The content and implications of the Right to be Forgotten:

Confrontation between the European Union and the United-States.

Research dissertation presented in partial fulfilment of the requirements for the degree of LLM in International Law

(Quality and Qualifications Ireland)

Law School, Griffith College Dublin

Lucile Singer

2016

Acknowledgements

Foremost, I would like to express my gratitude to my thesis supervisor, Dr Susan Power.
I would like to thank her for her precious guidance throughout my thesis research, her continuous support and enthusiasm. Her valued feedback was essential for the improvement of my thesis.

I would also like to thank my family: my parents for encouraging me throughout my university education; my sister for her support when I needed it the most.
Thank you also to my boyfriend who stood by my side throughout this year of hard work.

Abstract

In the Google Spain-Costeja case the CJEU recognised formally a right to be forgotten. It revived the traditional debate on privacy v freedom of speech.

This thesis will first define the right to be forgotten from a theoretical point of view, using scholarly work. It will next demonstrate that the right to be forgotten fits intro broader personality rights such as the right to privacy and the right to personal identity.

Secondly, this study will consider the right to be forgotten in the United-States. It will show that it is not a new concept in the US. The United States will be compared to the EU jurisdiction, particularly its different approach to legislate privacy and its different ideology subordinated to First Amendment rights.

Thirdly, the thesis will focus on the European Union and present how the concept of the right to be forgotten has evolved throughout history. After analysing the CJEU landmark ruling, this thesis will examine its implications on the search engines. A case study on France will then demonstrate that the implementation of the right to be forgotten was highly expected in some of the European States.

Lastly, this thesis will assess the responsibility placed by the CJEU on the search engine's shoulders. They have a quasi-judicial role regarding the processing of delisting requests. The thesis will show that these multinational corporations have economic interests that do not encourage them to respect the right to be forgotten. The thesis will also deal with the controversial issue on the extra-territorial application of the right to be forgotten in the United-States.

The thesis will conclude that the European and American perspectives are not incompatible. However, the implementation of a European-style right to be forgotten in the US would be very difficult because of the strong hurdles. The shape of the right to be forgotten should change in order to establish a common right to be forgotten. It might be necessary to conclude an international treaty to harmonise State practice on the right to be forgotten.

Table of contents

Introduction

The right to be forgotten is associated with the landmark decision rendered by the Court of Justice of the European Union (CJEU) on 13th May 2013.[1] The Court interpreted broadly the Data Protection Directive and held that Internet users have a right to be forgotten regarding their private data that is no longer 'relevant, inadequate or excessive in relation to the purposes of the processing'.[2] Therefore, individuals have the right, under certain conditions, to request search engines to remove links to pages containing information about them.
Accordingly, the right to be forgotten has arisen from the new challenges posed by two aspects of the expansion of the Internet: the storage of increasing amounts of personal data online and their easier accessibility, especially because of the widespread trend of sharing personal information.

The amount of data generated on the Internet is massive. In 2012, the global Internet population was around 2.1 billion people. Every minute in 2012, more than 2,000,000 search queries were received by Google, 204,166,167 emails were sent, 571 new websites were created, 684,478 pieces of content were shared on Facebook, 100,000 tweets were sent, 3,600 new photos were shared on Instagram, 48 hours of new video were uploaded on Youtube, and around 47 000 app downloads were received by Apple.[3] Being present online is more than a benefit, it has become an obligation in terns of enterprise, contributing to the growth of big data. In addition to the need to feel socially integrated, people build virtual identities[4] through online profiles to sell themselves and stay competitive on the labour market.

The key question arises: what happen to all of this information? It remains on the Internet as digital memory is eternal. Moreover, storage capacities have developed considerably while their costs have diminished. Therefore the economic cost of deleting does not encourage search engines to destroy or anonymise data.[5]

---

[1] Case C-131/12 Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario
[2] Ibid.
[3] Neil Spencer, 'How much data is created every minute ? ' (2012) Visual News <https://www.visualnews.com/2012/06/19/how-much-data-created-every-minute/?view=infographic> accessed 12 August.
[4] Craig Ross, Emily S. Orr, Mia Sisic, Jaime M. Arseneault, Mary G. Simmering, R. Robert Orr, 'Personality and motivations associated with Facebook use' [2009] Computers in Human Behavior 578.

[5] Cécile de Terwangne, 'The Right to be Forgotten and Informational Autonomy in the Digital Environment' in Alessia Ghezzi, Angela Guimaraes Pereira and Lucia Vesnic-Alujevic (eds), *The Ethics of Memory in a Digital Age* (Palgrave Macmillan 2014), 85.

Cécile de Terwangne posits that the eternal memory of the Internet contrasts with the limits of human memory.[6] Memory being linked to forgetfulness, Mayer-Schönberger, one of the most influential scholars on the issue, compared 'the unforgiving nature of persistent digital memory with the possibilities of forgiveness arising from human forgetfulness'.[7] In real life, forgetfulness is spontaneous and not intentional.[8] On the contrary, forgetfulness in cyberspace is a conscious and desired process. It requires the will to erase private information. Therefore, allowing individuals to move on from their past and to start fresh is not forgetting; it is rather a choice and needs willingness. The digital right to be forgotten is a societal capacity to offer forgiveness and free individuals from the burden of their digital baggage.[9]

A famous case study to illustrate the risks linked to the sharing of private data is that of Stady Snyder. This American student was refused graduation for her teaching degree because her college in Pennsylvania discovered a photograph she posted of her on MySpace wearing a pirate's hat and drinking from a plastic cup with the caption 'drunken pirate'.[10] This case demonstrates that digital memory prevents individuals from dissociating themselves from humiliating past moments. As such, social networks exacerbate the problem of digital eternity, and youth are particularly subject to the risks because of the poor choices they may make unwittingly.[11]

Search engines are so efficient that they enable one to gather all information about an individual. The results can be harmful. Information disclosed by both third parties and the individual himself can raise concerns.[12] At an earlier stage, the individual agrees to disclose information to a determined circle, for example family and friends. However, search engines make the information accessible outside the initial context.[13] Therefore, information posted in one particular context may be used in another context, such as the educational or professional context.[14] Many recruiters check an applicant Facebook profile to make a preliminary

---

[6] Ibid 84.
[7] V. Mayer-Schonberger, *Delete : The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009).
[8] Cécile de Terwangne (n 6).
[9] V. Mayer-Schonberger (n 8).
[10] Ibid.
[11] David Lindsay, 'The « Right to Be Forgotten »' in Normann Witzleb, David Lindsay, Moira Paterson and Sharon Rodrick (eds), *Emerging Challenges in Privacy Law* (Cambridge University Press 2014).
[12] Cécile de Terwangne (n 6).
[13] Cécile de Terwangne (n 6) 84.
[14] H. Nissenbaum, 'Privacy as Cotextual Integrity' (2004) 79 Washington Law Review 119.

judgment on him. The latter can be detrimental to the person concerned. The threat of being penalised by the digital past is considerable and individual's autonomy and self-determination are challenged. Viviane Redding, the EU Justice Commissionner, underlined the problems arising with digital eternity in the following way:

> *'The Internet has an almost unlimited search and memory capacity. So even tiny scraps of personal information can have a huge impact, even years after they were shared or made public. The right to be forgotten will build on already existing rules to better cope with privacy risks online'.*[15]

Therefore, the right to be forgotten represents a strong response to these risks. However, the right to be forgotten is not an absolute right and revives the traditional debate to determine the adequate balance between privacy on the one hand and on the other, freedom of speech and public's right to information.

The May 2014 CJEU ruling[16] has drawn attention worldwide. The European Union is not the only jurisdiction to struggle to balance those rights. In Argentina, two hundred plaintiffs including actresses, models or athletes have filed lawsuit against search engines to demand the removal of links to their photographs.[17] Additionally, a Japanese Court recently recognised the right to be forgotten in a lawsuit against Google.[18] Nevertheless, this thesis will confront the perspectives of the European Union, the cradle of the right to be forgotten, and the United States, home to the major companies such as Google, Facebook and Yahoo. As these two regions have different views on privacy and freedom of expression, it is all the more difficult to find the right balance.

---

[15] V.Reding, Vice-President of the European Commission, Eu Justice commissionner, 'The EU Data protection Reform 2012 : Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age' (Speech delivred at Innovation Conference Digital, Life, Design, Munich, 22 January 2012).

