 TEU, the Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights. These values are common to the Member States in a society where pluralism prevails. While the EU is not a state, and the Treaties are not a constitution, the Union's claim to respect fundamental rights, democracy and rule of law are characteristics similar to those of a state. As illustrated in section 2.4; if the EU fails to respect the ideological basis of the founding principles, it cannot claim authority over member states constitutions, as this claim rests of the premise that those values will be ensured and protected on the level of EU law. The founding principles of EU law are thus of utter importance for the EU's claim of authority. Thus, the Court's statements in e.g. *Kadi*, where it affirms that there

[128] C-404/15, *Aranyosi and Căldăraru*, 5 April 2016, EU:C:2016:198.
[129] Ibid, para. 88.
[130] Ibid, para. 89.
[131] Ibid, para. 83.
[132] Gill-Pedro, E. & Groussot, X. (2017) p. 271 and 272.
[133] Case C-578/16 *PPU CK and others v Slovenia* EU:C:2017:127, para. 84.

is no EU law, of whatever hierarchy, that can "authorize any derogation from the principles of liberty, democracy and respect for human rights and fundamental freedoms enshrined in Article 6(1) EU [now 2 TEU] as a foundation of the Union"[134] are pivotal in maintaining the member states' trust in the Union as a guardian of the values enshrined in Article 2 TEU. The argument that member states will not comply and accept the EU's claim of authority if it is not governed by rule of law, democracy and respect for fundamental rights is supported not the least by how and why the CJEU incorporated fundamental rights into the EU legal system, but also through the 'conditional' development of the principle of mutual trust.[135]

The EU's respect of the founding principles of EU law has implications for fundamental rights, as shown in section 2.5 In particular, for the right to be forgotten, derived from primary legislation; the fundamental rights of privacy and data protection, Article 7 and 8 of the Charter and access to information as guaranteed by Article 11 of the Charter and the Data directive. The *rationale* behind harmonising the area was to create an equivalent level of protection of the fundamental rights and freedoms of natural persons throughout the EU. Moreover, Article 2 TEU also tells us that the founding values of EU law are common to the member states: which means that in the EU, there are two layers of protection for those values; on an EU level, and in member states constitutions. These two layers coexist. However, by acceding to the EU, the member states have limited their sovereign rights and conferred it to the EU when they act inside the scope of EU law, which, due to the autonomy of EU law as explained by the CJEU in Opinion 2/13, gains interpretational monopoly in those areas. As explained by Spaventa in section 2.5.2, once the scope of EU law is triggered, the CJEU "[…] gains the hermeneutic monopoly over striking the balance between competing rights and interests", which "in turn, means that individuals are no longer protected by their domestic (constitutional) fundamental rights *and* that, lacking accession, they are also no longer protected by the ECHR".[136] As seen in *Melloni* in section 2.5.5 this could lead to lower protection for a citizen in a member state, but that does not change member states obligation to ensure the full effectiveness of EU law. I argued that the 'trend' of conditional development of the principle of mutual trust in areas concerning absolute fundamental rights does not easily translate into areas where non-absolute rights are triggered, where member states obligation to respect the full effectiveness of EU law is still absolute and not conditional. Thus, the importance that the EU strikes the balance right when reconciling rights and freedoms on an EU level cannot be stressed enough.

---

[134] *Kadi*, para. 303
[135] See section 2.5.5
[136] Spaventa, E, (2015), p. 40

3 The Right to be Forgotten

3.1 Introduction

As described in the previous chapter, the EU's founding principles of democracy, the rule of law and fundamental rights are values that need to permeate every measure taken by the Union. The online sphere is no exception to this, where the fundamental rights of privacy, data protection and freedom of expression and information are key prerequisites to create an environment where justice and democracy foster.[137] The rights of privacy and data protection are, thus, "elements of the wider ambitions of the Union to promote the values laid down in Article 2 TEU."[138] While the last Chapter painted the broader picture by explaining the EU legal system, and the founding principles that guide all actions taken in it, this Chapter will present the specific issue that this thesis aims to explore, that is, the right to be forgotten as interpreted in recent case-law by the CJEU. This chapter aims to answer the question of what the right to be forgotten is, and which rights, freedoms, and interests it specifically triggers. To answer this question, it is necessary to start by exploring *Google Spain*, which was the first case where the right was acknowledged in the EU legal system. The Court's reasoning in *Google Spain* is informative and provides important information on how the CJEU views the legal situation that the right triggers. Moreover, the case heavily influenced the subsequent provisions that codified the right to be forgotten in the GDPR.

Before this Chapter begins to explain the right to be forgotten, it may be wise for the reader to visit section 1.6, *Terminology* if he or she is not familiar with the genre-specific terminology of the Data protection framework.

3.2 Historic background – Data protection in the EU

The first data protection adopted by the EU was the Data Directive in 1995, which became the EU's main instrument for data protection until its replacement in 2018 by the GDPR. The Data Directive gave substance to, and amplify the core principles already laid down in the Council of Europe's

[137] Hijmans, H. (2016), p. 17.
[138] Ibid, p. 19.

Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108),[139] which was adopted as a complement to the right to privacy in Article 8 of the ECHR to safeguard automatic processing of personal data.[140] The *rationale* behind the directive was to promote two objectives: the protection of fundamental rights and freedoms of natural persons and their right to privacy with respect to the processing of personal data; and to promote economic progress and trade expansion without restricting nor prohibit the free cross-border flow of personal data in the internal market.[141] These objectives were considered interconnected and dependent on each other, as EU members states would no longer need to hinder the cross-border flow of personal data out of privacy concerns for their citizens.[142]

In accordance with the provisions of the Data Directive, personal data was only allowed to be processed if the general rules on lawfulness, found in Chapter II of the Directive, was fulfilled. The provisions therein stated that processing of personal data was only lawful if such activity upheld the principles on data quality, following Article 6 of the Data Directive: that the data was, *inter alia:* processed fairly and lawfully, collected for specified, explicit and legitimate purposes; accurate and where necessary kept up to date; *and* if one of the criteria stated in Article 7 of the Directive for making data processing legitimate could be invoked. The criteria on legitimate processing were, *inter alia*, if the data subject consented to the processing, or if it was necessary for the purposes of the legitimate interests pursued by the controller, save where such interests are overridden by the rights of privacy and data protection of the data subject. Moreover, the Data Directive offered several rights to the data subject, such as a right to access one's personal data and to object to it being processed. The rights of the data subject aimed to ensure that individuals had control of their personal data being processed so that they felt safe in using the internet.[143] Ensuring a safe environment for the individuals whose data was being processed had been recognised by the EU Commission as a *vital* prerequisite for stimulating economic growth on the

---

[139] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108.

[140] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (consolidated version) [1995] OJ L 281, 23.11.1995, p. 31–50, *(Data Directive)* Recitals 1 and 11.

[141] Data Directive, Article 1 and Recital 1-5.

[142] Lynskey, O. (2015) The foundations of EU data protection law (1st eds). Oxford University Press 2015, p. 46.

[143] European Commission, (2012) '*Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions: Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century*', COM/2012/09 final, 25 January 2012, p. 4.

EU market, as "concerns about privacy are among the most frequent reasons for people not buying goods and services online."[144]

3.3 C-131/12 *Google Spain*: The CJEU established a right to be forgotten

Nearly 20 years after the Data Directive was adopted, in 2014, the CJEU was asked in *Google Spain* to interpret the Directive's provisions concerning the responsibilities for search engines vis-à-vis the data subject's rights to have effective control over their data. The case concerned a Spanish national, who lodged a complaint in 2010 with the Spanish DPA against a Spanish newspaper, Google Spain and Google Inc, to remove or alter, either the links to or the original website of two news pages dating back to 1998, which mentioned a real-estate auction for the recovery of old social security debts that appeared following a search on his name. The Spanish DPA rejected his request to remove the information from the newspaper but upheld it against Google Spain and Google Inc, who both refused and brought actions against the decision, whereas the National High Court of Spain stayed proceedings and asked the CJEU for a preliminary ruling.[145]

While the Spanish Court brought several questions to the CJEU, we shall focus on those relevant to the scope of this thesis. Prior to *Google Spain,* the provisions of the Data Directive that allowed for lawful processing of personal data had not been applicable to SEOs; amongst other reasons, as they had not been considered 'controllers', and their activity had not been considered 'processing' within the meaning of the Directive. The CJEU was thus asked to clarify whether SEOs could be considered 'controllers' if the data was being processed under a Google search and if individuals had a right, following the provisions of the Directive to either demand that the data was erased or object to it being processed.

3.3.1 The opinion of AG Jääskinen

First and foremost, the AG argued that SEOs should not be forced to comply with the provisions of the Data Directive.[146] In the opinion of Advocate General Jääskinen, he argued that the "reasonable interpretation of the Directive" precluded SEOs from being considered 'controllers' within the meaning of the Directive following Article 2(d). In particular, as this would

[144] Ibid, p. 5.
[145] Google Spain, paras. 14 - 20.
[146] Opinion of Advocate General Jääskinen delivered on 25 June 2013, C-131/12 *Google Spain*, EU:C:2013:424 *(Opinion AG Jääskinen, Google Spain).*

lead to its activity by default becoming incompatible with the Data Directive in a situation where the links shown on display contained what is called 'special categories of data', described in Article 8(1) and (5) of the Directive as data revealing political opinions or religious beliefs or data concerning the health or sex life of individuals. The activity of a SEO would by default become incompatible with the data protection framework of the EU "when the stringent conditions laid down in that article [Article 8] was not fulfilled", a conclusion he finds "absurd".[147]

Furthermore, even if the Court ruled that SEOs were 'controllers', the AG still advised against deriving a 'right to be forgotten' from the provisions of the Data Directive. His concern was that such a right would not represent a fair balance of the rights and interests triggered by such a request, in particular with respect to internet user's access to the information. AG Jääskinen recognised that such request would be interfering with the fundamental freedom of expression and information enshrined in Article 11 of the Charter[148] and that there is a virtue for the EU to act cautiously when restricting access to information online, which "the internet has revolutionized access to and dissemination of".[149] By using a search engine, an internet user is "*actively using his right to receive information concerning the data subject from public sources* for reasons known only to him", which "[…] constitutes one of the most important ways a person can exercise this fundamental right in a contemporary information society". In his opinion, it would be unwise for the EU to restrain that freedom,[150] "especially in view of the ever-growing tendency of authoritarian regimes elsewhere to limit access to the internet or to censure content made accessible by it."[151] On those grounds, AG Jääskinen concluded that:

> "The particularly complex and difficult constellation of fundamental rights that this case presents prevents […] imbuing it [the Data Directive] with a right to be forgotten. This would entail sacrificing pivotal rights such as freedom of expression and information. I would also discourage the Court from concluding that these conflicting interests could satisfactorily be balanced in individual cases on a case-by-case basis, with the judgment to be left to the internet search engine service provider. Such 'notice and take down procedures', if required by the Court, are likely either to lead to the automatic withdrawal of links to any objected contents or to an unmanageable number of requests handled by the most popular and important internet search engine service providers."[152]

[147] *Opinion AG Jääskinen, Google Spain*, para. 89 - 90.
[148] Ibid. para, 128.
[149] Ibid. para, 121.
[150] Ibid, paras. 130 - 131.
[151] Ibid, para. 121.
[152] Ibid. para. 133.

3.3.2 The CJEU's legal assessment

The Court did not follow the opinion of AG Jääskinen. First and foremost, the Court ruled that SEOs must comply with the grounds for lawful processing in the Data Directive,[153] as another outcome would "compromise the directive's effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to ensure […] in particular their right to privacy, with respect to the processing of personal data, a right to which the directive accords special importance".[154] After affirming that the Data Directive was indeed applicable to SEOs, the CJEU moved on to scrutinize the extent of the responsibility for SEOs in the Data Directive. In particular, the Court assessed if SEOs have an "obligation to remove [a link] from the list of results displayed following a search made on the basis of a person's name links to web pages", even if the personal information those links led to had been lawfully published by third parties.[155]

In accordance with the provisions of the Data Directive, the only legal basis that could allow a SEO to lawfully process personal data was Article 7(f) of the Data Directive, which permitted processing only if it was *necessary for the purposes of the legitimate interests pursued by the controller save where such interests were overridden by the rights of privacy and data protection of the data subject*.[156] As the data subject's right to privacy and data privacy are fundamental rights protected in the Charter, the CJEU ruled that the assessment referred to in Article 7(f) of the Directive needed to be performed *in the light of* those fundamental rights, and be "balanced against the opposing rights and interests concerned […] in the context of which account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter".[157]

On the balancing of the opposing rights and interests triggered by such a request, the Court ruled that, given that the results of a search on a data subject's name provided a "more or less detailed profile of the data subject […] the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous".[158] The interference of the data subject's rights of

[153] *Google Spain*, paras. 41 and 60.
[154] Ibid, para. 58.
[155] Ibid, para. 62.
[156] Ibid, para. 73 – 74.
[157] Ibid, para. 74 and case-law cited therein.
[158] Ibid, para. 80.

privacy and data protection thus "cannot be justified by merely the economic interest which the operator of such an engine has in that processing", but must "override, as a general rule, that interest of internet users, that balance may, however, depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life."[159]

The last issue for the Court to assess was when such a right could be triggered, and if it was sufficient that the information was merely prejudicial to the data subject, and that he or she, therefore "wished it to be 'forgotten' after a certain time".[160] This was also affirmed by the Court, which ruled that "even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed" which would, in particular, be the case "where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed."[161] Hence, the Court declared that data subject's had a right to, on the basis of Article 12(b), and 14(a) of the Data Directive, ask a SEO to erase links, and/or object to the links being put on display after a search on the basis on the data subject's name, even if those links led to websites that had been lawfully published and contained true information. Additionally, the Court ruled that the data subject's right to have the information removed would *by default* override both SEO's economical interest to process the information, and internet user's interest in accessing the information, save be in situations where the processing of the information would be "justified by the preponderant interest of the general public in having […] access to the information in question".[162]

3.3.3 *The reactions that followed* Google Spain

The main critique that *Google Spain* received after it was published centred around the problems that were highlighted in the AG's opinion, such as the complexity of properly balancing the relevant rights and interests triggered in the situation.

[159] Ibid, para. 81.
[160] Ibid, 89.
[161] Ibid, para. 93.
[162] Ibid, para. 97.