[16] *Google Spain Costeja* (n 2)

[17] Edward L. Carter, 'Argentina's Right to be Forgotten' 27(1) Emory International Law Review 23, 24-25. The case of the singer Virginia Da Cunha is the most significant case. In 2009, she won against Google and Yahoo in the trial Court but lost on appeal in 2010; Da Cunha Virginia c/ Yahoo de Argentina SRL y otro s/ Daños y perjuicios (Juz. Nac. En lo Civil nø 75, Expte. Nø 99.620/06), 29 July 2009.

[18] Justin McCurry, 'Japan recognises « right to be forgotten » of man convicted of child sex offences' *The Guardian* (London, 1 March 2016).

The scope of application of the right to be forgotten covers different sectors. In several countries, a right to be forgotten exists in regards to criminal records. For instance, The Criminal Justice (Spent Convictions and Certain disclosures) Bill 2012 is currently in progress in Ireland.[19] When signed into law and enacted, certain convictions will become 'spent' after a rehabilitative period, removing obstacles to employment, education, and insurance.[20] Furthermore, the right to be forgotten can apply to medical records. For example, cancer survivors may request the right not to have their medical histories considered when getting bank loans, credit or insurance policies. France has achieved some progress in this regard, establishing a right to be forgotten for cancer patients in 2015, which provides them the access to bank credit under certain conditions.[21] Therefore the right to be forgotten affects different fields but is always defined by the same rationale: not being penalised by one's past.

This thesis will focus on the digital right to be forgotten as it has developed considerably over the past few years and raises many controversial issues. The methodologies the most used in researching the thesis are that of doctrinal analysis and comparative methodology. The former was used to define the right to be forgotten and analyse EU and US legislation on it. The latter was employed to confront the different conceptions of privacy in the United-States and Europe and to assess how they influence the implementation of a right to be forgotten.

One major issue which the thesis addresses is whether the European Union can persuade the United-States to apply the European-style right to be forgotten. In this vein, can the different views on privacy and freedom of speech be reconciled?

The thesis is divided into four chapters. The first chapter will define the right to be forgotten from a theoretical perspective distinguishing it from similar related notions. It will then examine how the right to be forgotten is connected to broader human rights such as the rights to privacy and identity. The second chapter will consider the United States' perspective on the

---

[19] The bill was debated and passed through both houses of the Oireachtas in January and February 2016. The bill will become known as the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016 when signed into law by President of Ireland.

[20] 'Passing of Spent Convictions legislation a historic step for Ireland, but could go much further' (*Irish Penal Reform Trust*, 3 February 2016) <http://www.iprt.ie/contents/2856> accessed 29 June 2016.

[21] 'New rules benefit cancer survivors' *The Connexion* (Nice, 12 April 2015) available at <http://www.connexionfrance.com/france-cancer-loan-insurance-companies-right-forgotten-disease-francois-hollande-16837-view-article.html>. Cancer patients are now able to take out insurance without waiting fifteen years after the end of their disease, but only ten years. The youth who reported their cancer before 18 years old may benefit from the right to be forgotten five years after the end of their disease.

right to be forgotten, starting with an overview of the different facets of the right to be forgotten as it has been observed in different sectors such as criminal law, bankruptcy and credit reporting. It will next give an overview on how privacy is perceived in American society and protected by the US legal system. Finally it will explore the main obstacles to the implementation of a European-style right to be forgotten in the US.

The third chapter will describe the evolution of the EU data protection laws that progressively recognised a right to be forgotten. Particular emphasis will be placed on the landmark decision of the Court of Justice of the European Union in the Google Spain Case.[22] It will next focus on France as a case study to evidence that the right to be forgotten was strongly expected in some European countries and implemented as soon as the CJEU rendered its decision. The final chapter will analyse the consequences of the Google Spain ruling on the search engines and particularly discuss the extra-territorial application of the European right to be forgotten in the United States. It will examine the main issues that arise, especially the unwanted responsibility that search engines must face and the uncertainties regarding the respect of the right to be forgotten.

[22] *Google Spain Costeja* 13

Chapter 1. Definition of the Right to be Forgotten

1.1 Related notions: same meaning?

There is a lack of homogeneity regarding the definition of the concept of the Right to be Forgotten. Some scholars or politicians use the terms 'Right to Deletion', 'Right to Forget', 'Right to Erasure', 'Right to be Forgotten' interchangeably while others believe these notions have a different meaning. [23] It is therefore necessary to examine the scope and significance of each of them in turn.

1.1.1 'The right to forget' and the Right to be Forgotten'

Antoinette Rouvroy considers that the right to be forgotten can be conceived as 'a legitimate interest to forget and be forgotten'.[24] This formulation highlights the two elements sought by the right to be forgotten: being forgotten and forgetting. [25] The right to be forgotten involves third parties who can forget an individual's past whereas the right to forget only concerns the individual capable of forgetting his/her past, changing his/her mind and whose future is not jeopardised by his/her past or present. [26] It would be very difficult to establish a right for persons to forget themselves. It seems from the above that Antoinette Rouvroy meant that the right to be forgotten and the right to forget are two rights which are inseparable. Indeed, a person is able to forget her/his past and start over in life only if third parties stop reminding them of their past actions.

Weber makes the same distinction between these active and passive components of 'the right to forget' and the 'right to be forgotten'. He defines the former as 'a historical event (...) no longer (...) revitalised due to the length of time elapsed since its occurrence' whereas the latter 'reflects the claim of an individual to have certain data deleted so that third persons can

---

[23] Aurelia Tamò and Damian George, 'Oblivion, Erasure and Forgetting in the Digital Age' (2014) 5 JIPITEC.
[24] Antoinette Rouvroy, 'Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?', version augmentée du chapitre paru, sous le même titre, dans Stéphanie Lacour (ed), *La sécurité de l'individu numérisé* (L'Harmattan 2008). Available at: http://works.bepress.com/antoinette_rouvroy/5, 25.
[25] Bert-Jaap Koops, 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the ''Right To Be Forgotten'' in Big Data Practice' (2011) 8(3) SCRIPTed, 3.
[26] Ibid.

no longer trace them'. [27] The contrast between the individual perspective and the third parties is present but Weber adds also a criterion of time. Indeed, the right to forget may be invoked only when personal information is no longer relevant due to the passing of time. On the contrary, an individual may always claim its right to be forgotten without considering the lapse of time. [28]

1.1.2 The 'Right not to Know'

The author Herman makes also the distinction between the 'Right not to Know' and the Right to Be Forgotten. Indeed, the article 10 of the Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine[29] provides that everyone is entitled to know any information about his/her health but can also wish not to be informed.[30] However, this right can be subject to restrictions in the interest of the patient. Whereas the 'Right not to Know' plans that the person exercising his/her right does not want to know her/ his status, the Right to be Forgotten enables third parties to forget about the person concerned and their personal data. By these two notions, Herman shows the 'autonomy of the person concerned' that maintains her will to control the accessibility to her private data. [31]

1.1.3 The Right to Oblivion and the Right to be Forgotten

The concept of the 'right to be forgotten' is known in French as the *droit à l'oubli*[32], and in Italian as *diritto al'oblio.*[33] The right to oblivion is a closer translation of these terms. It includes both 'being forgotten' (the right for individuals to have their past forgotten by third

---

[27] Rolf H. Weber, 'The Right to Be Forgotten : More Than a Pandora's Box' (2011) 2 JIPITEC 120, 120-121.
[28] Ibid.

[29] Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine [1997] OJ No.164/01.
[30] 'Everyone is entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed'.

[31] Herman Nys, 'towards a Human Right 'to Be Forgotten Online' (2011) 18 (5) European Journal of Health Law 469.
[32] Koops (n 26) 4.
[33] Norberto Nuno Gomes de Andrade, 'Oblivion : The Right to be Different...from Oneself : Re-proposing the Right to be Forgotten' in Alessia Ghezzi, Angela Guimaraes Pereira and Lucia Vesnic-Alujevic (eds), *The Ethics of Memory in a Digital Age* (Palgrave Macmillan 2014), 65.

parties) and "forgetting' (the right for individuals to forget their own antecedents) but we will analyse these two elements in detail below. [34]

Cécile de Terwangle associated the right to oblivion to the right to be forgotten and therefore asserts these notions are equal. She defined the Right to be Forgotten (or the Right to Oblivion) as the right to have private information erased after a specific period of time.[35] She distinguished three aspects of this right: 'the right to oblivion of the judicial past', 'the right to oblivion established by data protection legislation' and 'the digital right to oblivion'. [36]

The first form of the right to oblivion, or right to be forgotten refers to an individual's criminal past. Cécile de Terwangne explained that the Right to Oblivion linked to criminal records has been admitted by case law in several countries. The Right to be Forgotten regarding the judicial past is based both on the right to privacy and personality rights. Indeed, most societies permit an individual who has finished his sentence to restart his life without being reduced to his past through reintegration and rehabilitation. The author highlighted that today the Right to Oblivion of the judicial past is not reduced to criminal records, its scope is extended broadly. Several questions arise on whether a former convict can ask the deletion of his judicial past in case law databases and newspapers archives under the Right to Oblivion. [37] The second facet of the Right to oblivion according to De Terwangne is the one set by the Data Protection Legislation. The latter enables the extension of the right to oblivion, which is not longer limited to criminal past but can be implemented to the processing of any personal data.[38] This will be discussed in details later in the dissertation when we will analyse the historical development of the Right to be Forgotten. Finally, Cecile de Terwangne considers that the Right to Oblivion has a third dimension: the Digital Right to Oblivion. This new right claimed would permit to respond to the issues born from the development of Internet services such as the infinite Internet's capacity of memory. This 'new right' would be more extended, precisely applicable in the digital environment. Personal data would automatically be erased after an expiration date, which would need to be fixed, and therefore the erasure is not

[34] Meg Leta Ambrose and Jef Ausloos 'The Right to Be Forgotten Across the Pond' (2013) 3 Journal of Information Policy 1, 14.
[35] Cécile de Terwangne, 'Internet Privacy and the Right to Be Forgotten/Right to Oblivion' (2012) IDP 109, 109.
[36] Ibid.
[37] Ibid 111-112.
[38] Ibid 113.

decided on a case-by-case basis. This right could also enable the permanent deletion of personal data published by individual themselves, notably through social networks. [39]

Noberto Nuno Gomes de Andrade also uses the terms right to be Forgotten and right to oblivion interchangeably. Nevertheless, he explains the concept of this right not only from a privacy perspective but also from an identity point of view. He distinguishes the right to privacy and the right to identity in the following approach. Although they both constitute personality rights, the right to privacy protects true private facts from their disclosure in the public sphere. On the contrary, the right to identity ensures that the transmission of personal information to the public knowledge, whether true or not, defaming or not, does not reflect a wrong image of his/her personality. [40]

The author adds that one type of information is not protected by any of the rights to privacy and protection against defamation: de-contextualised information, that is to say information no longer truthful or out-dated information because of the passing of time. This kind of information leads to an inaccurate representation of the person's identity. Therefore, the combination of the right to be forgotten and the right to personal identity protects this other category of information.[41] To summarise, Noberto Nuno Gomes de Andrade argues that the right to be forgotten is a 'procedural data protection right' whose aim is to protect an individual's personal identity in a wider way. In other words, the right to deletion is a legal instrument allowing to be different from oneself, not determined by one's past and to start again. [42]

1.1.4 The Right to Erasure and the Right to be Forgotten

The right to erasure is guaranteed by Article 12(b) of Directive 95/46. The latter provides that 'every data subject (has) the right to obtain from the controller the (…) erasure or blocking of data processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data'. Cécile de Terwangne considers the Right of Erasure as a way for the subject data to achieve compliance with the protection

[39] Ibid 119.
[40] Norberto Nuno Gomes de Andrade (n 34) 65-68.
[41] Ibid 70.
[42] Ibid 68-76.

rules. Therefore she considers the Right of Erasure as being part of the Right to be Forgotten.[43]

Meg Leta Ambrose and Jef Ausloos also differentiate the right to erasure from the right to oblivion but in a different way. Nevertheless, they both maintain that the right to oblivion and the right to erasure are 'two interpretations of the right to be forgotten'.[44] Therefore, they claim that the combination of these two rights constitute the right to be forgotten defined in European Commission's 2012 proposed Data Protection Regulation[45] but assess that its respective scope and rationale are unclearly displayed.[46] According to Ambrose and Ausloos, it is necessary to highlight the distinction between the right to oblivion and right to erasure.

The right to oblivion is an older right, which was historically applied to expunge an individual's criminal past in exceptional cases. On the other hand, the right to erasure deals with the deletion of personal information that a subject data has released for an automatic processing by third parties. Therefore, the latter is a mechanical right that intends to erase information shared passively by users for commercial or marketing purposes.[47] The right to oblivion, founded on privacy grounds, aims to protect an individual's identity, personality, dignity and reputation but is in conflict with the right to information. On the contrary, the right to erasure enables to balance the power between data users and data controllers by giving the opportunity to the users to withdraw their consent to the collect and proceeding of their private information at any time.

Finally, another important difference between these rights is time. Indeed, while the right to oblivion may be invoked only after a certain period of time, the right to erasure does not necessarily require an element of time. [48]

---

[43] Cécile de Terwangne (n 6) 94.

[44] Meg Leta Ambrose and Jef Ausloos (n 35).

[45] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) COM(2012) 11 final, 25 January 2012.

[46] Meg Leta Ambrose and Jef Ausloos (n 35) 1-2.

[47] Ibid 2-14.

[48] Ibid 2-15.

1.2 Theoretical definitions

The right to be forgotten is difficult to define because there is no consensus on its meaning.[49] Koops discerns three angles on the right to be forgotten among policy and academic literature. The first dominant approach asserts that personal information may be deleted after a certain length of time. The second one underlines that outdated personal data should not be taken into consideration in order for an individual not to be identified according to his/her past. The third approach also analyses the right to be forgotten as a way to make a 'fresh start' but not from society's point of view but rather from the individual's perspective: he/she should not be threatened by the future consequences of what he/she expresses now. [50]

Cécile de Terwangne affirms that the right to be forgotten, which used to be restricted to a criminal past, was initially linked to the passage of time. Now, with the extension of its scope, the right to be forgotten is associated with informational autonomy. [51] The latter, also known as self-determination denotes control by individuals over their personal data. They can chose which personal information they want to reveal, to whom and for what goal. Informational autonomy is part of the right to privacy and especially of individual autonomy: individuals must be able to make their own decisions regarding certain aspects of their lives. [52] However, this author underlines that this right to 'informational self-determination' faces other interests such as public interest or historical interest and other rights (right to information) that may limit the right to self-determination behind the right to be forgotten. [53]

From the above it is clear that the authors have different conceptions of the right to be forgotten, regarding its scope and meaning. Moreover, according to several authors, the right to be forgotten is not only a legal right but may also constitute a policy aim or a value or interest worthy of protection.[54] However, although the authors do not agree on the same definition, it seems that some aspects of the right to be forgotten are accepted by all, namely

[49] Bert-Jaap Koops (n 26) 2.
[50] Ibid 5-6.
[51] Cécile de Terwangne (n 6) 87.
[52] Ibid 85-86.
[53] Ibid 87-92.
[54] Bert-Jaap Koops (n 26) 14.

that individuals have an interest not to be identified by others according to their past, especially when these past events are not relevant today. [55]

Nevertheless, Cécile de Terwangne insists on the fact that the right to be forgotten does not permit individuals to re-write their past and delete their undesirable past acts. On the other hand, the concept is to show that an individuals' future is not mapped out by their past and that their circumstances can change.[56] De Terwangne adds that currently, another aspect of the right to be forgotten is claimed: the right to delete private data when no longer needed for legitimate purposes (the individual revoked his/her consent or the storage period has expired). This recent facet of the right to be forgotten does not refer necessarily to the link between the past and the present, as the older one. This evolution demonstrates that the right to be forgotten must be protected under informational self-determination. Therefore, De Terwangne argues that the right to be forgotten is 'the right to require someone to forget (delete) what he/she knew because it is not legitimate to keep knowing it'.[57]

1.3 The Right to be Forgotten, as a component of broader human rights?

The key question that arises is what is the nature of the right to be forgotten. We can wonder whether it fits into broader human rights theories, notably personal rights theories. The right to be forgotten is undoubtedly linked to the rights to privacy and right to identity.