The interplay between the protection of private life and freedom of expression has been up for assessment several times by the ECtHR,[163] which on numerous occasions has stressed that "particularly strong reasons must be provided for any measure limiting access to information which the public has the right to receive".[164] Therefore, it was of particular concern that the Court did not acknowledge that the rights balanced against each other was neither absolute not in any hierarchical order,[165] and, as a matter of principle, deserve equal respect.[166] E.g. the Organisation for Security and Cooperation in Europe's Representative on Freedom of the Media, Dunja Mijatović, issued a press statement warning that the decision "might negatively affect access to information and create content and liability regimes that differ among different areas of the world, thus fragmenting the Internet and damaging its universality."[167] Mijatovic expressed concerns over the implications of the judgment, since "information and personal data related to public figures and matters of public interest should always be accessible by the media and no restrictions or liability should be imposed on websites or intermediaries such as search engines. If excessive burdens and restrictions are imposed on intermediaries and content provides the risk of soft or self-censorship immediately appears."[168]

On a similar note, as stated by Steve Peers in his blog post *"The CJEU's Google Spain judgment: failing to balance privacy and freedom of expression",* published the same day:

> "The essential problem with this judgment is that the CJEU concerns itself so much with enforcing the right to privacy, that it forgot that other rights are also applicable."[169]

Steve Peers' argument accentuates the key issue of the CJEU's reasoning, as the ruling did not refer to freedom of expression and information, even though the Directive expressly requires a balance of the rights of third parties to whom the data are disclosed,[170] or to case-law on how to best balance privacy

---

[163] *Węgrzynowski and Smolczewski v. Poland*, 16 July 2013, no. 33846/07, CE:ECHR:2013:0716JUD003384607, para. 56.
[164] Ibid, para. 57.
[165] Parliamentary Assembly of the Council of Europe, Resolution no. 1165 (1998) *'Right to Privacy'*, of 26 June 1998 on the right to privacy, p. 11.
[166] *Axel Springer AG v. Germany*, 7 February 2012, No: 39954/08, CE:ECHR:2012:0207JUD003995408, para. 87 and caselaw cited therein.
[167] Organisation for Security and Co-operation in Europe, (2014) *Communiqué by the Representative on Freedom of the Media on ruling of the European Union Court of Justice*, issued on 16 May 2014.
[168] Ibid.
[169] Peers, S. (2014) *"The CJEU's Google Spain judgment: failing to balance privacy and freedom of expression"*, Published 13 May 2014, accessed 2020-01-17 from: http://eulawanalysis.blogspot.com/2014/05/the-cjeus-google-spain-judgment-failing.html
[170] Data Directive, Article 7(f).

and freedom of expression. Whereas a balance would require an actual assessment of the two rights, this seems to be missing when the Court without much consideration declared that one right by default overrules the other.[171] This was also the main point of criticism brought forward by Eric Schmidt, Google's executive chairman at the time, who commented that the ruling was:

> "[…] a collision between a right to be forgotten and a right to know. From Google's perspective that's a balance. Google believes, having looked at the decision, which is binding, that the balance that was struck was wrong."[172]

Similarly, in an article from 2014, Eleni Frantziou expressed criticism on the lack of clarification of what the data subject's right to be forgotten entailed.[173] Despite the Court's emphasis on the importance of balancing the fundamental rights triggered by a request for erasure, this Court did not properly engage in fundamental rights reasoning. Frantziou shed light on the fact that the Court mislabelled the right to access information, with is a guaranteed under freedom of expression and information in Article 11 of the Charter, by referring to it as a *general interest*. The terminology wrongfully implies that the former is a norm of constitutional value, and the other one is not, while both norms are enshrined in the Charter and have equivalent value. The judgment thus indicates an internal hierarchy that does not exist. According to Frantziou, this *error in terminology* leads to "a presumption of non-applicability and hence fails to take account of its equal weight in the 'fair balance' discussion."[174]

Moreover, given the complexity of the assessment, and the fact that it will be performed by a private company driven by profit, the request of erasure may "risk being met not with more careful balancing of competing rights but, rather, with the option that best serves the primary goals of these undertakings, that is, the method which is most cost-effective".[175] Furthermore, as SEO:s are private companies, she observes that it will be impossible to monitor whether an SEO strikes the balance correctly on a case-by-case basis, or if different SEO's strike the same balance. If not, Frantziou

---

[171] Peers, S. (2014) *"The CJEU's Google Spain judgment: failing to balance privacy and freedom of expression"*.

[172] Quote from the following article: Arthur, C. *"Google faces deluge of requests to wipe details from search index"*, published 15 May 2014, accessed 2020-01-17 on: https://www.theguardian.com/technology/2014/may/15/hundreds-google-wipe-details-search-index-right-forgotten

[173] Frantziou, E. (2014). *'Further Developments in the Right to Be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos.'* Human Rights Law Review, 14(4) pp. 761-777.

[174] Ibid, p. 769.

[175] Ibid, p. 769 – 770.

predicts a similar conclusion as AG Jääskinen; that the data subject's right to be forgotten may interfere with the public's right to access information.[176]

3.3.4 *Article 29 WP issued* Guidelines

Following *Google Spain,* the Article 29 Working Party (*Article 29 WP*), which at the time was the European advisory body on data protection and privacy (now called the European Data Protection Board (*EDPB*)), published guidelines that aimed to clarify the CJEU's judgment of Google Spain.[177] The *Guidelines* were, more or less, an extended version on the Court's case, but also issued a set of criteria, none in itself determinative, which the Article 29 WP "strongly encouraged" SEOs to use when balancing the public's interest against the data subject.[178]

The Article 29 WP did, however, provide some comments on the balancing on the rights and freedoms triggered by a request to be forgotten by a data subject, by specifically emphasizing that "the impact of the exercise of individuals' rights on the freedom of expression of original publishers and users will generally be very limited". Even so, the Article 29 WP noticed that "[s]earch engines must take the interest of the public into account in having access to the information in their assessment of the circumstances surrounding each request. Results should not be de-listed if the interest of the public in having access to that information prevails."[179] Important to note, is that the *Guidelines* did, as AG Jääskinen, take into consideration the fact that the right to be forgotten would interfere with freedom of expression and access to information is protected by Article 11 of the Charter, albeit arguing that the impact on the right would be very limited. The EU body was of the same opinion of the Court, and deemed that "[i]n practice, the impact of the de-listing on individuals' rights to freedom of expression and access to information will prove to be very limited".[180]

---

[176] Ibid, p. 770 and 775 – 777.

[177] Article 29 Working Party, (2014) *'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-131/13'*, 14/EN WP 225, Adopted on 26 November 2014.

[178] Article 29 WP, (2014), *Guidelines* p. 3 and p. 12 and forward.

[179] Article 29 WP, (2014), *Guidelines*, p. 6

[180] Article 29 WP, (2014), *Guidelines* p. 2

3.4 The right to be forgotten codified in the GDPR

Two years after *Google Spain*, the Data Directive was replaced by the General Data Protection Regulation (the GDPR), which was adopted on 27 April 2016. While the objectives and principles of the Data Directive remained solid, its implementation had caused a fragmented framework of data protection across the Union. Those differences between member states, in particular in the right to the protection of personal data, was considered a hinder to the free flow of personal data throughout the Union. Thus, the EU changed the approximation method from a directive to a 'general regulation', which effectively omits the need for implementation by being directly applicable in all member states.[181] However, while the GDPR does not *require* any transformative act to be binding for the member states, as we shall see, it *allows* for some national variation due to its several 'opening-clauses' where member states may implement national legislation in specific areas.[182] These opening clauses, as we will return to in section 4.4.3, are of utter importance when we are discussing the implications on the founding principles of EU law following *Google CNIL* and *GC and others*, as they *explicitly leave room for member states to deviate from the GDPR*. The opening clauses will entail national differences and effectively prevent a consistent level of data protection throughout the EU.[183] Consequently, "[a]s the respective national laws are likely to differentiate data protection-wise between the EU Member States, entities should be very attentive as regards the occurrence of national peculiarities" which is found in these opening clauses.[184]

The GDPR codified the right of erasure of data in Article 17, and the right to object to the processing of such data in Article 21, which shall be explored in the section below. But before outlining the two provisions, it is necessary to note that what is referred to, especially in media,[185] as a 'right to be forgotten' is in fact composed of two separate rights: a right to have the personal data in question erased, and a right to object to the processing of it.[186] The following section will be a description of the current provisions that codify the right to

[181] GDPR, Recitals 9 and 10.
[182] GDPR, Article 85 – 91 of the GDPR; Bussche, A. von dem., & Voigt, P. (2017). *'The EU general data protection regulation (GDPR): a practical guide',* Springer International Publishing AG, 2017, p. 219.
[183] Ibid, (2017), p. 223.
[184] Ibid, p. 219.
[185] See e.g. https://www.theguardian.com/technology/2019/sep/24/victory-for-google-in-landmark-right-to-be-forgotten-case; https://www.bbc.co.uk/news/technology-49808208
[186] GDPR, Article 17 and 21.

erasure, and the right to object in GDPR. However, before embarking on the process of describing the provisions one can have in mind that since one of the grounds for the *erasure* of data is *when the data subject objects* to the processing, the line between the two (although) separate rights is *somewhat* blurred, and not the most important since the outcome is the same for the internet user, irrespectively of which provision is invoked by the data subject, the information is no longer shown following a search on the data subjects name.

3.4.1 Article 17 of the GDPR: The right to erasure

Article 17 of the GDPR offers the data subject a right to have personal data concerning him or her, without undue delay, erased where the retention of such data fulfils one of the six listed criteria in 17(1): (1) the personal data are no longer necessary in relation to the purpose for which they were processed; (2) the data subject *no longer consents* to the processing; (3) the data subject *objects* to the processing; (4) the personal data have been *unlawfully published*; (5) the personal data have to be erased for compliance with a *legal obligation*, or (6) the personal data have been collected in relation to the offer of information society services. According to the recitals to the GDPR, erasure should *especially* be approved if the information is no longer necessary in relation to the purpose for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing, or where the processing does not otherwise comply with the regulation.[187] The right of the data subject to request erasure of his or her personal data corresponds with the SEO's obligation to remove the data, that is, as the former triggers the latter. The burden of proof is thus on the data subject requesting the data to be erased by invoking one of the grounds listed in Article 17(1).[188] As the provision describes a *subjective* and not an *objective* right, the data subject must specify which ground he or she invokes to exercise his or her right to be forgotten, and, depending on which ground he or she invokes, provide additional circumstances to strengthen the claim for erasure. However, this 'burden of proof' is not excessive, since one of the grounds provided for the data subject to have the data erased is to expressly withdraw consent to the processing and may thus be fulfilled by a simple request.[189]

The request of a data subject to invokes his or her right to erasure, supported by one the grounds in Article 17(1), does not equate an automatic obligation

[187] GDPR, Article 17(1) and Recital 65.
[188] Bussche, A. von dem., & Voigt, P. (2017). p. 159.
[189] Ibid, p. 159.

for a controller to erase the data. The criteria have to be read in conjunction with Article 17(3), which prevents erasure if it is necessary for, amongst other grounds listed in the paragraph, the right of freedom of information for internet users.[190] Together, the paragraphs guarantee that the data subject's right to have personal data erased or modified is balanced against the counterfeiting interests requiring further retention of the data before the request is granted,[191] something that must be performed on a case-by-case basis, a responsibility resting on the controller, which thus carries the burden of proof for the exception invoked.[192]

3.4.2 Article 21 of the GDPR: The right to object

If the lawfulness of processing personal data is based on the *legitimate interest* of the controller, as the processing of personal data by search engines is,[193] data subjects always have a right to object, at any time, to the processing. The controller then has an obligation to stop the processing unless it demonstrates "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claim",[194] that is, grounds "so important that the purposes of processing cannot be achieved without the processing activities that the data subject objected to".[195] The article is primarily meant to target situations where the data processing is lawful per se, but the data subject no longer wants it to be processed and is triggered when '*new circumstances* that *influence the initial balancing of interests*' arise, shifting the balance in favour of the data subject's right to privacy and data protection. The provision "cannot be interpreted extensively" – as this would undermine the legal bases for processing for controllers – but should regard specific situations.[196] But compared to the Data Directive, which also contained a right for data subjects to object,[197] the right to object in the GDPR is clearly enhanced, and is meant to have a greater chance of success when invoked.[198]

[190] GDPR, Article 17(3)(a).
[191] GDPR, Recital 65.
[192] Bussche, A. von dem., & Voigt, P. (2017). p. 161.
[193] *Google Spain* paras. 72 – 73.
[194] GDPR, Article 21(1).
[195] Bussche, A. von dem., & Voigt, P. (2017), p. 178.
[196] Bussche, A. von dem., & Voigt, P. (2017), p. 177.
[197] Data Directive, Article 14(a).
[198] Bussche, A. von dem., & Voigt, P. (2017). p. 177.

3.5 What rights and freedoms are especially triggered by a request to be 'forgotten'?

As mentioned in *Google Spain*, the subsequent *Guidelines* and the critique that followed, and the codification of the right to be forgotten in the GDPR, the right to be forgotten illustrates a reconciliation of the rights of privacy and data protection and the right to access information as guaranteed by freedom of expression and information. Consequently, in order to understand the implications of a request to be forgotten, which is the focal point of *Google CNIL* and *GC and others*, we must explore the core values that are triggered by such a request. This section thus aims to explore the competing rights and interests that must be reconciled for a request of personal data to be erased from the result of a search engine. As described in the previous chapter, the rights of privacy and data protection and freedom of expression and information are intrinsically linked, and together enables the creation of a society which respects fundamental rights, democracy, and rule of law. As recognised by the AG Kokott in his opinion on *Satamedia,* a "[s]trict application of data protection rules could substantially limit freedom of expression",[199] a freedom that "constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded."[200] Moreover, as I argued in the conclusion to Chapter 2, the EU's claim of authority is dependent on the fact that these values are respected.

The need for co-existence and reconciliation of the two rights was recognized early by the CJEU, e.g. in one of the first cases on the Data Directive, *Lindqvist*, where the Court stressed that individuals need to be free to express their opinions by placing information on the internet, even if it may lead to the disclosure of personal information about others.[201] The balance has amounted to a considerate body of case law under both the ECHR and the CJEU. It is important to note that, as a starting point, case-law emphasize that the rights deserve equal respect.[202]

---

[199] Opinion of Advocate General Kokott delivered on 8 May 2008, C-73/07 *Satamedia,* EU:C:2008:266 Para. 43.
[200] *Tele2 Sverige*, para. 93.
[201] C-101/01 *Lindqvist*, 6 November 2003, EU:C:2003:596, para 86.
[202] *Delfi AS v. Estonia,* 10 October 2013, no. 64569/09, CE:ECHR:2013:1010JUD006456909, para. 138 and case-law cited therein.