Jed Rubenfeld analyses the scope of the constitutional right to privacy. He maintains that the right to privacy is used as a 'constitutional limit on governmental power'.[58] He distinguishes two different concepts of privacy. There is the right to privacy created to protect the intrusion upon one's life by the conduct of other individuals. There is also the substantive right to privacy that concerns the right holder's own choices and actions, such as using contraceptives or aborting a pregnancy.[59]

The right to be forgotten results from the right to privacy understood in the first meaning, namely the informational sense. Rubenfeld specifies that this right to privacy limits the ability

---

[55] Ibid 4.
[56] Cécile de Terwangne (n 6) 83.
[57] Ibid 83-84.
[58] Jed Rubenfeld, 'The Right to Privacy' (1989) 102(4) Harvard Law Review 737, 737.
[59] Ibid 740.

of other individuals to disseminate private information or use it against oneself. According to him, both are constitutional rights but the substantive right to privacy is of a more recent origin whereas the informational right to privacy emerged, in the United States, with the Fourth Amendment and tort law.[60]

As we have seen earlier,[61] Noberto Nuno Gomes de Andrade defines the right to be forgotten not only from a privacy standpoint but also considers the right to identity. The author believes that the right to be forgotten is a data protection right creating a procedural right to request the removal of personal information.[62] The right to be forgotten pursues the protection of two substantive rights: the rights to privacy and identity. These two personality rights both derive from fundamental rights to dignity and self-determination.[63] Moreover, Noberto Nuno Gomes de Andrade emphasises that there are important differences between the right to privacy and the right to identity. Indeed, the right to identity concerns the transmission of the correct image that an individual wished to project in society. The individual desires that the main attributes of his personality (such as his name, life history, character and appearance) to be recognised and respected by society. On the contrary, the right to privacy concerns the protection of personal information from being disclosed to the public.[64] Noberto Nuno Gomes de Andrade argues that identity is a *'cultural and social contruct, something we choose, construct and adhere to'*.[65] The right to be forgotten is a tool to be used in the process of negotiation and choices to make enabling to create new identities by removing previous ones.[66]

---

[60] Ibid 740.
[61] See pages 14-15.
[62] Norberto Nuno Gomes de Andrade (n 34) 67-63.
[63] Ibid 67-63.
[64] Ibid 67-63.
[65] Ibid 67-63.
[66] Ibid 67-63.

Chapter 2. The United States' perspective on the right to be forgotten

2.1 Is there a right to be forgotten in the United States?

Currently, no digital right to be forgotten is recognised by a common law or statutory scheme in the United States, or at least not in the same way the Europeans define it.[67] However, the United States has a certain experience with the notion of 'forgive and forget'.[68] Several cases such as *Melvin v. Reid* (1931)[69] or *Briscoe v. Reader's Digest Association, Inc* (1971)[70] deal with it and their argumentation emphasises the importance of legal forgiveness in one's rehabilitation, even though they were finally overruled in the name of the First Amendment, which protects the freedom of expression. Indeed, in both cases the defendant was accused of violation of the plaintiff's privacy because of the use of his criminal past and his name in a movie or documentary. Notwithstanding, the Court considered in both cases that this use was inhibiting the process of rehabilitation. However, in both final judgements, it was held that there were no causes of action as those facts were true and of public record.

However, the right to be forgotten is not an unknown concept in the United Sates. US laws recognise some variations of a 'right to be forgotten' in other fields than in cyberspace: for example, criminal law, bankruptcy and credit reporting, among others. [71] Because a reputation as a former criminal can represent a burden when starting again in life and becoming part of the society, pardons and statutes of limitations enable an individual to move on from their past mistakes. Furthermore, the use of criminal records, and particularly of juvenile criminal records[72], is governed by sealing and expungement policies. States such as New-York[73] or Wisconsin[74] prohibit denial of employment because of a previous conviction. A measure to postpone the background checks of applicants until after the preliminary hiring decisions has

---

[67] Giovanna Giampa, 'Americans Have a Right to Be Forgotten' (Law School Student Scholarship, Seton Hall University 2016), 11.
[68] Steven C. Bennett, 'The ''Right to Be Forgotten'' : Reconciling EU and US Perspectives' (2012) 30(1) BERKELEY J. INT'L 161, 167.
[69] Melvin v Reid [1931] 112 285 (Call. App).
[70] Briscoe v. Reader's Digest Association, Inc (1971)

[71] Steven C. Bennett (n 69)167.
[72] In most states, the person making the request for juvenile record sealing must be at least eighteen years old ; Kathleen Michon, 'sealing Juvenile Court Records' (nolo.com) < http://www.nolo.com/legal-encyclopedia/sealing-juvenile-court-records-32228.html> accessed 8 August 2016.
[73] N.Y Correction Law § 752 (2010).
[74] Wisconsin Statute §111.321 (2010)

been adopted in other states.[75] These schemes aim to facilitate the rehabilitation.

Similarly, bankruptcy law provisions incorporate the principles of legal forgiveness. For example, the bankruptcy code prohibits private and public actors from discriminating former debtors on that status[76], in order to reduce the stigma of bankruptcy information.[77]Another representative field is the field of credit reporting by limiting the dissemination of financial information about them.[78] The Fair Credit Reporting Act prevents the spread of inaccurate information[79] and unauthorised invasions of the consumers' right to privacy.[80]

Lastly, one shall also mention the law SB-568 adopted by California Governor Jerry Brown in September 2013 and effective since 2015, which gives children a new tool to protect their digital privacy. Often heedless of the consequences of their actions and the consequences of their publications, minors must be protected against themselves. The bill protects Californian minors in two important ways:

- It requires an "eraser button" on websites directed to minors so they can remove information they personally posted on websites, online services, and mobile apps.
- It prohibits websites, online services, and mobile apps aimed at minors from marketing certain dangerous goods or services.

However, the enforcement of the law remains severely limited. First, it applies only to Californian residents and only to minors. Secondly, the law applies only to content uploaded by the minor making the request. The real problem arises when this content is posted by a third party; this case is not covered by the law.[81] Although the law is already controversial because of its limited effectiveness, it may be considered as a first step towards effective protection for minors.

This subsection has shown that the idea of a right to be forgotten exists in the United States, and applies already in different sectors, but in a limited capacity. Adapting the right to be

---

[75] See for instance Minnesota Statute §364.021 (2009), Connecticut General Statute §10-142 (2010), Massachusetts Acts, Ch. 256.
[76] 15 U.S.C. § 525 (a).
[77] Meg Leta Ambrose and Jef Ausloos (n 35) 9.
[78] Ibid 9.
[79] *Treadway v. Gateway Chevrolet Oldsmobile Inc.* (7th Circuit, 2004).
[80] *In re Grand Jury Subpoena to Credit Bureau of Greater Harrisburg* (Middle District, Pennsylvania, 1984).
[81] Rahul Kapoor, W. Reece Hirsh and Shokoh H. Yaghoubi, « Get to know California's 'Online Eraser' Law » The National Law Review (12 July 2016) < https://en.wikipedia.org/wiki/The_National_Law_Review> accessed 21 July 2016.

forgotten in the digital age is challenging and faces many hurdles, including the strength of the First Amendment but this will be discussed in detail later.

2.2 Privacy in the United States

Having analysed whether the American legal system provides a 'Right to be Forgotten', we will now focus on the American view on privacy and next outline the main legal mechanisms, which permit an individual to control the flow of his private information.

2.2.1 Brief history on privacy in the United-States and its different conception from Europe

To further understand the issues relative to personal privacy in the online environment, it is necessary to examine the general right to privacy in the United States.

Curiously, the right to privacy traced its roots in a law review article, co-authored in 1890 by two Boston lawyers Samuel D. Warren and Louis Brandeis and entitled the 'Right to Privacy'.[82] They characterised the right to privacy as 'the right to be let alone' [83] and notably maintained that it 'secures (...) each individual the rights of determining, ordinarily, to what extent his thoughts, sentiments and emotions shall be communicated to others'. [84]
This law review article is regarded as one of the most influential as it founded the modern right to privacy in the United States. [85] However, no express right to privacy exists in the United States. The right to privacy is not a fundamental right in the United States as the legal concept of 'privacy' is lacking in the American constitutional documents.[86] The term privacy does not appear either in the U.S. Constitution or in the Bill of Rights. However, the Supreme Court has held, in significant decisions[87], that an inherent right to privacy does exist, deriving from the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments to the Constitution.[88]

---

[82] Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.
[83] Ibid.
[84] Ibid.
[85] Michael C. James, 'A comparative analysis of the Right to Privacy in the United States, Canada and Europe' (2014) 29(2) Connecticut Journal of International Law 257, 264.
[86] Senator D. Brent Waltz, 'Privacy in the digital age' (2014) 48(1) Indiana Law review 205, 205.
[87] See for example Whalen v. Roe,429 U.S. Reports (22 February 1977), 589-604, in which the Supreme Court recognised the right to information privacy.
[88] Jean Slemmons Stratford and Juri Stratford, 'Data Protection and Privacy in the United States and Europe' (1980) 22 Iassist Quarterly 17, 17.

The United States and the European Union have traditionally had different conceptions of privacy. While the U.S. perceives privacy as an aspect of personal liberty, the European Union believes it is part of personal dignity.[89] In Europe, States are involved in protecting citizens' privacy whereas in the United States, individuals must protect their own privacy in order to promote personal liberty and free expression.[90] The U.S privacy laws constitutes a "patchwork', with an array of federal and state laws, regulations... leading to an heterogeneous application of privacy protection but we will further discuss this issue later in the chapter. [91] Finally, Europeans truly believe privacy to be a fundamental right whereas the Americans give prominence to freedom of expression. They allow almost no restrictions to the First Amendment, which preserves freedom of speech. [92]

2.2.2 Legal tools to protect privacy in the United States

2.2.2.1 The privacy Torts

The US has other current legal mechanisms different from the right to be forgotten, which aim to protect one's reputation or to control the information flow.[93] Privacy torts, which have been 'significantly restricted to protect free speech', are divided into four separate branches: intrusion upon seclusion, public disclosure of private facts, misappropriation and false light. Privacy torts as well as defamation enable to recover damages for invasion of privacy.

The tort of intrusion upon seclusion is defined in the Restatement of Torts, Second. Rodney A. Smolla specified that it protects an individual against the 'intentional invasion of solitude or seclusion of another through either physical or nonphysical means' including 'eavesdropping, peeping through windows of surreptitiously opening another's mail'. [94]

As described in the Restatement of Torts, Second, public disclosure of private facts is:

> *"one who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicised is of a kind that*
>
> *(a) Would be highly offensive to a reasonable person, and*

---

[89] James Q. Whitman, 'The two Western Cultures of Privacy : Dignity Versus Liberty' (2004) 113 Yale L. J. 1151, 1161.
[90] Steven C. Bennett (n 69)168-169.
[91] See pages 26-27.
[92] Steven C. Bennett (n 69)168-169.
[93] Meg Leta Ambrose and Jef Ausloos (n 35) 8.
[94] Rodney A. Smolla, Smolla and Nimmer on Freedom of Speech (Clark Boardman Callaghan 2010) § 24 :1.

(b) Is not of legitimate concern to the public."[95]

This tort has been very criticised, due to its inherent conflicts with the Freedom of expression, protected by the First Amendment. In theory, a newspaper is liable for the public disclosure of fact if it publishes a compromising, but true fact about an individual.[96] This raises the question of whether the media has protection under the First Amendment to disseminate this private information. Generally, 'many Courts provide media with the extraordinarily broad newsworthiness defence, leaving the public disclosure tort effectively impotent'. [97] This privilege given to newsworthy public disclosures of private true facts is undeniably contradictory to the right to be forgotten. Newsworthiness as a defence to privacy claims is still very common, for instance it was used in the case *Martin v. Hearst Corp. in* January 2015[98]. In the latter, the Court of Appeals for the Second Circuit reaffirmed its view on the traditional opposition between journalism and the right to be forgotten. The claimant, Lorraine Martin, was arrested in 2010 for drug offences. Local media outlets reported accurately the arrest and the charges of which Martin was accused. The plaintiff sued the publishers for 'libel and related claims' maintaining that it became false and defamatory to publish her arrest once the charges against her were nulled and all records of her arrest erased pursuant to Connecticut's Criminal Records Erasure State.[99] The problem in this case is whether the plaintiff can arraign the publishers of news accounts of her arrest on the ground that those publications are now false and misleading.[100] The Court of Appeals upheld the District Court's decision and found that the Erasure Statute 'does not render tortious historically accurate news accounts of an arrest' because the news report were factually true.[101] The Court of Appeal's position in this recent case shows that the public's right to information prevails over the protection of Martin's reputation.

One may also be prosecuted for misappropriation in case of 'appropriat[ion] to his own use or benefit the name or likeliness of another'.[102] In other words, this cause of action provides a remedy against the use of another person's name or likeliness for exploitative purposes and

---

[95] American Law Institute, Restatement of Torts, Second, §652 D (1977).
[96] Geoff Dendy, 'The Newsworthiness Defense to the Public Disclosure Tort' (1996) 85 KY. L. J 147, 148.
[97] Ibid.
[98] *Martin v. Hearst Corp.* (2nd Cir. 28 January 2015), 1.
[99] *Martin v. Hearst Corp.* (2nd Cir. 28 January 2015), 2
[100] Eugene Volokh, 'Statute allowing erasure of arrest record doesn't require newspapers to erase news stories' *The Washington Post* (28 January 2015).
[101] *Martin v. Hearst Corp.* (2nd Cir. 28 Janurary 2015), 16.
[102] American Law Institute, Restatement (Second) of Torts § 652 (c) (1977).

without the owner's permission. [103] Finally, a claim for publicity placing a person in a false light can be brought if the respondent publishes a matter which places a person in a highly offensive light and which is not of legitimate concern to the public.[104] This tort is once again threatened by the newsworthiness exception. The Martin's case[105], previously explained, could also fit into the false light tort.

We can observe that some torts are quite close to the right to be forgotten. For example, the torts of public disclosure of private facts or false light constitute causes of action to protect one's privacy and reputation. However, the right to be forgotten is very different from the privacy torts, as it does not address the same type of personal data. The one relative to the right to be forgotten is not necessarily illegal or undesirable when initially published or posted online. On the contrary, the privacy torts protect false or undisclosed information. The main difference between the two types of information is time.[106] 'The right to oblivion addresses information that may be out-dated, irrelevant, harmful, and/or inaccurate.[107] Over time, personal information might become embarrassing; privacy torts would be irrelevant in this case as they provide an immediate cause of action when data is published or posted; the right to be forgotten would be more appropriate.

Furthermore, the privacy torts have been undeniably restricted by several limitations such as the newsworthiness defence as we have seen in the Martin case. Therefore, it seems that the constitutional right to free speech prevails over privacy torts.

2.2.2.2 Copyright

Copyright may, under certain conditions, enable an individual to control a content he created. For instance, it is unlawful to post online copyrighted material, such as photographs, without the authorisation of the copyright's owner. The photographer would have a copyright cause of action in that case. However, a work must comply with several requirements in order to be subject to copyright. Firstly, a criterion of originality is required for literary, dramatic, musical or artistic works. Moreover, copyright protection cannot be afforded for works that

[103] Meg Leta Ambrose and Jef Ausloos (n 35) 8.
[104] American Law Institute, Restatement of Torts, Second, §652 E (1977).
[105] *Martin v. Hearst Corp.* (2nd Cir. 28 Janurary 2015).
[106] Meg Leta Ambrose, 'It's about time : Privacy, Information Life cycles, and the Right to Be Forgotten' (2013) 16(2) STAN. TECH. L. REV 369, 376.
[107] Ibid 376.

are trivial or insignificant (principle *de minimis non curat lex*). Finally, the idea must be expressed in a tangible form in order to be protected. According to Eugene Volock, 'an intellectual property right in information is the right to exclude others from communicating the information – a right to stop the others from speaking'.[108] As copyright aims to protect the author's expression and not the author's idea, 'speech that borrows creative expression is restrictable but speech that borrows only facts remains free'. [109]

Another limit to the author's exclusive rights is the fair use defence. The latter is defined in the article 17 U.S Code § 107: 'The fair use of a copyrighted work (...) for purposes such as criticism, comment, news reporting, teaching (...), scholarship, or research is not an infringement of copyright'.[110] To determine whether the use of a work is a fair use, the factors to consider are the following: 'the purpose and character of the use', 'the nature of the copyrighted work', 'the amount and substantiality of the portion used in relation to the copyrighted work as a whole' and 'the effect of the use upon the potential market for or value of the copyrighted work'.[111] Therefore fair use may protect copyrighted data. In that way, this kind of defence may reduce the tensions existing between copyright and free speech.[112]