3.6 Article 7 and 8 of the Charter: The fundamental rights to privacy and protection of Personal Data

Article 8(1) of the Charter states that: "[e]veryone has the right to the protection of personal data concerning him or her"; 'everyone' being all alive, natural persons.[203] The wording of Article 8 of the Charter codifies, and highlights, the core values associated with the right: that processing of personal data, must be *fair* and *for specified purposes*, be based on either *consent* or some other *legitimate basis laid down by law*, and must ensure everyone a right to access and/or rectify their personal data.[204] To ensure that those conditions are complied with, all member states must establish independent authorities to exercise control and safeguard the rights therein. In the EU, those authorities are called Data Protection Agencies (DPAs).[205]

The right to data protection is closely related to the right to respect for private life,[206] as both strive to protect related values; the autonomy and human dignity of individuals by ensuring that they are free to develop their personalities, thoughts, and opinions.[207] However, the right to data protection is more inclusive than the right to respect for private life, as it covers all information that constitutes 'personal data' and is triggered by any type of processing, while protection of private life requires an actual impact on a person's private life to be triggered.[208] With that said, most international instruments (except the Charter) does not recognise the right to protection of personal data as a self-standing right, but rather as a part of a person's private life.[209] Article 8 of the Charter, therefore, does not have a correspondent provision in the ECHR, which is instead a part of the right to respect for private and family life, as guaranteed by Article 8 of the ECHR, as guided, complemented and reinforced by the Convention 108 on data processing.[210]

---

[203] GDPR, Article 1 and Recital 27.

[204] European Union Agency for Fundamental Rights and Council of Europe (2018) '*Handbook on European data protection law – 2018 edition*', Published 24 May 2018, accessed 2019-12-03 from https://fra.europa.eu/, p. 19.

[205] Charter, Article 8.

[206] *Volker and Schecke*, para. 47.

[207] European Union Agency for Fundamental Rights and Council of Europe (2018), p. 19.

[208] Ibid, p. 20

[209] Kranenborg. H. (2014) *'Article 8 Protection of Personal Data'*. In Peers, S., Tamara, H., Kenner, J., Ward, A. (Eds) (2014), *The EU Charter of Fundamental Rights: A Commentary.* Oxford: Hart Publishing, 2014. p. 228.

[210] See e.g. *Z v. Finland,* 25 February 1997, no. 22009/93, CE:ECHR:1997:0225JUD002200993, para. 95; *Explanations to the Charter* (2007) Explanations on Article 7 and 8 of the Charter.

Even though the ECHR does not have an independent provision for data protection that Article 8 of the Charter, it is closely connected to Article 7 of the ECHR. This can be seen, e.g. in the *Explanations to the Charter,* which hold that the meaning and scope of Article 7 of the Charter, i.e. the right to privacy, correspond to and have the same limitations as Article 8 of the ECHR and that Article 8 of the ECHR is cited as one of the provisions that Article 8 of the Charter is based on.[211] Moreover, following Article 52(3) of the Charter, in so far as it contains rights which correspond to rights guaranteed by the ECHR, that level shall constitute the minimum level of protection guaranteed by the Charter, which can always prove more extensive protection.[212] Thus, when exploring the minimum protection that must be upheld by the EU, the ECHR provides guidance.

What is protected in a person's private life is extensive and not susceptible to an exhaustive definition.[213] In case-law, the ECtHR has departed from a classical interpretation of 'privacy' as a 'right to be left alone'[214] and allowed it to protect a more extensive sphere. The ECtHR has stated that the provision cannot be restricted to only protect the "inner circle" of a person's life,[215] but "the physical and psychological integrity of a person and can embrace multiple aspects of a person's identity, such as gender identification and sexual orientation, name or elements relating to a person's right to their image",[216] including activities of a professional or business nature.[217] The core of what must be protected is individuals' right to "establish and develop relationships with other human beings".[218] The data subject must not be mentioned by name for his or her integrity to be compromised, the decisive factor is whether he or she can be identified. In *Scarlet Extended,* the CJEU held that users' IP addresses are 'personal data' and must thus be processed in accordance with Article 8 of the Charter since the address allow those users to be precisely identified.[219] The information gathered on the person does not need to be sensitive, nor an inconvenience to him or her in any way to constitute 'private data',[220] the mere storing of data relating to the private life

---

[211] *Explanations to the Charter,* (2007) Explanations on Article 7 and 8.
[212] Charter, Article 52(3) and Article 53.
[213] *M.L and W.W v. Germany*, para 86 and case-law cited therein.
[214] Kranenborg. H. (2014), p. 228.
[215] *Niemietz v. Germany,* 16 December 1992, no. 13710/88 CE:ECHR:1992:1216JUD001371088, para 29.
[216] *M.L and W.W v. Germany*, para. 86.
[217] *Amann v. Switzerland*, 16 February 2000, no. 27798/95, CE:ECHR:2000:0216JUD002779895, para. 65.
[218] Ibid.
[219] CJEU, C-70/10, *Scarlet Extended*, 24 November 2011, EU:C:2011:771 para. 51.
[220] *Amann v. Switzerland,* para 70.

of an individual amount to an interference with his or her right to respect for private life.[221]

3.6.1 *Interferences must be provided for by law and be necessary in a democratic society*

The CJEU has recognized that the right to protection of personal data, following Article 8(2) and 52(1) of the Charter, is not an absolute right but must be considered in relation to its 'function in society'.[222] However, derogations and limitations to the right must apply *only in so far as strictly necessary*.[223] According to Article 52 of the Charter, interferences must be laid down by law, and can only be imposed if necessary and proportionate in a democratic society, to safeguard public security or other important objectives of general public interest of the Union or a Member State, in particular, to protect the rights and freedoms of others. The 'general interests' are the objectives of the EU, i.e. those interests enshrined in Article 3 TEU – *inter alia* to establish an area of freedom, security and justice, and an internal market, and the 'other' rights and freedoms are the other ones enshrined in the Charter.[224] Those restrictions should be in accordance with the requirements set out in the Charter and in the ECHR.[225]

3.7 Article 11 of the Charter: Freedom of expression and information

Freedom of expression and information sometimes referred to as *freedom of speech,* is a widely recognised fundamental human right which "constitutes one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded.[226] Article 11(1) of the Charter guarantees that:

> "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."

In accordance with the *Explanations to the Charter*, the meaning and scope of Article 11 of the Charter corresponds with Article 10 of the ECHR and, in

---

[221] *Leander v. Sweden*, 16 February 2000, no. 9248/81 CE:ECHR:1987:0326JUD000924881
[222] Volker und Schecke, para. 48.
[223] Case C-73/07 *Satamedia*, 16 December 2008, EU:C:2008:727, para. 56.
[224] *Explanations to the Charter* (2007), Explanation on Article 52; TEU, Article 3.
[225] GDPR, Recital 73.
[226] Tele2 Sverige, para. 93.

accordance with Article 52(3) of the Charter, has the same meaning and scope.[227]

The provision does not only guarantee individuals the freedom to express ideas that are uncontroversial but also those that may be regarded as critical, controversial, shocking, offending or disturbing, as "such are the demands of that pluralism, tolerance and broadmindedness without which there is no democratic society".[228] The right protects legal as well as natural persons,[229] irrespective of the aim pursued by the expression or opinion, is profit-making or not.[230] What is protected by the term 'expression' is not defined, but the spectra of activities that enjoy the protection of the right are broad. It includes oral communications as well as written, printed or in electronic form,[231] images, and music,[232] and extends to the substance of the ideas and information expressed as well as the form in which they are conveyed.[233] However, not all expressions or opinions are protected. The ECtHR has declared that speech "incompatible with the values proclaimed and guaranteed by the Convention is not protection by Article 10", such as all forms of expression which incite to racial hatred, xenophobia, antisemitism and all forms of intolerance,[234] such as statements denying the Holocaust, justifying a pro-Nazi policy, linking all Muslims with grave acts of terrorism, or portraying the Jews as the source of evil in Russia.[235]

3.7.1 Freedom of expression and information and state interference

Although the main method used to achieve freedom of expression and information is that states and public authority *refrain* from interfering with the right, it may trigger positive obligations that *promote* state interference if

[227] *Explanations to the Charter,* (2007) Explanation on Article 11.
[228] *Axel Springer AG v. Germany*, para. 78 and case law cited therein.
[229] Woods, L. (2014) *'Article 11 Freedom of Expression and Information'.* In Peers, S., Tamara, H., Kenner, J., Ward, A. (Eds) (2014), *The EU Charter of Fundamental Rights: A Commentary.* Oxford: Hart Publishing, 2014, p. 321.
[230] *Neij and Sunde Kolmisoppi v. Sweden,* 19 February 2013, no. 40397/12, CE:ECHR:2013:0219DEC004039712.
[231] Opinion of Advocate General Trstenjak delivered on 24 November 2010, MSD Sharp & Dohme GmbH v Merckle GmbH. ECLI:EU:C:2010:712, para. 81.
[232] Woods, L. (2017) *'Chapter 18: Digital freedom of expression in the EU',* in, Douglas-Scott, S., & Hatzis, N (eds). *'Research handbook on EU law and human rights',* 2017, Edward Elgar Publishing Limited, p. 395.
[233] *Gough v. The United Kingdom,* 28 October 2014, no. 49327/11 CE:ECHR:2014:1028JUD004932711, para. 149.
[234] Recommendation No. R (97) 20 of the Committee of Ministers to member states on "hate speech", Adopted by the Committee of Ministers on 30 October 1997.
[235] Delfi AS v. Estonia, no. 64569/09, ECLI:CE:ECHR:2013:1010JUD006456909, para. 136 and the case-law cited therein.

necessary to prevent private actors from restricting the exercise of the freedom by others or to achieve certain goals.[236] This was seen in *Editorial Board of Pravoye Delo and Shtekel v. Ukraine,* where the ECtHR ruled that states have a positive obligation to create a sufficient legal framework to guarantee journalists freedom of expression on the internet.[237] States have positive and negative obligations to ensure that it is safe to *speak*, *share opinions* and *receive information* for *everyone*, through *all communication media* inside their territories, including the Internet and social media platforms.[238]

3.7.2 Access to information and search engines

Based on the nature of search engines' activities,[239] its impact on democracy is *indirect* rather than *direct,* as search engines in themselves do not 'create' information, but index information that is already available on the Internet.[240] SEOs' 'indirect effect' on democracy does not, however, equate a weak effect,[241]on the contrary, SEOs play a pivotal role in the information society, as they "emerge as critical chokepoints on the internet" acting as the intermediary between the information available on websites and internet users, fostering access to information and participation in our society and hence affect democratic discourse.[242] SEOs are, in particular, vital for rendering information and ideas on the Internet accessible to a worldwide public and enable the publics' possibility to seek, receive, and impart information and ideas in order to acquire knowledge, engage in debate and participate in democratic processes and thus, are liable to interfere with the freedom of expression and information.[243] In 2017, the Committee of experts on internet intermediaries from the Council of Europe published a report where they referred to search engines as 'gatekeepers' for persons who wish to seek, receive, or impart information in today's society; as content that are not listed high, or shown at all, in search engines' indexes is less likely to reach a large audience or to be seen at all.[244] The Committee acknowledged

[236] Woods, L. (2014) p. 324.
[237] *Editorial Board of Pravoye Delo and Shtekel v. Ukraine,* paras. 64 – 66.
[238] Akdeniz. Y, Commissioned by the Office of the OSCE Representative on Freedom of the Media, (2016) *'Media Freedom on the Internet: an OSCE Guidebook'*, March 2016, accessed 2020-03-11 from: https://www.osce.org/netfreedom-guidebook?download=true p. 103.
[239] See section 1.6.
[240] Laidlaw, E. (2015) p. 172 and 174.
[241] Ibid.
[242] Ibid. p. 176.
[243] Recommendation CM/Rec(2012)3 of the Committee of Ministers to member States on the protection of human rights with regard to search engines (Adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies), para. 1 – 4.
[244] MSI-NET, Committee of experts on the internet intermediaries, "Meeting report" (6 October 2017), MSI-NET (2017)06, Appendix 4 "Final draft study on the human rights

an increase in concern for search engines', and the potential harm it could have for freedom of expression of individuals, groups and whole segments of societies; mot only for the individual's right to be able to freely express himself but also with respect to "the inherent aim of Article 10 [ECHR] of creating an enabling environment for pluralist public debate that is equally accessible and inclusive to all."[245]

Given their prominent role in facilitating public access to information, there exists a need to "protect and promote access, diversity, impartial treatment, security and transparency in the context of search engines."[246] Although the removal of specific links from search engine indexes in certain situations may be necessary in order to respect the right of privacy and protection of personal data for individuals, such removal must be governed by transparent and narrowly tailored requirements which must be reviewed regularly subject to compliance.[247] Therefore, the Council of Europe has recommended its member states to ensure that when state authorities or private-sector actors take measures to block, filter or remove content from the internet, they must ensure that those actions comply with the requirements of legality, legitimacy, and proportionality that presuppose the validity of restrictions to the right to freedom of expression and information.[248]

3.7.3 Restrictions on freedom of expression and Information on the Internet

Both Article 11 of the Charter and Article 10 ECHR are subject to exceptions, found in Article 52(1) of the Charter and Article 10(2) of the ECHR respectively. Limitations that may be lawfully imposed are thus the same for Article 11 of the Charter as those provided for in Article 10(2) of the ECHR.[249] So, when the CJEU explores the minimum level of freedom of expression and information that needs to be guaranteed by Article 11 of the Charter, it does so on the basis of Article 10 ECHR, as clarified and interpreted by ECtHR's case law.[250] Moreover, the CJEU only allows for restrictions that do not undermine the 'substance' or 'essence' of the right.[251]

---

dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications", p. 35 - 36.

[245] Ibid.

[246] Recommendation CM/Rec(2012)3, para. 6.

[247] Recommendation CM/Rec(2012)3, paras. 12 – 14.

[248] Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom, 13 April 2016, section 2.

[249] Woods, L. (2017) p. 399.

[250] *Explanations to the Charter* (2007) Explanation on Article 11.

[251] *Wachauf,* para. 18.