Finally, a last limit is that protection of data by copyright cannot extend to content created by someone else than the information subject.[113] For example, the case about Nikki Catsouras raises the question on an individual's privacy following his death. In 2006, two employees of the California Highway Patrol illegally transmitted to the public horrific photos of the body of Nikki Catsouras's body, killed in a car accident in Orange County. The young girl's parents sued the California Highway Patrol for violation of privacy, negligence and infliction of emotional distress.[114] Yet their struggle to remove the photos was unsuccessful since the pictures did not belong to them. Clearly, copyright is ineffective in these circumstances; the subject's relatives, namely the Catsouras' family could not prevent the circulation of these morbid photos on the Internet. The implementation of the right to be forgotten in the United

---

[108] Eugene Volokh, 'Freedom of speech, information privacy, and the troubling implications of a right to stop people from speaking about you' (2000) 52 STAN. L. REVIEW 1, 15.
[109] Ibid.
[110] 17 U. S. C. § 107.
[111] 17 U. S. C. § 107.
[112] Giovanna Giampa, 'Americans Have a Right to Be Forgotten' (Law School Student Scholarship, Seton Hall University 2016), 17.
[113] Meg Leta Ambrose and Jef Ausloos (n 35) 8.
[114] Greg Hardesty, 'CHP dispatcher says suit over crash photos is misguided' (The Orange County Register, 23 January 2008) http://www.ocregister.com/articles/nikki-179866-catsouras-chp.html accessed 17 July 2016.

States is in this case essential to provide means for the parents to force Internet providers to erase the links giving access to the photographs.[115]

2.2.2.3 The U.S Data Protection Laws

Concerning the data protection laws, the United States does not have a uniform and coherent federal legal system of data and privacy protection. No single law provides a comprehensive treatment of data protection contrary to Europe where privacy protection is addressed by omnibus legislation such as the EU Data Protection Directive. Nevertheless, several laws deal with a particular aspect of data protection. The Privacy Act of 1974 and the Computer Matching and Privacy Protection Act of 1988 govern the collection, maintenance, use and dissemination of personal information held by the federal government. Therefore these types of laws do not have any authority over the treatment of personal information in the hands of other private and public sector entities, contrary to Europe where both sectors are regulated in the same way.[116] Additional to those acts, other privacy and data laws apply narrowly to specific types of personal information. For instance, 42 U.S.C. 242m protects private data collected by the National Centres for Health Services Research and for Health Statistics. A lot of them deal with the treatment of personal financial information, such as the Fair Credit Reporting Act. Finally, several laws were enacted in response to distinct abuses. The Video Privacy Protection Act of 1988 aims to prohibit the disclosure of video rental records containing private data.[117]

Therefore, the American system of privacy protection is divided into a variety of state and federal laws, regulations or guidelines developed by governmental agencies. Each one deals with a specific category of information such as health, financial, telemarketing, commercial information. They apply in a particular field and there is an imbalance between legislation governing the treatment of personal information held by the federal government and information held by other sources.[118] This consequently leads to an incoherent and heterogeneous system with differences from state to state, field to field. Moreover, several laws may overlap or contradict themselves. All these weaknesses of the system raise a concern on its efficacy to protect people's privacy.

---

[115] Jeffrey Toobin, 'The Solace of Oblivion' *The New Yorker* (29 September 2014).
[116] Jean Slemmons Stratford and Juri Stratford, 'Data Protection and Privacy in the United States and Europe' (1980) 22 Iassist Quarterly 17, 18-19.
[117] Ibid.
[118] Ieuan Jolly, 'Data Protection laws in the United States : overview' (*Practical Law*, 1 July 2016) <http://us.practicallaw.com/6-502-0467#a762707> accessed 19 July 2016.

2.3 Main obstacles to the implementation of a European-style right to be forgotten in the United-States

2.3.1 The First Amendment

The major question addressed here is whether the right to be forgotten can coexist with the constitutional provisions of freedom of speech and press, particularly contained in the First Amendment. The latter states: 'Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances'.[119]

The value of the free press is very important in the United States and it is generally protected when privacy rights conflict with newsgathering. The media is expected to reveal the truth about people and not only about government and public affairs.[120] Moreover, US law on freedom of expression is very permissive. Contrary to French law, the First Amendment protects even hate speech[121]. The major full restrictions to the freedom of speech concern obscenity, child pornography, and 'fighting words' associated with true threats.[122]

Undeniably, one person's right to be forgotten can interfere with others' rights of freedom of expression. Some regard the right to be forgotten as the 'biggest threat to free speech on the Internet in the coming decade'[123]. To examine whether the right to be forgotten violates the freedom of expression and more broadly, the First Amendment, we must question who are the actors implicated by the right to be forgotten? The primary groups involved are the subjects of data collected online and posted, the creators of the content, such as pictures on Facebook, videos on Youtube, blog posts etc and finally third-party websites, mainly search engines that display or link to information created by others.[124] The question arises whether granting data subjects the right to have personal information deleted from the Internet infringes the rights of either content creators or third-party websites protected by the First Amendment? For

[119] Constitution of the United States, Amendment 1.
[120] Robert Kirk Walker, 'The Right to Be Forgotten (2012-2013) 64(1) Hastings Law Journal 257, 274.
[121] Eugene Volokh, 'No, there's no « hate speech » exception to the First Amendment', *The Washington Post* (Washington, 7 May 2015).
[122] Kathleen Ann Ruane, 'Freedom of Speech and Press : Exceptions to the First Amendment' (2014) Congressional Research Service, 1-4.
[123] Jeffrey Rosen, 'Symposium Issue : The Right to Be Forgotten' (2012) 64 Stan L Rev 88, 88.
[124] Robert Kirk Walker, 'The Right to Be Forgotten (2012-2013) 64(1) Hastings Law Journal 257, 274.

instance, a photographer has a constitutional right to take photographs and to present his work to the public, through his website. However, the photographs also convey information related to the person photographed. Pictures are part of the scope of data protected by the right to be forgotten: 'any information relating to a data subject'.[125] In the United-States, in most cases, the speech rights of the creators and third-party websites trump the privacy rights of the subjects data.[126]

However, we might also ask ourselves: Can the right to be forgotten foster freedom of expression? Indeed, the right to be forgotten offers the possibility to the individuals to express themselves freely without fear that what they say or write at one point in their lives will be kept forever in someone's archives and may be used against them in the future.[127]

2.3.2 The Communications Decency Act

A second element of relevance is the Communications Decency Act, which represents another obstacle to the implementation of the right to be forgotten in the United States. Congress passed the Communications Decency Act in 1996 to regulate the problems surrounding indecency and obscenity in cyberspace. Therefore the initial purpose of the Communications Decency Act was to restrict free speech on the Internet. However, following a strong objection of the Internet Community, the Supreme Court held that several provisions of the act were unconstitutional because they infringed the First Amendment.[128] One of the survival provisions is section 230, which grants immunity to Internet service providers from being held liable for the content posted on the websites. [129] CDA 230 creates a broad protection for any online service that publishes third-party content.

Several conclusions emerge from this chapter. The evidence highlights that the U.S. legal framework does contain the concept of a right to be forgotten. The principle of legal oblivion already exists in different fields. A first step of a digital right to be forgotten has come to light in California although it is very limited as it does not apply to content created by third-parties.

---

[125] European Commission, Proposal for a Regulation of the European Parliament and of the Council', art 4(2) (25 January 2012).
[126] Robert Kirk Walker (n 125) 274.
[127] Mike Wagner and Yun Li-Reilly, 'The Right to be Forgotten' (2014) 72(6) The Advocate 823, 830.
[128] Paul Ehrlich, 'Communications Decency Act 230' (2002) 17(1) Berkeley Technology Law Journal 401, 401.
[129] 47 U. S. C § 230.

Therefore, there is no digital right to be forgotten similar to the European one in the U.S and there are several hurdles to its implementation. Firstly, the United-States has a very different conception of privacy compared to Europe and freedom of speech prevails over it in most cases. Secondly, there is no generic privacy legislation in the United-States and data protection in the private sector is largely self-regulatory. Furthermore, privacy torts seem out-dated and irrelevant to the right to be forgotten as they address a different type of information. Finally, the First Amendment is fundamental and very few exceptions are permitted.
Nowadays, U.S. Courts generally reject claims regarding privacy, especially when the media are involved. The Communications Decency Act also represents an important hurdle to the development of the right to be forgotten in the United-States. To implement it, there is a need to balance rights to privacy with freedom of expression. Moreover, changes must be realised at the legislative level. Though the US government and the US Courts are the decision makers, citizens and companies will need to endorse the potential changes in order for the right to be forgotten to become effective.

Later in the thesis, in the discussion section, it will be interesting to determine whether the European Union can exercise a certain pressure to persuade the United-States to adopt the European approach of the Right to be forgotten or if there is a major intercontinental clash.

Chapter 3. Evolution of the European Legislation on the Right to be Forgotten

The right to be forgotten cannot amount to a mere theoretical issue: rather it is a legal concept, characterised by laws and regulations governing its implementation, as well as case law which is developing in favour of the legal recognition of this principle. This chapter, divided into three parts, will present in chronological order the European legislation on the right to be forgotten. Part one will offer an overview of the legal background, which evolved in line with the developments of technology. Part two will focus on the famous Google Spain ruling and will examine its direct implications on the search engines. Lastly, part three will consider the General Data Protection Regulation and will show that the right to be forgotten is part of a more ambitious project within the Digital Single Market.

3.1 Legal foundations and background of the Right to be Forgotten

3.1.1 The progressive development of an implicit right to be forgotten

Europe has known a lot of privacy regulations. We can mention several of them, which contributed to the process leading to the emergence of the right to be forgotten.[130]
Article 8 of the European Convention on Human Rights[131] introduced an explicit right to respect for private and family life. Article 7 of the Charter of Fundamental Rights of the European Union guarantees, as well, the respect for private and family life.[132] Moreover, Article 8 of the Charter explicitly established the protection of personal data.[133] Additionally, Convention 108 of the Council of Europe[134] specifically protected the automatic processing of personal data.

For several years, EU laws on the protection of personal data remained unchanged while new technologies evolved considerably. The law found itself overwhelmed by the technology, which has a major impact on the treatment and security of personal data. The Directive (EU) No 95/46 on the protection of individuals with regard to the processing of personal data and

[130] Meg Leta Ambrose and Jef Ausloos (n 35) 6.
[131] Convention for the Protection of Human Rights and Fundamental Freedoms [1950].
[132] Charter of Fundamental Rights of the European Union [2000] OJ 364/1, article 7.
[133] Ibid article 8.
[134] Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, No. 108, Jan. 28, 1981.

on the free movement of such data (The Data Protection Directive)[135] was written with the aim of adapting the European Union framework to the technological challenges. Therefore, the 95/46/EC Directive represents a milestone in the evolution of data protection in the European Union and shows the will to harmonise European national laws.[136] A general and explicit right to be forgotten is not mentioned in the DP Directive. However, some provisions can be interpreted as very close to the right to be forgotten.[137] For instance, article 6(1)(e) of the Data Protection Directive declares that personal data can be kept 'for no longer than is necessary for the purposes for which the data were collected or for which they are further processed'. This provision does not require the user to do any action, as the data must be automatically removed once the purpose is fulfilled. This can be considered as a form of a right to be forgotten, but more in a passive way.[138]

Besides, several articles in the 95/46/EC Directive deal with consent. Consent is of particular importance in data protection. Indeed, it gives control to the data subject with regard to the processing of his data. Consent is necessary to ensure the individual autonomy and self-determination.

The consent of the data subject is defined in Article 2(h) and then used in Articles 7, 8 and 26 of the 95/46/EC Directive. The Article 29 data Protection Working Party (29 WP), as part of its work programme for 2010-2011, defined precisely what constituted a valid consent and provided guidelines on its requirements in its Opinion 15/2011 on the Definition of Consent.[139]

Pursuant to Article 2(h), the '*data subject consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*'.[140] Several elements in this article were clarified by the 29 WP:

The fragment '*...any... indication of his wishes...signifying...*' means that there must be a clear indication of the data subject's wishes for the consent to be valid. The indication must

---

[135] Directive (EU) No 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

[136] Peter Hustinx, 'EU Data Protection Law : The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (2014) EUR. DATA PROTECTION SUPERVISOR.

[137] Meg Leta Ambrose and Jef Ausloos (n 35) 7.

[138] Aidan Forde, 'Implications of the Right to Be Forgotten' (2015) 18 Tul. J. Tech. & Intell. Prop 83, 93.

[139] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent' WP187, 13 July 2011.

[140] Directive (EU) No 95/46 n (136) art 2(h).

be understandable by the data controller. [141]

The expression *'...Freely given...'* means that consent must result from a choice. The data subject must not fear any risk of deception, intimidation or negative consequences if he refused to give his consent.[142]

The term *'specific'* means that blanket consent is not acceptable. The consent must be intelligible and should refer clearly to the scope and implications of the data processing. Therefore consent must be applied to a limited context.[143]

The term *'informed'* means that appropriate information must be given before the consent is asked. The type of information that must imperatively be provided to individuals is listed in Articles 10 and 11 of the Directive. The quality, accessibility and visibility of information are crucial for this requirement to be satisfied.[144]

Article 7(a) of the Directive indicates that consent is one of the six legal grounds to process personal data. Moreover, the individual's consent must be *'unambiguous consent'*.[145] It means that the procedure to obtain consent must leave no doubt as the data subject's intention to provide consent. Different types of mechanisms may be used to seek consent for data other than sensitive data. Express consent is not necessarily required for this type of data. However, an individual's inaction or silence may not represent a valid consent, especially in the online environment.[146]

Article 8.2(a) deals with data of a sensitive nature. *'Explicit consent'* is required to process sensitive data.[147] This requirement means that the data subject must give an active response, oral or in writing whereby he agrees to have his data process for specific purposes. Therefore, a pre-ticked box (opt-out) is not considered as an explicit consent as a positive action is

---

[141] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent' WP187, 13 July 2011.
[142] Ibid.
[143] Ibid.
[144] Ibid.
[145] Directive (EU) No 95/46 n (136) art 7(a).
[146] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent' WP187, 13 July 2011.
[147] Directive (EU) No 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31, art 8.2(a).

required from the data subject to signify his consent.[148]

Article 26.1 (a) requested an *'unambiguous'* consent to transfer data to third countries which do *'not ensure an adequate level of protection'*.[149]

Finally, it is worth questioning how consent may be obtained from individuals lacking full legal capacity, including children. The 29 WP specified that the 95/46/EC Directive did not provide particular rules and that the conditions vary from Member State to Member State. Therefore, the 29 WP underlines the need to harmonise the rules and especially clarify the circumstances in which consent of an incapable individual should be obtained from parents or representatives.[150]

Regarding the right to be forgotten, Article 12(b) and Article 14 were the most relevant. The former provides that each data subject has the right to 'obtain from the controller... the rectification, erasure or blocking of data'.[151] However its scope of application is limited as it only applies 'when the processing does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data'. Article 14 provides that the data subject has a right to object to data processing but this provision is also limited in scope. It only applies to matters relating to articles 7(e) and (f) and if such are based on 'compelling and legitimate grounds'. [152] However, pursuant to article 14, the individual always has a right to object without having to provide any explanation if the data is used for marketing purposes or will be disclosed to third parties.

However, the 95 Directive was not sufficiently effective as it had been subject to varied national transpositions. This multitude of transpositions created disparities between the states in terms of personal data processing. Indeed it was found that some countries' procedures of the European Union were more flexible than others.

The enactment of new Directives such as the E-Commerce Directive[153] in 2000 or the E-Privacy Directive[154] in 2002 aimed to solve problems appearing with the development of new

[148] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent' WP187, 13 July 2011.
[149] Directive (EU) No 95/46 (n 136) article 26.1(a).
[150] Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent' WP187, 13 July 2011.
[151] Directive (EU) No 95/46 (n 136) article 12(b).
[152] Aidan Forde (n139) 94.
[153] Directive (EU) No 2000/31 on certain aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178. (Directive on electronic commerce)

activities on Internet. The former harmonised rules on issues relating to online service providers, commercial communications, and electronic contracts. The latter intends to protect the right to privacy and confidentiality, regarding the processing of personal data in the electronic communications sector and the free movement of such data and equipment and electronic communications services in the European Union. However, there were still some aspects not covered by these Directives' provisions and EU data protection legislation still seemed inadequate to the new challenges societies had to face, especially with the advent of smartphones and the omnipresent Internet. Therefore the existing framework soon proved to be 'unable to represent the realities of a world in which data has become a primary currency exchanged between consumers, businesses and organisations'.[155]

In 2010, the European Commission clarified the Right to Be Forgotten for the first time 'in a communication proposing a comprehensive approach on personal data protection in the European Union'. It was defined as 'the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes'.[156]
In 2012, the European Union enacted the proposed Data Protection Regulation[157], which was intended to harmonise the data protection rules across the European Union. It represents a fundamental modernisation of the data protection rules in EU. In Article 17 of the proposed Regulation, the general principle relating to the Right to be Forgotten was established and updated to for the digital age.[158]

---

[154] Directive (EU) No 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L 201 (Directive on privacy and electronic communications).
[155] Chris Combemale, 'New data protection regulation should reflect marketing needs' *The Guardian.com* (2012) < https://www.theguardian.com/media-network/media-network-blog/2012/sep/24/data-protection-regulation-marketing-law> accessed 26 July 2016.
[156] European Commission, Communication on personal data protection in the European Union, COM(2010)609, 4 November 2010.
[157] European Commission, Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such Data, COM (2012) 11 final, 25 January 2012.
[158] European Commission, Factsheet on the « Right to be Forgotten » ruling (C-131/12) ec.europa.eu > http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf> accessed 26 July 2016.