Given that freedom of expression constitutes “one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual’s self-fulfilment”, interferences with the right must be interpreted strictly and established convincingly.[252] Restrictions must be properly balanced in accordance with a three-step test following Article 10(2) of the ECHR, i.e. (1) be prescribed by law, (2) pursue a ‘legitimate’ aim and (3) be necessary in a democratic society. The criteria embody the need for restrictions to be prescribed by legislative provisions worded with sufficient precision to enable interested parties to regulate their conduct, taking, if need be, appropriate advice.[253] Restrictions must further be necessary, which require a “pressing social need”,[254] and although ‘[t]he contracting States have a certain margin of appreciation in assessing whether such a need exists’, restrictions must always be proportionate to the legitimate aim pursued and the reasons adduced by the national authorities to justify it must be relevant and sufficient.[255]

3.8 Conclusion

This Chapter aimed to answer the second sub-question of this thesis; what the right to be forgotten is, and which rights, freedom, and interests it specifically triggers. In this chapter, we used the knowledge of the constitutional ‘framework’ that guides the EU when adopting measures, including those of secondary legislation such as the Data Directive and its successor the GDPR, and explained how the right to be forgotten fit into that context. The chapter explained how the EU and the CJEU have interpreted the right to be forgotten, and how it has developed from *Google Spain* to the provisions in the GDPR. What was shown was that the EU takes privacy and data protection seriously, and has ruled that those rights override, as a general rule, the rights of internet users to access information save in specific cases. This inherent hierarchy of rights, established in Google Spain, was criticised by freedom of expression advocates, but also by scholars such as Steve Peers and Eleni Frantziou.[256] I argued, in line with the Peers and Frantziou, that there was a lack of balancing of the two rights and a lack of reference to Article 11 of the Charter. This was disappointing, as search engines are one of the most important and easiest ways an individual may use his or her right to access information, as shown in section 3.7.2. Moreover, I highlighted the fact that states have an obligation to create a favourable environment for freedom of expression and information

[252] *Axel Springer AG v. Germany*, para. 78 and case law cited therein.
[253] *Sunday Times v. United Kingdom* judgment of 26 April 1979, no. 6538/74, CE:ECHR:1979:0426JUD000653874, para. 49.
[254] Ibid, para. 59.
[255] *Axel Springer AG v. Germany,* para. 85 and forward.
[256] See section 3.3.3.

to allow individuals to freely participate in democratic discourse, one of the founding principles of the EU. With that said, the EU legislature did take this into account when adopting the GDPR, replacing the Data Directive, in particular in Article 17(3)(a), which expressly allows SEOs to reject a request to be forgotten by a data subject, if necessary for freedom of expression and information.

The answer to the sub-question is thus the following. The right to be forgotten, as I described in section 3.4 is in fact two different 'rights' in the GDPR; the right to the erasure of data, and the right to object to data being processed. The right(s) are now codified in Article 17 and 21 of the GDPR. Together, they provide a legal basis for an individual to obtain control over one's data that is being processed and be able to request a SEO to stop processing it and remove the links from the results of a search on the basis of the data subjects name. Moreover, as described by Steeve Peers, Eleni Frantiziou and AG Jääskinen above, the interests and rights *particularly* triggered are the rights of privacy and data protection; enshrined in Article 7 and 8 of the Charter and Article 8 of the ECHR and the internet user's right to access information, as protected by freedom of expression and information; enshrined in Article 11 of the Charter and Article 10 of the ECHR.

4 C-507/17 *Google CNIL* and C-136/17 *GC and Others*

4.1 Introduction

In the first chapter, we explored the 'grand structural scheme' of the EU; the founding principles of democracy, rule of law and fundamental rights, and how they affected all measures taken by the EU. This was followed by a chapter which set the scene of the right to be forgotten, how the right developed from first being acknowledged by the CJEU in Google Spain and what fundamental rights and freedoms that are especially triggered by such a request. In this chapter, we will explore the recent developments of the right to be forgotten in the two cases *Google CNIL* and *GC and others,* from the point of view of the founding principles of EU law and the rights and freedoms triggered by a request to be forgotten. This chapter aims to answer the question of how the Court resonates in *Google CNIL* and *GC and others*, and what arguments paved the way to the outcomes of the judgments. To answer this question, the two cases will first be explored separately along with the Opinions of AG Szpunar and a few additional commentaries, and then together, as the cases must be read in conjunction to give a proper understanding of the developments on the right to be forgotten.

Both *Google CNIL* and *GC and others* were published on 24 September 2019 and complements *Google Spain* in two different aspects; *Google CNIL* on the territorial scope of the right to be forgotten, and *GC and others* on the processing of sensitive data, and its relationship with the right to be forgotten.[257] Together, they further depict the scope of the right to be forgotten for SEOs. As the previous chapter explained, the Data Directive was replaced by the GDPR in 2016. Hence, by the time *Google CNIL and GC and others* were up for consideration by the CJEU, the Data Directive had been repealed by the GDPR. Both judgments were therefore based on both frameworks, but, as they delivered equal conclusions irrespectively of which framework was used, only the legal assessment based on the GDPR will be presented.

[257] Globocnik, J. (2020) *'The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17),'* GRUR International, 0(0), 2020, 1–9, p. 1.

4.2 C-507/17 *Google v. CNIL*: the territorial scope of the right to be forgotten

In May 2015, the French DPA (CNIL) sent a notification to Google informing the SEO that when it granted the erasure of links to web pages containing personal data following a search on a data subject's name, it must remove those data from all versions of its SEO, worldwide. For context, Google is broken down into different domain names, or 'versions', by geographical extension. Google's layout for the national versions of its search engines automatically redirects internet users to their national version based on a geo-location process, irrespectively of which domain he or she enters into the search bar, e.g. if an individual enters 'google.fr' but is located in Sweden, he or she will be redirected to 'google.se'.[258]

Google refused to comply with the notice, confining itself to only perform such removal of links on the domains that corresponded to the EU member states. As a result, CNIL imposed a EUR 100 000 fine on Google, a fine Google refused to pay, and instead applied to the Council of State in France to annul the adjudication. The French Court noted that the argument raised "serious difficulties" regarding the interpretation of the Data Directive and decided to stay the proceedings and referred to the CJEU for a preliminary ruling.[259] In essence, CJEU was asked to clarify if SEOs were required to delete links on either: all versions of its search engine; the versions corresponding to all EU Member States; or only on the version corresponding to the Member State in which the request was made.[260]

4.2.1 The opinion of AG Szpunar

Both the AG Szpunar and the Court concluded that SEOs should not be required to carry out de-referencing on all domains, but only those inside the EU.[261] AG Szpunar's key argument against forcing Google to remove links from all versions of its search engine was not that EU law could not *per se* create rights and obligations outside its territory, but that "EU authorities would not be in a position to define and determine a right to receive information, still less to strike a balance between that right and the other

[258] *Google CNIL*, para 42. When the Council of State referred the case to the CJEU, Google's had a different layout system that did not automatically redirect the internet user to his or her national domain that corresponded to the place where the search was conducted, making it possible to enter any Google domain from any EU member state.
[259] *Google CNIL*, para. 39.
[260] Ibid, para. 43.
[261] Opinion of Advocate General Szpunar delivered on 10 January 2019, C-507/17 *Google CNIL*, EU:C:2019:15 *(Opinion AG Szpunar, Google CNIL).*

fundamental rights to data protection and to private life" of a world-wide public.[262]

Additionally, AG Szpunar expressed concerns over possible consequences on freedom of expression and information if the Union were to 'open the door' to remove links from all versions of its search engine, as this could influence non-EU States to the same, creating a "genuine risk of a race to the bottom, to the detriment of freedom of expression, on a European and world-wide scale."[263] While the Advocate General did not think that the EU authorities could strike a balance between rights and freedoms affected by a request for erasure on a world-wide scale, he argued that such an assessment could be carried out inside the EU. He connected the right to be forgotten, stemming from Article 7 and 8 of the Charter, and the right to access that information for EU citizens using search engines as a part of the right to freedom of expression and information in Article 11 of the Charter (the latter being absent in the Court's judgment),[264] and concluded that as the GDPR is by its nature of being a regulation directly applicable in all member states, search engines must delete links from all EU versions, not only in the single member state the request originates from.[265]

4.2.2 The CJEU's legal assessment

The Court started by recognising "that the objective of […] [the GDPR] is to guarantee a high level of protection of personal data throughout the European Union",[266] an objective that would be fully met if search engines removed links from all versions of its search engines as, from the perspective of the data subject, it does not matter whether an internet user is located inside or outside the EU.[267] There are thus, according to the CJEU, strong reasons to justify search engines to remove links from all versions of its search engine to protect data subject's right to protection of personal data inside the EU;[268] as internet's global dimension provides a unique platform, where "information and links contained in a list of results displayed following a search conducted on the basis of an individual's name ubiquitous".[269]

However, the Court recognises two main problems with this approach. First, that numerous third states do not recognize the right to de-referencing or

[262] Ibid, para. 60.
[263] Ibid, para. 61.
[264] Ibid, para. 44.
[265] Ibid, paras. 75 – 76.
[266] *Google CNIL*, para. 54 – 55.
[267] Ibid, para. 56.
[268] Ibid, paras. 57 – 58.
[269] Ibid, paras. 54 – 56.

interprets it differently, meaning that it would be impossible to reconcile the two on a world-wide basis, and second, that the right to data protection is not absolute but must be “considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality”.[270]

The CJEU declared that “[w]hile the EU legislature has, in Article 17(3)(a) of Regulation 2016/679, struck a balance between that right and that freedom so far as the Union is concerned [as interpreted by *GC and others*] […] it has not, to date, struck such a balance as regards the scope of a de-referencing outside the Union.”[271] Rejecting the obligation for SEOs to remove links from all versions of its search engine on a world-wide basis, the Court ruled that:

> “[I]t follows from, inter alia, the fact that the EU legislature has now chosen to lay down the rules concerning data protection by way of a regulation, which is directly applicable in all the Member States […] that the de-referencing in question is, in principle, supposed to be carried out in respect of all the Member States.”[272]

That being said, the Court recognised that “the interest of the public in accessing information may, even within the Union, vary from one Member State to another, meaning that the result of weighing up that interest, on the one hand, and a data subject’s rights to privacy and the protection of personal data, on the other, is not necessarily the same for all the Member States”.[273] However, those differences would in particular concern Article 85 of the GDPR, i.e. processing undertaken solely for journalistic purposes or the purpose of academic artistic or literary expression, such variation should be solved by the cooperation of the national DPAs according to the procedure laid down in the GDPR.[274] Such variations should be solved by the DPAs, which “must cooperate […] in order to reach a consensus and a single decision which is binding on all those authorities and with which the controller must ensure compliance as regards processing activities in the context of all its establishments in the Union.”[275] The final responsibility “to take, if necessary, sufficiently effective measures to ensure the effective protection of the data subject’s fundamental rights” is, however, still on the SEOs, who must adopt measures that “have the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from

[270] Ibid, para. 60 and case-law cited therein.
[271] Ibid, para. 61 and case-law cited therein.
[272] Ibid, para. 66.
[273] Ibid, para. 67.
[274] Ibid, para. 67 - 68.
[275] Ibid, para. 68.

gaining access to the links in question using a search conducted on the basis of that data subject's name".[276]

As a final remark, the CJEU held that "it should be emphasized that" while there are currently no obligations for Google to remove links from all versions of a search engine, EU law does not prohibit such a practice. The Court thus ascertains that the DPA or judicial authority of a Member State is competent to balance, in the light of national standards of protection of fundamental rights, referring to *Åkerberg Fransson* and *Melloni*,[277] a data subject's right to privacy and protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and when necessary, order a SEO to remove links on all versions of that search engine.[278]

4.2.3 Comments to the case

Google CNIL was described as a 'win' for Google,[279] as the Court did not oblige Google to remove links from all versions of its search engine, but only those inside the EU. As this thesis focus on the right to be forgotten from an internal EU perspective, the global consequences of the judgment will not be discussed in extent. However, it must be said that, as Mary Samonte recognised in her blog post, the Court's assessment shows a much more nuanced approach to the territorial scope than what seems to be portrayed in media. Even though the Court declared that the 'standard' scope of the right to be forgotten was inside all EU member states, EU law does not prohibit a national DPA or judicial authority from obliging Google to remove links globally. By acknowledging this possibility, the Court, in the words of Samonte, "leaves the door wide open for the possibility of global de-referencing as determined by a national DPA or a national court in the EU", thereby neutralizing Google's claim of victory in the case.[280]

Leaving the global effects of the judgments aside, the case has implications inside the EU as well, since the Court declared that Google should, in principle, remove links from all versions of its search engine inside the EU. Oscar J. Gstrein criticises the CJEU in his blogpost '*The Judgment That Will*

[276] Ibid, para. 70.
[277] Described in section 2.5.5.
[278] *Google CNIL*, para. 72.
[279] See e.g. Kelion, L '*Google wins landmark right to be forgotten case*', published 24 September 2019, on https://www.bbc.com/news/technology-49808208
[280] Samonte, M. *'Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law,'* published 29 October 2019, on: https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law/

Be Forgotten',[281] for being too vague and not providing enough leadership in the decision, as it does not offer much guidance to *how* the DPAs should determine if a SEO should remove links from the whole Union, in a single member state, or world-wide. This is left in the hands of the DPAs, which should cooperate and reach consensus, while the EU at the same time recognises that there are differences between the public's right to access information, and the data subject's rights of privacy and data protection even amongst the member states of the EU.[282]

Moreover, as Mary Samonte points out, the Court's reasoning in the ruling supports the conclusion that the GDPR "is setting data protection standards as a floor, not a ceiling", as it is drawing parallels to *Melloni* and *Åkerberg Fransson*, which the Court refers to in paragraph 72 of its judgment. Thus, national standards of protection of the fundamental rights triggered by a request for erasure may be protected, provided that the level of protection provided for by the Charter, as interpreted by the Court, and the primacy, unity, and effectiveness of EU law are not compromised.[283] How member states are meant to apply their higher level of protection for fundamental rights, while at the same time, the standard option for Google is to remove all links from all versions inside the EU is not clear, as the CJEU in *Google CNIL* asserts that, in principle, the balancing in one member state based on their subjective preferences of rights of privacy and data protection compared to the freedom of expression and information for internet users will be binding for all member states.

4.3 C-136/17 *GC and Others:* the processing of sensitive personal data

In *GC and others*, the individuals GC, AF, BH, and ED, independently requested Google to remove links from the result that followed after a search on their name, which led to different web pages containing personal information concerning them: *GC* wanted to remove a link to a website leading to a satirical photomontage with her and a municipal mayor placed on YouTube in 2011; *AF* requested the removal of links leading to an article published in a newspaper 2008, mentioning that he had been a public relations officer of the Church of Scientology, a position he no longer held; *BH* requested the removal of links leading to articles, mainly in the press,

[281] Gstrein, Oskar J. *'The Judgment That Will Be Forgotten: How the ECJ Missed an Opportunity in Google vs CNIL (C-507/17), VerfBlog,* 2019/9/25', accessed 2020-03-07 from: https://verfassungsblog.de/the-judgment-that-will-be-forgotten/
[282] *Google CNIL*, para. 68.
[283] *Taricco II*, paras. 42 - 47.

concerning judicial investigation from 1995, which had been closed by discharge in 2010, something that most of the links did not mention the outcome of the case; and *ED* requested de-referencing of links leading to two articles published in two newspapers reporting that he had been sentenced to 7 years' imprisonments, conjoint with 10 years' social and judicial supervision, for sexual assaults on children under the age of 15. Google rejected all four requests. The applicant then brought complaints before CNIL, which also rejected the application and closed the procedures of their complaints. Following the refusal of CNIL to order Google carry out the erasure of the links, *GC and others* applied to the Council of State in France. Finding that the applications raised "several serious difficulties of interpretation", the Court stayed proceedings, joined the cases and asked the CJEU for a preliminary ruling.[284] The legal issue the French Court sought clarification on was, in essence, if the general prohibition of processing sensitive data, found in Article 9 of the GDPR also applied to SEOs, and if the answer was affirmative, when such a request should be approved and when it should be rejected.

For context, processing of sensitive personal data is generally prohibited following Article 9(1) of the GDPR, as such data "merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms".[285] It is only lawful if one of the exceptions in Article 9(2) of the GDPR is applicable, providing a less extensive scope of situations compared to the grounds in Article 6 of the GDPR, regulating lawful processing of 'non-sensitive' personal data. Furthermore, the processing of personal data relating to criminal convictions and offences is also generally prohibited, regulated in Article 10 of the GDPR, and can only be carried out "under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects." Article 10 of the GDPR applies irrespectively if the person was found guilty or not.[286]

4.3.1 The opinion of AG Szpunar

AG Szpunar, who also issued the opinion in *Google CNIL,* argued in favour of SEOs having a responsibility to systematically grant requests by data subjects to erase sensitive personal data from its search results, since by virtue of Article 9 of the GDPR, "the legislature considers that the processing of certain data is unlawful."[287] However, with that said, he recognised that if

[284] *GC and others*, paras. 24 – 31.
[285] GDPR, Article 9 and Recital 51.
[286] *GC and others*, para 72.
[287] *Opinion AG Szpunar, GC and others,* para. 72.

SEOs must oblige the general prohibition of processing sensitive data, they must, equally as other controllers, have the ability to invoke exceptions and derogations from it for processing carried out for journalistic, artistic, or literary expressions, on the basis of Article 85 of the GDPR.[288] This would, in the Advocate General's opinion, be necessary in order to ensure freedom of expression and information of internet users.[289] To support his conclusion, he refers to *Times Newspapers Ltd v. the United Kingdom,* where the ECtHR held that "in the light of its accessibility and its capacity to store and communicate vast amounts of information, the internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general",[290] and the fact that the fundamental right does not only guarantee *the content of information* but also to the *means of transmission or reception*.[291] Furthermore, the AG refers to CJEU's *Scarlet Extended*,[292] and the AG Jääskinen's opinion to *Google Spain,*[293] both of which emphasized that Article 11 of the Charter protects not only the right of the public to receive and impart information made available on the internet by a publisher but also made available by internet search engines.[294] Hence, he argued that as SEOs must comply with the provisions of the GDPR concerning processing of sensitive data, they must also have the possibility to rely on the exceptions provided in Article 85 of the GDPR for processing for journalistic, artistic or literary purposes, as a publisher in the same situation could.[295]

4.3.2 The CJEU's legal assessment

First of all, the CJEU dismissed Google's argument that SEO's should be exempted *a priori* and generally from compliance from Article 9(1) and 10 of the GDPR, as such conclusion would "run counter to the purpose of those provisions, namely to ensure enhanced protection as regards such processing, which, because of the particular sensitivity of the data, is liable to constitute [...] a particularly serious interference with the fundamental rights to privacy and the protection of personal data, guaranteed by Articles 7 and 8 of the Charter."[296] However, due to the specific features of the processing of a SEO, the Court recognises that extent of its responsibilities and obligations under

[288] Ibid, paras. 80 – 83.
[289] Ibid, para. 89.
[290] Ibid, para. 84; referring to *Times Newspaper Limited v. United Kingdom*, 13 November 2018, No. 64367/14, CE:ECHR:2018:1113DEC006436714, para. 27.
[291] *Opinion AG Szpunar, GC and others,* para. 84; referring to *Neij and Sunde v. Sweden*, Application No 40397/12, para. 10.
[292] *Scarlet Extended*, para. 48.
[293] See *Opinion AG Jääskinen, Google Spain,* para. 121.
[294] *Opinion AG Szpunar, GC and others,* para. 85.
[295] Ibid, para. 86.
[296] *GC and others*, para. 44.

Article 9(1) and 10 of the GDPR is different from other controllers, and therefore, the general prohibition of processing sensitive personal data in the GDPR can only apply to SEOs "via a verification, under the supervision of the competent national authorities, on the basis of a request by the data subject."[297]

Next, the Court moved on to assess when an SEO must grant requests from data subjects to erase links leading to such data, and when it can invoke the exceptions provided in Article 9(2) that allows them to reject such request. The legal provisions regulating the removal of data from the internet is Article 17 and 21 of the GDPR, which enshrine the right to the erasure of personal data being processed, and the right to object to such processing. In accordance with Article 17(1) of the GDPR, one of the grounds for erasure is if the data subject objects to the processing pursuant to Article 21(1) and (2). Those provisions must be read in conjunction with Article 17(3) of the regulation, which provides for exceptions to the data subject's right to erasure, *inter alia*, for the exercise of the right of information, guaranteed by Article 11 of the Charter;[298] "an expression of the fact that the right to protection of personal data is not absolute […] but must be considered in relation to its function in society and be balanced against other fundamental rights in accordance with the principle of proportionality".[299] Article 17(3)(a) of the GDPR "thus expressly lays down the requirement to strike a balance between the fundamental rights to privacy and protection of personal data guaranteed by Articles 7 and 8 of the Charter, on the one hand, and the fundamental right of freedom of information guaranteed by Article 11 of the Charter, on the other", and it is in the light of those considerations that a SEO must grant or refuse a request of de-listing.[300]

The exceptions that allow processing of sensitive data following Article 9(2)(a)-(j) of the GDPR,[301] states that the general prohibition of processing sensitive data *should not apply when*: (a) the data subject consents to the processing; (e) the data has been manifestly made public by the data subject; or (g) where it is necessary for reasons of substantial public interest, on the basis of European Union or Member State law which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Since ground 9(2)(a) is based on consent, it can be more or less excluded by the mere fact that a person makes a request

[297] Ibid, paras. 45 and 47.
[298] Ibid, paras. 55 - 56.
[299] Ibid, para. 57.
[300] Ibid, paras. 59 - 60.
[301] The exceptions mentioned are the ones relevant for SEOs.

for delisting,[302] in practice, SEOs are left with only two situations where processing may be lawful according to the GDPR: (e) if the data subject has 'manifestly' made the data public themselves, or (g) for reasons of 'substantial public interest'.[303]

The focus of the Court in the case was on situations where the SEO supports its processing of sensitive data for reasons of 'substantial public interest', Article 9(2)(g). On the assessment of what constitutes a substantial public interest, the Court ruled the following:

> "In any event, when the operator of a search engine receives a request for de-referencing, he must ascertain, having regard to the reasons of substantial public interest referred to in […] [Article 9(2)(g) of the GDPR] and in compliance with the conditions laid down in those provisions, whether the inclusion of the link to the web page in question in the list displayed following a search on the basis of the data subject's name is necessary for exercising the right of freedom of information of internet users potentially interested in accessing that web page by means of such a search, a right protected by Article 11 of the Charter. While the data subject's rights protected by Articles 7 and 8 of the Charter override, as a general rule, the freedom of information of internet users, that balance may, however, depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life."[304]

SEOs thus have an obligation to assess requests to remove data in the light of public interest, and may only reject those if "the inclusion of that link in the list of results displayed following a search on the basis of the data subject's name is strictly necessary for protecting the freedom of information of internet users potentially interested in accessing that web page by means of such a search, protected by Article 11 of the Charter".[305]

That being said, the Court moved on to the assessment of personal data falling inside the scope of Article 10 of the GDPR, i.e. information relating to criminal convictions and offences.[306] Processing of such information may be lawful, but must be justified by a substantial public interest, equal to other types of sensitive data.[307] The CJEU referred to *M.L. and W.W. v. Germany,* where the ECtHR ruled that in order to strike a fair balance concerning a data subject's right to erasure, and public's freedom of information, account must be taken of the "essential role played by the press in a democratic society,

[302] *GC and others*, para. 62.
[303] Ibid, para. 61.
[304] Ibid, para. 66.
[305] Ibid, para. 68.
[306] Ibid, para. 72.
[307] Ibid, para. 75.

which includes reporting and commenting on legal proceedings. Moreover, to the media's function of communicating such information and ideas, there must be added the public's right to receive them. The […] [ECtHR] acknowledged in this context that the public had an interest not only in being informed about a topical event, but also in being able to conduct research into past events, with the public's interest as regards criminal proceedings varying in degree, however, and possibly evolving over time according in particular to the circumstances of the case."[308]

The SEO must assess whether a request for erasure concerning criminal proceedings and legal proceedings should be granted or not, in the light of all circumstances of the case, bearing in mind that, even "initially lawful processing of accurate data may over time become incompatible with the directive or the regulation where those data are no longer necessary in the light of the purposes for which they were collected or processed".[309] The Court concluded its ruling on the processing of data referring to criminal convictions and offences by stating that:

> "It is thus for the operator of a search engine to assess, in the context of a request for de-referencing relating to links to web pages on which information is published relating to criminal proceedings brought against the data subject, concerning an earlier stage of the proceedings and no longer corresponding to the current situation, whether, in the light of all the circumstances of the case, such as, in particular, the nature and seriousness of the offence in question, the progress and the outcome of the proceedings, the time elapsed, the part played by the data subject in public life and his past conduct, the public's interest at the time of the request, the content and form of the publication and the consequences of publication for the data subject, he or she has a right to the information in question no longer, in the present state of things, being linked with his or her name by a list of results displayed following a search carried out on the basis of that name."[310]

Nevertheless, even if the result of such investigation is that the request must be rejected as it is overridden by a substantial public interest, the SEO is required to place the link containing information that reflects the current legal situation in first place on the list.[311]

---

[308] *M.L. and W.W. v. Germany,* paras. 89 and 100 – 102.
[309] *GC and others,* para 74; GDPR, Article 5(1)(c) - (e).
[310] *GC and others,* para. 77.
[311] *GC and others*, para. 78.

4.4 Analysis of the cases

4.4.1 The EDPB issued Guidelines

After *Google CNIL* and *GC and others* were published, the European Data Protection Board (EDPB) adopted *Guidelines on the criteria of the Right to be Forgotten in the search engine cases under the GDPR* on 2 December 2019,[312] similarly as after *Google Spain*. The *Guidelines* pointed out the fact that Article 17(1)(c) of the GDPR, that is, where a SEO must erase personal data from its search result if he or she objects to the processing according to Article 21(1) of the GDPR is more stringent than its predecessor Article 14 of the Data Directive, since he or she no longer has to demonstrate "compelling legitimate grounds" relating to his or her particular situation to have a right to object. The provisions in the GDPR thus provides a presumption in favour of the data subject in order to refuse such a request for removal of links, unless the SEO can demonstrate "overriding legitimate grounds" that would overturn the presumption.[313] Moreover, on the exception provided for on the basis freedom of expression and information, following Article 17(3)(a) of the GDPR; which the Court used in *GC and others*, the EDPB declared that the provision does "not appear suitable in case of a delisting request", and that "such inadequacy pleads in favour of the application of Article 21 [of the] GDPR for delisting requests".[314] However, with that said, the EDPB confirms the reasoning of the Court in GC and others, and concludes that "depending on the circumstances of the case, search engine providers may refuse to delist a content in the event where they can demonstrate that its inclusion in the list of results is strictly necessary for protecting the freedom of information of internet users."[315]

4.4.2 Comments to the Case

As argued by Eliska Prikova and Estelle Massé in their article written for *Access Now,* it is problematic that the CJEU puts Google responsible for properly balancing the data subjects right to be forgotten with the public's right to have access to the information, a balance that is often "context-

[312] EDPB, *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)*, adopted on 2 December 2019, *(Guidelines(2019)* accessed 2019-12-28 on: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublicconsultation.pdf
[313] Ibid, p. 8.
[314] Ibid, p. 11.
[315] Ibid, p. 13.

dependent and highly nuanced and therefore challenging even for experienced national and international judges".[316] According to Prikova and Massé, one of the most concerning elements in *GC and others,* and one of the more concerning aspect of how the right has developed in case-law, is that the Court holds Google, a private company, responsible for deciding what information should be removed from their result list and what should remain. The two authors argue that "[p]rivate actors should not be put in a situation where they have a *de facto* judicial role over content and are required to weigh data protection against freedom of information", when they neither have a democratic mandate to do so nor makes transparent decisions which comply with the rule of law. Therefore, they stress that it is of utter importance that "the courts and independent public regulators" interpret and evaluate Google's assessment.[317]

In the light of those arguments, it is fitting to highlight, and stress the differences between *GC and others* and *M.L. and W.W. v Germany*; which both the CJEU refers to in *GC and others*, and the EDPB in the *Guidelines*. In *M.L and W.W v. Germany*, the ECtHR offers a *wide discretion for the member states* of the ECHR to strike a fair balance between the right to be forgotten and freedom of expression and information. Compared to *GC and others*, the CJEU holds that "it is thus for the *SEO* to assess […] he or she has a right to the information in question no longer., in the present state of things, being linked with his or her name by a list of results displayed following a search carried out on the basis of that name" (my emphasis).[318] There is an important difference between letting *states* and *SEOs* do this assessment. As pointed out by Rikke Frank Jørgensen, in *New Technologies for Human Rights Law and Practice;*[319] "[i]nternet platforms are rarely subject to regulation concerning the negative impact they have on freedom of expression".[320] Whereas, as explained in section 3.7, states are responsible for the measures they take, and the measures that private actors take in their territory if it has a negative impact on freedom of expression and information. This was has also been recognised by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, which specifically pointed out that states have a responsibility to ensure that "the private sector is able to carry out its functions independently in a manner

---

[316] Massé, E. & Pirkova, E. *'EU Court decides on two major "right to be forgotten" cases: there are no winners here',* published 23 October 2019, accessed 2020-02-21 from https://www.accessnow.org/eu-court-decides-on-two-major-right-to-be-forgotten-cases-there-are-no-winners-here/
[317] Ibid.
[318] *GC and others,* para. 77.
[319] Jørgensen, R. (2018) *'Human Rights and Private Actors in the Online Domain.'* In Land, M., & Aronson, J. (Eds.). (2018) *'New Technologies for Human Rights Law and Practice.'* Cambridge: Cambridge University Press.
[320] Ibid, p. 259.

that promotes individuals' human right." States have thus a responsibility not only to refrain from violating fundamental rights, but also to ensure that the private actors operating in their territory refrain from violating them, and hold them accountable if they do.[321] When private companies decide what content should stay and what should be removed, they are directly acting as judiciaries for rights of privacy and data protection for the data subject and freedom of expression and information for internet users. Jørgensen uses *Twitter* as an example, and states the following:

> "When content is filtered, blocked, or taken down by Twitter […] the company is acting in a judicial capacity […] but without the human rights requirements that would apply if Twitter were a state body rather than a private company. […] In contrast, if a state-owned Twitter were to remove content from the public domain, this practice would have to follow the three-part test governing limits on freedom of expression".[322]

Furthermore, the case was discussed by Mark Leiser and Bart Schermer in their blogpost *"GC & others vs CNIL and Google: This is a Special case"*.[323] They argue that while the case sheds light on the question *when* the exceptions that allow for processing of sensitive personal data, the question of whether Google may *rely* on either of them remains unanswered. While the CJEU recognises that Google can invoke to legitimise processing of such data is Article 9(2)(g), which states that it must be necessary for reasons of substantial public interest, the Court does not elaborate on what a substantial public interest is, and when the threshold for invoking such is met. In this context, it is important to have in mind what Emily Laidlaw argues in her book, "*Regulating Speech in Cyberspace";* as SEO are not, contrary to publishers, directly involved in publishing information, "certainly not all – in fact very little – of what is brought up on search results is in the public interest". On the light of those grounds, Google may have a hard time invoking the exception in Article 9(2)(g), as sensitive personal data merits particularly high protection.[324] But this does not mean that SEOs are not important for democracy and freedom of expression and information.[325] Laidlaw argues the following:

> "Even if most searches are for inane matter, this simply reflects the general public's democratic participation in the real world. […] This illustrates what is so unique about what search engines do. Visitors input search terms and search

[321] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, para. 77.
[322] Jørgensen, R. (2018), p. 259.
[323] Leiser, M & Schermer, B. *"GC & others vs CNIL and Google: This is a Special case"*, published 20 November 2019, accessed 2020-03-01 from: https://europeanlawblog.eu/2019/11/20/gc-others-vs-cnil-and-google-this-is-a-special-case/
[324] GDPR, Recital 51.
[325] E. Laidlaw (2015), p. 202.

> providers offer results. This immediately sets up a discourse between the visitor and the provider. The product of this discourse is a list of search results, ranked in order of purported relevance, which guides the user's attention. Thus, it is not that a specific article is of public interest, but that simply search engines are of public interest because they now play an essential role in democratic society in structuring how we understand the informational world. This role is intimately tied with the roots of the protection of freedom of expression and the importance attached to the role of media in democratic society".[326]

As argued, it will be hard for Google to demonstrate a substantial public interest on a case by case basis. The last stop before Google must grant a request is the possibility to invoke the more general exception of the freedom of expression and information, in Article 85 of the GDPR, which allows member states to adopt national legislation for processing for journalistic, academic, artistic, and literary purposes from *inter alia* the rights of the data subject to have data removed or object to it being processed. *How, when,* and most importantly *if* SEOs can invoke Article 85 of the GDPR may, therefore, play a vital role in the freedom of expression and information of internet users.

4.4.3 Article 85 of the GDPR and SEOs

As already mentioned,[327] the GDPR contains several 'opening clauses' that allow for national differences and variations. Amongst the opening clauses "with the highest practical relevance" are those relating to the data subject rights, the processing of special categories of personal data and the specific requirements for the lawfulness of processing based on a legal obligation of the controller or processing carried out in the public interest. These will above all be challenging for actors carrying out processing in several different EU member states or processing data which has a transborder effect in the EU.[328] They were implemented to ease the tension between the rights of privacy and data protection and freedom of expression and information to allow member states more leeway to reconcile the rules in situations highly connected with freedom of expression and information.[329] Member states are both empowered and responsible for reconciling the protection of personal data with freedom of expression and information.[330]

One of those provisions is Article 85 of the GDPR, formerly Article 9 of the Data Directive. Article 85(2) of the GDPR states the following:

[326] Ibid.
[327] See section 3.4.
[328] Bussche, A. von dem., & Voigt, P. (2017) p. 223.
[329] GDPR, Article 85 and Recital 153.
[330] Leczykiewicz, D. (2020) p. 70 - 71.

> "For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations […] if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information."

Article 85 provides exceptions and derogations from all provision in Chapter III of the GDPR, including Article 9, sensitive personal data; Article 10, data concerning criminal convictions and offences; Article 17 'the right to erasure'; and Article 21, 'the right to object', and is, therefore, relevant for all types of personal data that has been discussed in this thesis. The provision is mentioned in the recitals, which states that "[i]n order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly."[331] Moreover, in *Satamedia*, the CJEU clarified that an activity may be classified as 'journalistic', "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."[332]

Article 85 GDPR is *similar but not identical* to its predecessor, Article 9 of the Data Directive, which stated that such exceptions should be provided for the processing of personal data carried out *solely* for journalistic purposes, *only* if they are necessary to reconcile the right to privacy with the rules governing freedom of expression. While both publishers of information and SEOs processing the link to that information may be classified as 'controllers' of personal data, case law has developed a distinction between the two, as the publisher conducts an activity which "is at the heart of what freedom of expression aims to protect", and thus merits higher protection than the activity of a SEO.[333] This distinction was recognised from the origin of the right to be forgotten when the CJEU in *Google Spain* ruled that while a publisher of information may carry out an activity *solely* for journalistic purposes and thus benefit from derogations provided by Article 9 of the Data Directive it "does not appear to be so" for a SEO.[334] This was subsequently affirmed in the *Guidelines* from Article 29 Working Party, which held that:

> "[D]epending on the context, it may be relevant to consider whether the information was published for a journalistic purpose. The fact that information is published by a journalist whose job is to inform the public is a factor to weigh in the balance. However, this criterion alone does not provide a sufficient basis for refusing a request, since the ruling clearly distinguishes

[331] GDPR, Recital 153.
[332] *Satamedia*, para. 61.
[333] *W.W. and M.L. vs. Germany,* para. 97.
[334] *Google Spain,* para. 85.

> between the legal basis for publication by the media, and the legal basis for search engines to organise search results based on a person's name."[335]

The same distinction was also more recently confirmed by the ECtHR in *M.L. and W.W. v. Germany*, where the Court referred to the CJEU's assessment in *Google Spain*, and held that:

> "Consequently, the balancing of the interests at stake may result in different outcomes depending on whether a request for deletion concerns the original publisher of the information, whose activity is generally at the heart of what freedom of expression is intended to protect, or a search engine whose main interest is not in publishing the initial information about the person concerned, but in particular in facilitating identification of any available information on that person and establishing a profile of him or her"[336]

In *GC and others*, The CJEU, in turn, referred to *M.L. and W.W. v. Germany,* that on the balancing between the two rights, account must be taken of the "essential role played by the press in a democratic society, which includes reporting and commenting on legal proceedings."[337] In assessing that balance, the media's function of communicating such information and ideas must be added to the public's right to receive them.[338] Moreover, the CJEU acknowledged that the ECtHR stressed that "the public had an interest not only in being informed about a topical event, but also in being able to conduct research into past events, with the public's interest as regards criminal proceedings varying in degree, however, and possibly evolving over time according in particular to the circumstances of the case".[339] From the foregoing statements, it is clear that both the ECtHR and the CJEU agrees that publishers of information have a stronger legitimate interest in disseminating information compared to that of a SEO.

That being said, in *GC and others*, the CJEU appointed Google the obligation to balance the fundamental rights of privacy and data protection against freedom of expression and information as one part of the assessment of a request to remove links from its search result, by ruling that:

> "In any event, when the operator of a search engine receives a request for de-referencing, he must ascertain, having regard to the reasons of substantial public interest […] whether the inclusion of the link to the web page in question in the list displayed following a search on the basis of the data subject's name is necessary for exercising the right of freedom of information of internet users

[335] Article 29 Working Party, (2014), *Guidelines* p. 19.
[336] *M.L. and W.W v. Germany*, para. 97.
[337] Ibid, para. 89.
[338] *GC and others,* para. 76.
[339] Ibid; *M.L. and W.W v. Germany*, para. 101.

> potentially interested in accessing that web page by means of such a search, a right protected by Article 11 of the Charter."[340]

Moreover, as Article 17(3)(a) "is an expression of the fact that the right to protection of personal data is not an absolute right but […] must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality",[341] the Court acknowledges the possibility for SEOs to decline a request to erase personal data in favour of protecting freedom of expression and information of internet user, when necessary. This conclusion is also supported by the EDPB's *Guidelines*, which interprets the Court analysis as implying that SEOs have an obligation to "consider what would be the impact of a delisting decision on the access to information by Internet users", and in case of a "preponderant interest of the general public in having access to the information", reject the request.[342] Article 85 of the GDPR in relation to search engines is, unfortunately, left uncommented by the CJEU and the EDPA. What is clear, is that there is a distinction between publishers of information and SEOs, where the former may undertake processing "exclusively for the purposes of journalism" and thus benefit from Article 85 of the GDPR, but nothing indicates that it should be interpreted *e contrario* and preclude SEOs from being able to invoke it.[343]

On the contrary, as pointed out by AG Szpunar in *GC and others*, the mere fact that the controller of the data is a SEO and not a publisher should not prevent it from being able to rely on the exceptions and derogations that follow from Article 85 of the GDPR, and therefore, he invites the Court to adjudicate *GC and others* in a way which ensures sufficient respect to freedom of expression, by *inter alia* allowing SEOs to rely on Article 9 of the Data Directive, now Article 85 of the GDPR.[344] While *Google Spain* provides "great temptation" to preclude SEOs from being able to invoke Article 9 of the GDPR, AG Szpunar proposes "that the Court should resist such temptation".[345] To support his argument, he referred to *Times Newspapers Ltd v. the United Kingdom,* where the ECtHR held that "in the light of its accessibility and its capacity to store and communicate vast amounts of information, the internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general",[346] and the fact that the fundamental right does not only guarantee

[340] GC and others, para 66.
[341] Ibid, para 57.
[342] *Guidelines* (2019), p. 12.
[343] *Guidelines* (2019), p. 12.
[344] *Opinion AG Szpunar, GC and others*, para. 5.
[345] Ibid. paras. 82 – 83.
[346] Ibid, para. 84; referring to *Times Newspapers Ltd v. the United Kingdom*, para. 27.

the content of information but also to the *means of transmission or reception*.[347] In addition, he referred to the CJEU's *Scarlet Extended*[348] and AG Jääskinen's Opinion to *Google Spain*[349] which both stressed that Article 11 of the Charter protects not only the right of the public to receive and impart information made available on the internet by publishers but also by SEOs. His conclusion is therefore that SEOS must be able to invoke that the personal data is being processed for journalistic, artistic or literary expression within the meaning of Article 9 of the Data Directive, now Article 85 of the GDPR, and be able to rely on those exceptions, as a publisher of information in the same situation could.[350]

As a last note, it is important to stress that even if the GDPR opens up for national legislation to be adopted in order to reconcile the fundamental right to data protection and the fundamental freedom of expression and information, this margin of manoeuvre may only be exercised inside the framework of EU law,[351] thus inside the interpretational monopoly by the CJEU. As explained in section 2.5.5 member states may apply a higher level of protection for fundamental rights if it does not undermine the primacy, unity and effectiveness of EU law.[352] For contrast, the recent case *TSN*[353] concerned the implementation of a provision of a directive imposing minimum obligations on the member states, where the CJEU ruled that when member states implement minimum obligations governed by a Directive, they were not acting inside the scope of EU law.[354] The situation in TSN differs from situations where member states implement Article 85 of the GDPR for two reasons. First, since the opening clauses only allow for *further specification* of certain provisions in the GDPR by national legislation,[355] and secondly, as member state using its discretionary power, granted by a regulation to adopt exceptions and from it, must still comply with the other provisions of the regulation, since they are, 'implementing Union law' within the meaning of Article 51(1) of the Charter.[356]

---

[347] Ibid, para. 84; referring to *Neij and Sunde v. Sweden*, para. 10.
[348] *Scarlet Extended*, para. 48.
[349] See *Opinion AG Jääskinen, Google Spain,* para. 121.
[350] *Opinion AG Szpunar, GC and others,* para 85 – 86.
[351] *Explanations to the Charter* (2007) Explanation on Article 51; *Wachauf.*
[352] See *Melloni* and *Taricco I.*
[353] Joined Cases C-609/17 and C-610/17, *TNS*, 19 November 2019, ECLI:EU:C:2019:981
[354] Ibid, para. 53.
[355] Bussche, A. von dem., & Voigt, P. (2017), p. 219.
[356] Joined cases C-411/10 and C-493/10 *N.S.* 21 December 2011, ECLI:EU:C:2011:865 Paras. 66 – 68; *Explanations to the Charter* (2007) Explanation on Article 51.

4.5 Conclusion

This Chapter presented the two most recent cases on the right to be forgotten, *Google CNIL* and *GC and others*, and aimed to answer the fourth and last sub-question of the thesis on how the Court resonate in Google CNIL and GC and others, and what arguments paved the way to the final outcomes of the judgments.

Starting with *Google CNIL* on the territorial scope of the GDPR, the CJEU ruled that when a SEO grants a request to remove personal data from its result, it should by default remove it from all EU versions of its search engines to ensure a consistent and high level of protection for personal data for the data subject. This decision was possible even though the interests of the public in accessing information may vary from one member state to another since those differences will most likely concern processing is undertaken solely for journalistic purposes or the purpose of academic artistic or literary expression and should when necessary be solved by cooperation between the affected member states' DPAs.[357] In *GC and others*, the CJEU ruled that SEOs must rely on one of the exceptions provided in Article 9(2) of the GDPR to comply lawfully process such data and that such assessment would be triggered by a request of the data subject whose data is being processed. A contrary conclusion would undermine the data subject's right to privacy and data protection, as guaranteed by Article 7 and 8 of the Charter. For SEOs, that means that they can only process sensitive personal data if Article 9(2)(g) is fulfilled; if the processing is 'necessary for reasons of substantial public interest'.

In line with *Google Spain*, the CJEU stood by its reasoning that the data subject's rights protected by Articles 7 and 8 of the Charter override, as a general rule, the freedom of information of internet users", but that SEOs have an obligation to assess "whether the inclusion of the link to the web page in question in the list displayed following a search on the basis of the data subject's name is necessary for exercising the right of freedom of information of internet users potentially interested in accessing that web page by means of such a search, a right protected by Article 11 of the Charter".[358]

As shown in section 4.4.3, whether SEOs may invoke the exception in Article 85 of the GDPR will be highly relevant for freedom of expression and information in the EU, as the provision provides exceptions and derogations from all provision in Chapter III of the GDPR, including sensitive personal

[357] See section 4.2.
[358] *GC and others*, para. 66.

data, data concerning criminal convictions and offences, and 'regular' personal data. *In the first scenario*, the one advocated by AG Szpunar, we presume that SEOs *may* invoke the exceptions and derogations that stem from Article 85 of the GDPR and, when necessary, reject requests of erasure of personal data from its search results to guarantee freedom of expression and information. As Article 85 of the GDPR is an opening clause, each member state implements national exceptions from the right to be forgotten on the basis of journalistic purposes. If, and how, such exceptions are implemented into national legislation will thus vary from one member state to another, causing hinders and irregularities to the otherwise harmonised area of data protection in the EU. In conjunction with *Google CNIL*, this becomes problematic, as the Court ruled that Google should by default remove links from all EU versions of its search engine. This leads us to yet another layer of complexity: the same situation may be regarded as falling inside one member state's national implementation of Article 85 of the GDPR and falling outside another, depending on how they have been transposed. Thus, data subjects requesting similar personal data to be removed may be granted removal in one state, and following Google CNIL, be removed from all EU versions of its search engine, whilst not being incompatible with other states national implementation of Article 85 of the GDPR. This could lead to an unjustifiable interference with an individual's right to access information in those state where the information is removed from the version of the SEO he or she uses to access information as the interference is not done on the basis of national legislation, one of the grounds that must be fulfilled to allow restrictions of Article 10 of the ECHR, and thus, in his or her member state, the information is protected by freedom of expression and information. This in turn, would not be compatible with the EU's claim to respect rule of law, democracy and fundamental rights

In the second scenario, we can presume that SEOs *are not able to* invoke the exceptions for journalistic purposes, following Article 85 of the GDPR when assessing a request of erasure of personal data. First, in situations concerning sensitive personal data, and data relating to criminal following Article 9(2)(g) and Article 10 of the GDPR, the same situation as described above, regarding Article 85, would apply as exceptions from the general prohibition to process sensitive personal data for reasons of substantial public interest must be on the basis of Union or member state law. Secondly, in situations concerning 'regular' personal data, SEOs may refuse a request on either Article 17 or 21 of the GDPR. Article 17(3)(a) lays down the possibility for SEOs to reject a request to remove personal data where the processing is necessary for exercising the right of freedom of expression and information. However, as pointed out in section 4.4.1; the *Guidelines* issued by the EDPB states that Article 17(3) is not suitable in cases of a delisting request and that Article 21

should be used instead. Whilst Article 17(3)(a) and 21(1) is similar, the difference is that the latter requires that the SEO demonstrates '*compelling legitimate grounds*' to reject a request to remove information from its search results, whereas the former only required that the processing was '*necessary'* for exercising the right of freedom of expression and information. Article 21 of the GDPR thus lays down a more stringent requirement for SEOs to be able to reject a request for erasure. As I pointed out in section 4.4.2, Laidlaw argued that "it is not that a specific article is of public interest, but that simply search engines are of public interest because they now play an essential role in a democratic society in structuring how we understand the informational world".[359] As a consequence, it will be difficult and require a strenuous effort for SEOs to demonstrate compelling legitimate grounds on a case by case basis in order to reject a request to remove information from its search engine.

[359] Laidlaw, E. (2015), p. 202

5 Conclusion

This conclusion aims to answer the main thesis question, if the right to be forgotten, in the light of the development of the recent case law, is compatible with the founding principles of the EU.

In chapter two, we learned that the founding principles of EU law are, *inter alia,* respect for democracy, rule of law and respect for human rights, and that they are of the highest hierarchical norm of EU law, that can never be violated in any way by the CJEU or by a EU legal act. I argued that the Union's claim of authority and member states compliance with the autonomy of EU law is based on the premise that these values are respected. The third chapter explained that the right to be forgotten is a right for individuals to ask SEOs to remove personal data from their search results, which especially triggers the fundamental rights of privacy, data protection and freedom of expression and information. I argued that there was a lack of balancing between the two rights, as the precedence set by *Google Spain* indicated an internal hierarchy between the triggered rights which does not exist. The fourth chapter presented the two cases *Google CNIL* and *GC and others*, in which the former the Court ruled that SEOs should as, a general rule, remove links from all EU member states' version of the search engine, and in the latter that SEOs must comply with the general prohibition of processing sensitive personal data and data revealing criminal conduct and offences. I argued that the two cases, in conjunction, may be problematic for SEOs for two reasons. Firstly, since SEOs are faced with the task of demonstrating 'compelling legitimate grounds' in order to process sensitive/criminal personal data, and secondly since Article 85 and Article 9(2)(g) are opening clauses, which allows for some leeway for member states' national peculiarities on freedom of expression and information.

Respect for the founding principles of democracy, rule of law, and human rights is not a status quo that exists without effort but must be continuously upheld through internal and external measures, such as ensuring individuals a safe environment to speak, share opinions, seek and receive information. The decision to appoint private SEOs as a 'guardians of freedom of expression and information', is problematic, as the assessment is complex and, if not done correctly, will interfere with the fundamental rights of an individual. The implications *Google CNIL* and *GC and others* can have on the founding principles of respect for fundamental rights, is a detriment of freedom of expression due to the normative hierarchy with deems freedom of

expression and information as less important than the rights of privacy and data protection. This hierarchy stems from the CJEU's ruling in *Google Spain*, and was heavily criticised at the time. E.g. As argued by Steve Peers,[360] the essential problem with *Google Spain* is that it lacks balancing and does not acknowledge the corresponding effect that a request to erase personal data have; that it interferes with the public's right to access information on a free and public domain. In *Google Spain,* the Court did not seem to acknowledge that it was balancing two normatively equal, non-absolute fundamental rights, as it referred to the right to access information as an *interest*. While the error in terminology was rightfully 'corrected' in *GC and others*, where the Court recognised that the public's right to access information is indeed guaranteed by Article 11 of the Charter, the the internal hierarchy between the two rights was still maintained and reaffirmed. The right to be forgotten thus still is lacking the sufficient balance needed to respect individual's right to access information, as protected by freedom of expression. The importance of SEOs for freedom of expression and information has been reaffirmed several times both by the CJEU and the ECtHR, and it is thus unfortunate to rule that one right by default override the other. In addition, since SEOs must comply with a request unless compelling grounds can be demonstrated, this leaves little room for balance between the two rights, and is constraining for those member states whose wants to uphold a strong national protection for their citizen's freedom of expression and information. The specific characteristics of EU law furthermore amplifies the consequences on freedom of expression and information, as the member states are bound by the CJEU's interpretation and cannot disregard the internal hierarchy between the two rights without undermining the full effectiveness of EU law. The level set by the EU thus becomes both the floor and the ceiling for fundamental rights and constitutes the framework which member states cannot deviate from

As emphasized in the Guidelines issued after *Google CNIL* and *GC and others*, SEOs may only reject a request if they can demonstrate a preponderant interest of the general public in having access to the information. By setting the threshold almost impossibly high to reject a request to be forgotten, the EU seems to be neglecting the fact that search engines are one of the most important ways an individual can utilize his or her freedom of expression and information, and thus when restricted, can seriously harm an individual's access to information. On those grounds, as I argued in section 4.4 and 4.5, the question if, when, and how search engines are able to invoke the exceptions for processing for journalistic purposes will be vital for individual's access to information. By restricting SEOs possibilities to invoke exceptions on the basis of freedom of expression and information, as a

[360] See section 3.3.3.

consequence, the CJEU is also restricting individual's ability to access information from search engines, which, in the words of AG Jääskinen, constitutes "one of the most important ways a person can exercise this fundamental right in a contemporary information society."[361]

The Union's claim to be founded on democracy has resulted in different provisions and regulations,[362] all which have the same aim – to ensure that the EU is an area where openness and transparency are respected, as they are values that matter for a society which claims to be democratic. Access to information is protected under freedom of expression and information and is one of the fundamental pillars of a democratic society.[363] Thus, when the EU claims to be founded on *democracy,* it entails a coexistence of data protection and privacy and freedom of expression and information to ensure that the EU is a sphere where citizens are free to express themselves. Democracy is closely connected to rule of law, as citizens must be ensured full exercise of their fundamental rights under the rule of law, to engage in democratic discourse. It is also therefore problematic from a rule of law point of view that SEOs are given such a prominent role in protecting individual's rights and freedoms, as their assessments are not transparent. As pointed out in section 4.4.2 by Jørgensen, and her use of *Twitter* as an example, when content is removed from the index of search engines, SEOs are acting in a judiciary capacity normally granted to authorities of the member states, not private parties, but without the framework that usually safeguards such a restriction. The lack of transparency on how SEOs balance the rights of privacy and protection of personal data against the public's right to access information adds another layer of complexity to the issue, as it is hard to for an individual to know if his or her right to access information is violated by a private party acting inside another EU member state.

Moreover, as argued by Spaventa in section 3.3.3, the lack of reference to the ECHR and case-law from the ECtHR on restrictions to freedom of expression and information is problematic, as this would provide SEOs and DPAs a better understanding on how to assess requests to be forgotten. In this context, it is important to note that while the ECtHR allows member states a "certain margin of manoeuvre" when deciding on the necessity of restricting freedom of expression and information, such restrictions must always be "proportionate to the legitimate aim pursued and the reasons adduced by the national authorities to justify it must be relevant and sufficient";[364] as the prime responsibility to ensure the protection of the rights and freedoms

[361] *Opinion AG Jääskinen, Google Spain,* paras. 130 – 131.
[362] See section 2.2.3.
[363] *Bavarian Lager*, para. 18.
[364] *Axel Springer AG v. Germany,* para. 85 and forward.

guaranteed in the ECHR is on the member states. This is different when we are dealing with the Charter, as when the Charter rights are triggered, member states are inside the scope of EU law and thus confined by the autonomy of EU law and the interpretational monopoly of the CJEU.[365]

It is important to note that even if SEOs are able to invoke a national implementation of Article 85 of the GDPR on the basis of freedom of expression, SEOs and member states are still acting inside the scope of EU law.[366] As the common EU denominator is binding for member states due to their obligation to ensure the full effectiveness of EU law,[367] as *Opinion 2/13* explained; even if that particular level of freedom of expression that is the EU level is lower than the level that stems from member states constitutions, they must lower their constitutional protection when acting inside the scope of EU law. In the example of Data protection, the very *rationale* behind taking EU measures in the area was to harmonise and create an equivalent level of protection of the fundamental rights and freedoms of natural persons throughout the EU: and with that comes the 'hermeneutic monopoly' of reconciling the competing rights and interests in the area of law.[368] Hence, as the CJEU ruled that the removal of links should be done by default on all versions inside the EU: the national peculiarities that allow for divergence due to freedom of expression and information following Article 85 cannot be applied if this would undermine the full effectiveness of EU law.

Even though the CJEU states that member states DPAs should "cooperate and reach consensus" and a final decision that is binding in all member states, the requests that are directed to a SEO is not subject to the DPAs' cooperation mechanism. However, it is the DPA's responsibility to ensure that their national implementation of Article 85 GDPR is respected by the SEOs, as member states must ensure the full effectiveness of EU law. While the EU allows member states to reconcile the protection of personal data with freedom of expression and information by, *inter alia,* Article 85 and 9(2)(g) of the GDPR, it is difficult to see how this will apply in practice, as an implication of *Google CNIL* is that those requests render the risk of being by default removed from all EU versions of the SEO. This would have a negative impact on the founding principle of pluralism of the EU legal order, rule of law, and the fundamental right to freedom of expression for those individuals in those member states where the links would have been deleted, but instead exempted from deletion based on the member states national implementation of Article 85 of the GDPR.

---

[365] See section 2.5.1 on autonomy of EU law.
[366] See section 4.4.3 on Article 85.
[367] See section 2.5.5 on *Melloni* and *Taricco.*
[368] GDPR, Recital 10.

Bibliography

Presented in an alphabetical order

Literature:

Bogdandy, A. von (2009) *'Founding principles'* Chapter 1 in Bogdandy A. von and Bast, J. (eds), '*Principles of European constitutional law'* (2nd edn) Oxford: Hart Publishing, 2009, ISBN:978-1-84113-822-0

Bussche, A. von dem., & Voigt, P. (2017). *'The EU general data protection regulation (GDPR): a practical guide',* Springer International Publishing AG, 2017. DOI 10.1007/978-3-319-57959-7

Corthaut, T. (2012) *'EU ordre public',* Kluwer Law International, 2012, ISBN: 9789041132321

Craig, P., & De Búrca, G. (2015). 'EU law: text, cases, and materials (6. Ed.) Oxford: Oxford University Press, 2015

Gill-Pedro, E. (2019) 'EU law, fundamental rights and national democracy.' New York: Routledge, Taylor & Francis Group 2019. ISBN: 978-1-351-17635-4

Hettne, J. (2011) *'EU-rättsliga tolkningsmetoder'*, in Eriksson Otken, I., Hettne, J. (eds) (2011) *'EU rättslig metod, Teori och Genomslag i Svensk Rättstillämpning,'* (2nd ed), Stockholm: Nordstedts Juridik AB, 2011

Hijmans, H. (2016). *'The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU',* Springer International Publishing Switzerland 2016, DOI 10.1007/978-3-319-34090-6

Ivanova Y. (2020) *'Can EU Data Protection Legislation Help to Counter "Fake News" and Other Threats to Democracy?'* In Katsikas S., Zorkadis V. (eds) *'E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age. e-Democracy 2019.'* Communications in Computer and Information Science, vol 1111. Springer, Cham. ISBN: 978-3-030-37545-4

Jørgensen, R. (2018) *'Human Rights and Private Actors in the Online Domain.'* In Land, M., & Aronson, J. (Eds.). (2018) *'New Technologies for Human Rights Law and Practice.'* Cambridge: Cambridge University Press. DOI:10.1017/9781316838952

Kranenborg. H. (2014) *'Article 8 Protection of Personal Data'.* In Peers, S., Tamara, H., Kenner, J., Ward, A. (Eds) (2014), *The EU Charter of Fundamental Rights: A Commentary.* Oxford: Hart Publishing, 2014.

Laidlaw, E. (2015). *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility*. Cambridge: Cambridge University Press, 2015. doi:10.1017/CBO9781107278721

Leczykiewicz, D. (2020) *'Judical Development of EU Fundamental Rights Law in the Digital Era: A Fresh Look at the Concept of 'General Principles',* Chapter 3 in U. Bernitz, X. Groussot et. al, (eds) *General Principles of EU law and the EU Digital Order*, Kluwer Law International, 2020.

Lynskey, O. (2015) The foundations of EU data protection law (1st eds). Oxford University Press 2015.

Rosas, A., & Armati, L. (2018). *'EU Constitutional law: an introduction'* (Third edition). Hart Publishing, 2018

Woods, L. (2014) *'Article 11 Freedom of Expression and Information'.* In Peers, S., Tamara, H., Kenner, J., Ward, A. (Eds) (2014), *The EU Charter of Fundamental Rights: A Commentary.* Oxford: Hart Publishing, 2014.

Woods, L. (2017) *'Chapter 18: Digital freedom of expression in the EU',* in, Douglas-Scott, S., & Hatzis, N (eds). *'Research handbook on EU law and human rights',* 2017, Edward Elgar Publishing Limited. ISBN: 9781782546405

Electronic sources:

European Union Agency for Fundamental Rights and Council of Europe (2018) '*Handbook on European data protection law – 2018 edition*', Published 24 May 2018, accessed 2019-12-03 from https://fra.europa.eu/

Fransse, F. (2014) *'Melloni as a Wake-up Call – Setting Limits to Higher national Standards of Fundamental Rights' Protection'*, posted on 10 March 2014, accessed 2020-01-29 from: https://europeanlawblog.eu/2014/03/10/melloni-as-a-wake-up-call-setting-limits-to-higher-national-standards-of-fundamental-rights-protection/

Gstrein, Oskar J. *'The Judgment That Will Be Forgotten: How the ECJ Missed an Opportunity in Google vs CNIL (C-507/17), VerfBlog,* 2019/9/25', accessed 2020-03-07 from: https://verfassungsblog.de/the-judgment-that-will-be-forgotten/

Leiser, M & Schermer, B. *"GC & others vs CNIL and Google: This is a Special case"*, published 20 November 2019, accessed 2020-03-01, from: https://europeanlawblog.eu/2019/11/20/gc-others-vs-cnil-and-google-this-is-a-special-case/

Massé, E. & Pirkova, E. *'EU Court decides on two major "right to be forgotten" cases: there are no winners here',* published 23 October 2019, accessed 2020-02-21 from: https://www.accessnow.org/eu-court-decides-on-two-major-right-to-be-forgotten-cases-there-are-no-winners-here/

Peers, S. (2014) '*The CJEU's Google Spain judgment: failing to balance privacy and freedom of expression*', Posted 13 May 2014, retrieved 2020-01-17 from: http://eulawanalysis.blogspot.com/2014/05/the-cjeus-google-spain-judgment-failing.html

Samonte, M. *Google v CNIL Case C-507/17: The Territorial Scope of the Right to be Forgotten Under EU Law*, published 29 October 2019, accessed 2020-03-15 on: https://europeanlawblog.eu/2019/10/29/google-v-cnil-case-c-507-17-the-territorial-scope-of-the-right-to-be-forgotten-under-eu-law/

Articles:

Besselink, L. F. M. (2014). '*The parameters of constitutional conflict after Melloni.'* European Current Law, 2014(10), p. 1185.

Frantziou, E. (2014). *'Further Developments in the Right to Be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos.'* Human Rights Law Review, 14(4) pp. 761-777.

Frantziou, E. (2015). *'The Horizontal Effect of the Charter of Fundamental Rights of the EU: Rediscovering the Reasons for Horizontality'*, European Law Journal, Vol. 21, No. 5, September 2015, pp. 657-679.

Gill-Pedro, E & Groussot, X. (2017) 'The Duty of Mutual Trust in EU Law and the Duty to Secure Human Rights: Can the EU's Accession to the ECHR Ease the Tension?', Nordic Journal of Human Rights, 35:3, 258-274

Globocnik, J. (2020) *'The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17),'* GRUR International, 0(0), 2020, 1–9.

Lenaerts, K. (2012). *'Exploring the Limits of the EU Charter of Fundamental Rights'*. European Constitutional Law Review, 8(3), pp. 375 – 403.

Spaventa, E. (2015) *'a Very Fearful Court: The Protection of Fundamental Rights in the European Union after Opinion 2/13'*, Maastricht Journal of European and Comparative Law, 22(1), pp. 35- 56.

Spaventa, E. (2011) 'The horizontal application of fundamental rights as general principles of Union Law.', in A constitutional order of states : essays in honour of Alan Dashwood. Oxford: Hart Publishing, pp. 199-218.

Official Documents and Reports from European Union Institution:

Article 29 Working Party, (2014) *'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-131/13'*, 14/EN WP 225, Adopted on 26 November 2014

European Commission, (2019), *'Communication from the Commission to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions: Strengthening the Rule of Law within the Union - A blueprint For Action',* COM/2019/343 final, Brussels, 17 July 2019

European Commission, (2012) '*Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions: Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century*', COM/2012/09 final, 25 January 2012

European Data Protection Board, (2019), *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)*, Adopted on 2 December 2019.

Official Documents and Reports from the Council of Europe Institutions:

Council of the European Union, (2012) '*EU Strategic Framework and Action Plan on Human Rights and Democracy*', Luxembourg, 25 June 2012 11855/12.

Parliamentary Assembly of the Council of Europe, Resolution no. 1165 (1998) *'Right to Privacy'*, of 26 June 1998 on the right to privacy.

Recommendation No. R (97) 20 of the Committee of Ministers to member states on "hate speech", Adopted by the Committee of Ministers on 30 October 1997.

Recommendation CM/Rec(2012)3 of the Committee of Ministers to member states on the protection of human rights with regard to search engines, Adopted by the Committee of Ministers on 4 April 2012.

Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom, 13 April 2016.

Others:

Akdeniz. Y, Commissioned by the Office of the OSCE Representative on Freedom of the Media, (2016) *'Media Freedom on the Internet: an OSCE Guidebook'*, March 2016, accessed 2020-03-11 from: https://www.osce.org/netfreedom-guidebook?download=true

Arthur, C. '*Google faces deluge of requests to wipe details from search index'*. published 15 May 2014 sccessed 2020-01-17 on: https://www.theguardian.com/technology/2014/may/15/hundreds-google-wipe-details-search-index-right-forgotten

Committee of experts on the internet intermediaries, (2017) "Meeting report" (6 October 2017), MSI-NET (2017)06, *"Final draft study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*", Strasbourg, 6 October 2017, accessed 2019-12-28 from: https://rm.coe.int/msi-net-4th-meeting-18-19- september-2017/168075f8e9

Google's Transparency policy available at: *https://transparencyreport.google.com/*

Kelion L. (2019) '*Google wins landmark right to be forgotten case*', published 24 September 2019, accessed 2020-03-01 from: https://www.bbc.com/news/technology-49808208

Organisation for Security and Co-operation in Europe, (2014) *Communiqué by the Representative on Freedom of the Media on ruling of the European Union Court of Justice*, issued on 16 May 2014, accessed 2020-01-20 from: https://www.osce.org/fom/118632

United Nations Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40, 17 April 2013, accessed 2020-03-11 from: https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

Table of Cases

Presented in a chronological order

Court of Justice of the European Union:

Case 26/62 *van Gend & Loos*, 5 February 1963, EU:C:1963:1

Case 6/64 *Costa v. Enel*, 15 July 1964, EU:C:1964:66

Case 29/69 *Stauder,* 12 November 1969, EU:C:1969:57

Case 11/70 *Internationale Handelsgesellschaft*, 17 December 1970, EU:C:1970:114

Case 43/75 *Defrenne*, 8 April 1976, EU:C:1976:56

Case 294/83 *Les verts v. Parliament,* 23 April 1986, EU:C:1986:166

Case C-5/88 *Wachauf,* 13 July 1989, EU:C:1989:321

Case C.260/89 *ERT,* 18 June 1991, EU:C:1991:254

Case C-340/00P, *Commission v. Cwik*, 13 December 2001, EU:C:2001:701

Case C-101/01 *Lindqvist*, 6 November 2003, EU:C:2003:596

Cases C-39/05 P and C-52/05 *P, Sweden and Turco v. Council*, 1 July 2008, EU:C:2008:374

Joined cases C-402/05 P and C-415/05 P, *Kadi*, 3 September 2008, EU:C:2008:461

Case C-73/07 *Satamedia*, 16 December 2008, EU:C:2008:727

C-28/08 P *Bavarian Lager*, 29 June 2010, EU:C:2010:378

Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen*, 9 November 2010, EU:C:2010:662

Case C-70/10, *Scarlet Extended*, 24 November 2011, EU:C:2011:771

Joined Cases C-411/10 and C-493/10, *N.S.*, 21 December 2011, EU:C:2011:865

Case C-617/10 *Åklagaren v Åkerberg Fransson*, 26 February 2013, EU:C:2012:340

Case C-399/11 *Stefano Melloni v Ministerio Fiscal*, 26 February 2013, EU:C:2013:107

Case C-176/12 *Association de médiation sociale*, 15 January 2014, EU:C:2014:2

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland*, 8 April 2014, EU:C:2014:238

Case C-131/12 *Google Spain*, 13 May 2014, EU:C:2014:317

Case C-105/14 *Taricco I,* 8 September 2015, EU:C:2015:555

Case C-362/14 *Schrems,* 6 October 2015, EU:C:2015:650

Joined Cases C-203/15 and C-698-15, *Tele2 Sverige AB*, 21 December 2016, EU:C:2016:970

Case C-404/15 *Aranyosi and Căldăraru*, 5 April 2016, EU:C:2016:198

Case C-578/16 *PPU CK and others v Slovenia*, 16 February 2017, EU:C:2017:127

Case C-42/17 *M.A.S and M.B. (Taricco II)*, 5 December 2017, EU:C:2017:936

Case C-619/18 *Commission v Poland*, 24 June 2019, EU:C:2019:531

Case C-136/17 *GC and others v CNIL*, 24 September 2019, EU:C:2019:773

Case C-507/17 *Google v CNIL,* 24 September 2019, EU:C:2019:772

Joined Cases C-609/17 and C-610/17 *TNS*, 19 November 2019, EU:C:2019:981

European Court of Human Rigts:

Sunday Times v. United Kingdom judgment of 26 April 1979, no. 6538/74, CE:ECHR:1979:0426JUD000653874

Leander v. Sweden, 26 March 1987, no. 9248/81 CE:ECHR:1987:0326JUD000924881

Niemietz v. Germany, 16 December 1992, no. 13710/88 CE:ECHR:1992:1216JUD001371088

Z v. Finland, 25 February 1997, no. 22009/93, CE:ECHR:1997:0225JUD002200993

Amann v. Switzerland, 16 February 2000, no. 27798/95, CE:ECHR:2000:0216JUD002779895

Editorial Board of Pravoye Delo and Shtekel v. Ukraine, 5 May 2011, no. 33014/05 CE:ECHR:2011:0505JUD003301405

Axel Springer AG v. Germany, 7 February 2012, No: 39954/08, CE:ECHR:2012:0207JUD003995408

Ahmet Yldrim v. Turkey, 18 December 2012, No. 3111/10 CE:ECHR:2012:1218JUD000311110

Neij and Sunde Kolmisoppi v. Sweden, 19 February 2013, no. 40397/12, CE:ECHR:2013:0219DEC004039712

Węgrzynowski and Smolczewski v. Poland, 16 July 2013, no. 33846/07, CE:ECHR:2013:0716JUD003384607

Delfi AS v. Estonia, 10 October 2013, no. 64569/09, CE:ECHR:2013:1010JUD006456909

Gough v. The United Kingdom, 28 October 2014, no. 49327/11 CE:ECHR:2014:1028JUD004932711

M.L and W.W v. Germany, 28 June 2018, nos. 60798/10 and 65599/10, CE:ECHR:2018:0628JUD006079810

Times Newspaper Limited v. United Kingdom, 13 November 2018, No. 64367/14, CE:ECHR:2018:1113DEC006436714

Opinions by Advocate Generals of the Court of Justice of the European Union:

Opinion of Advocate General Poiares Maduro delivered on 21 May 2008, C-127/07 *Société Arcelor Atlantique et Lorraine and Others v Premier ministre, Ministre de l'Écologie et du Développement durable and Ministre de l'Économie, des Finances et de l'Industrie,* EU:C:2008:292

Opinion of Advocate General Kokott delivered on 8 May 2008, C-73/07 *Satamedia,* EU:C:2008:266

Opinion of Advocate General Trstenjak delivered on 24 November 2010, *MSD Sharp & Dohme GmbH v Merckle GmbH.* EU:C:2010:712

Opinion of Advocate General Jääskinen delivered on 25 June 2013, C-131/12 *Google Spain*, EU:C:2013:424

Opinion of Advocate General Szpunar delivered on 10 January 2019, C-136/17 *GC and Others*, EU:C:2019:14

Opinion of Advocate General Szpunar delivered on 10 January 2019, C-507/17 *Google CNIL*, EU:C:2019:15

Opinions by the Court of Justice of the European Union:

Opinion 2/13 of the Court (Full Court) delivered on 18 December 2014, EU:C:2014:2454

Table of Legislation

Legislation adopted by the European Union

Primary Law:
Charter of Fundamental Rights of the European Union [2012] OJ C326/02

Treaty on the European Union (consolidated version) [2012] OJ C326/13

Treaty on the Functioning of the European Union (consolidated version) [2012] OJ C236/47

Secondary Law:
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (consolidated version) [1995] OJ L 281, 23.11.1995, p. 31–50

Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31.5.2001 p. 43 – 48

Regulation (EU) 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast) [2013], OJ L. 180/31-180/59 29.6.2013

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (consolidated version) [2016] OJ L 119, 4.5.2016, p. 1–88

Other:
Explanations Relating to the Charter of Fundamental Rights, [2007] OJ C303/2

Legislation adopted by the Council of Europe:

Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, Rome, 4 November 1950, ETS 5

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108