3.1. 2 The Google Spain Case[159]: the formal recognition of the right to be forgotten

- **Facts**

In 2011, a Spanish man Mario Costeja Gonzáles lodged a complaint with the Spanish Data Protection Agency against the publisher of a daily newspaper, *La Vanguardia Editiones,* and against Google Spain and Google Inc. His complaint concerned the fact that a Google search of his name resulted in links to two pages of *la Vanguardia's* newspaper. Those pages contained notification of an auction of real estate to recover social security debts owned by Mr. Gonzáles. He did not want to be associated with his 90s misfortune any longer. Therefore he requested the *Agencia Española de Protección de Datos (*AEDP) to order *La Vanguardia* to remove or alter the pages in question and order Google Spain and Google Inc. to remove or conceal personal data relating to him so that it would no longer appeared in search results. Mr. Gonzáles maintained that the proceedings in question had been fully resolved for a number of years and that reference to them had become entirely irrelevant.

The AEDP dismissed the complaint against the newspaper, arguing that the publication of the information was legally justified as it had been ordered by the Ministry of Labour and Social Affairs and aimed to give publicity to the auction.

However, the complaint against Google Spain and Google Inc. was upheld and the Spanish Agency ordered them to withdraw the data and deny access to it in the future. The companies took the matter to Spain's National High Court to have that decision annulled. A series of difficult questions were raised regarding the obligations of the operators of search engines to protect personal information linked to individuals who do not want them to be available to Internet users indefinitely. The Spanish National High Court decided to request the help of the Court of Justice of the European Union for a preliminary ruling.

- **Significant decision of the Court of Justice of the European Union**

The questions concerned the interpretation and application of European Union law and especially the meaning of Directive 95/46/EC on the protection of individuals with regard to

[159] Google Spain Costeja (n 2).

the processing of personal data and on the free movement of data. [160] Firstly, the material scope of the Directive 95/46 had to be interpreted. Does the activity of a search engine qualify as 'processing of personal data' pursuant to Article 2(b) of the Directive? Is the operator of a search engine classified as the controller of the processing of personal data within the meaning of Article 2(d)? [161] Moreover, the referring Court raised questions relating to the territorial scope of Directive 95/46. Is it possible to apply the Spanish legislation, transposing Directive 95/46, in this case?[162] The Court then considered the extent of the responsibility of the operator of a search engine under the same Directive. Should Article 12(b) and Article 14(1)(a) be interpreting as meaning that the operator of a search engine is compelled to remove links to web pages, which contain personal data relating to a person? Does this obligation exist even when the web page is lawful?[163] Finally, the Court considered the scope of the data subject's rights guaranteed by Directive 95/46. More precisely, the Court dealt with the so-called 'right to be forgotten'. Can Article 12(b) and Article 14(1) be interpreted as permitting the data subject to request the operator of a search engine to remove his private data from the list of results, on the grounds that that information may be harmful to him or that he wishes this information to be 'forgotten' after a certain time? [164]

To summarise the judgement, the European Court of Justice held that Google "processed" personal information and offers the possibility to any Internet user, when searching on the basis of a person's name, to obtain private information about him on the Internet. Moreover, the information about Mr. Gonzáles concerned aspects of his private life that could not have been interconnected, or could only have been found with high difficulty, without the search engine. In addition, the Court recognised that even the processing of accurate data, which is lawful at the time, may in the course of time become incompatible with the law.[165] Therefore the Court declared that Google should be held responsible for the obligations and guarantees enshrined in Directive 95/46/EC. Therefore, the Court held that search engine providers have an obligation, in certain circumstances, to remove links to personal information that are 'inadequate, irrelevant or excessive in relation to the purposes of the processing… not kept up to date, or… kept for longer than is necessary.' [166] This case is fundamental because the Court

---

[160] Directive 95/46/EC (n 136)
[161] Herke Kranenborg, 'Google and the Right to Be Forgotten' (2015) 1 EDPL 70, 71.
[162] Ibid 71.
[163] Ibid 72.
[164] Ibid 73.
[165] Mike Wagner and Yun Li-Reilly, 'The Right to be Forgotten' (2014) 72(6) The Advocate 823, 824-825.
[166] Michael Douglas, 'Questioning the Right to Be Forgotten' (2015) 40(2) Alternative Law Journal 109, 109.

affirmed that users of search engines have a right to be forgotten in light of the Directive 95/46. On the territorial scope of the Directive, the Court asserted that Google Spain was an 'establishment', as described in the Directive, of Google Inc. The Court highlighted that pursuant to Article 4(1)(a) of Directive 95/46, the processing of personal data does not require to be carried out by the establishment concerned itself but only 'in the context of the activities' of the establishment. [167]

These decision had a global impact as it was held that EU laws apply extraterritorially and that search engines such as Yahoo, Google, Bing must respect data protection laws as long as they are involved in Europe activities that are connected to their main array of activities, namely processing of data. The right to be forgotten was explicitly recognised in this decision. Indeed, when the Spanish Supreme Court referred to the European Court of Justice, the right to be forgotten was not completely new but at an embryonic stage. In addition, The Court held that privacy rights should prevail over the economic interests of the operator of the search engine but also over the interests of the public. [168] The outcome of the Court's decision was very controversial and entailed a lot of critics[169] and fear of its implications.

The Court of Justice limited the scope of the right to be forgotten to persons only, that is to say that a removal request form cannot be used by either a brand's name of a company's name. Moreover, search engines will consider a removal request from someone in the public eye differently as the right to information is more important when dealing with this type of person.

- **Implications of the CJEU ruling**

The CJEU ruling recognised formally the right to be forgotten. Therefore, it was impossible for the European jurisdictions to deny it anymore. Moreover, new standards of data protection were imposed. It forced Google and other search engines to comply with the judgement and to establish a special procedure in order to enable European users to request the delisting of certain results related to personal information about them. Therefore, search engines had to

[167] Herke Kranenborg (n 72).
[168] Mike Wagner and Yun Li-Reilly, 'The Right to be Forgotten' (2014) 72(6) The Advocate 823, 825.
[169] Jeffrey Rosen is strongly opposed to the right to be forgotten. See for example : 'The Deciders : The Future of Privacy and Free Speech in the Age of Facebook and Google'(2012) 80(4) Fordham Law Review 1525; 'The Web Means the End of Forgetting' *The New York Times* (New York, 21 July 2010) ; 'The Right to Be Forgotten' (2012) 64 Stanford Law Review Online 88.

put a delisting form online to comply with the decision of the Court. For instance, Google launched its official request process on 29 May 2014.[170] Google is maintaining an updating list of the requests taken from removal in its Transparency Report. Today, more than 490,000 removal requests have already been submitted to Google.[171] On all the URL address that Google has evaluated for removal, more than half of them (57%) have not been removed. [172] The nature of the websites most impacted by the right to be forgotten will be examined in detail later in the discussion section.[173]

It is interesting to highlight that, since this Google Spain ruling two years ago, delisting requests are becoming increasingly frequent and each EU national Court is facing right to be forgotten cases. In May 2016, a landmark ruling on the right to be forgotten came before the Irish Courts. There a politician, Mark Savage, initiated a request to Google to remove a link to a Reddit post which, he claimed, brands him wrongly as homophobic. His initial request was rejected by the search engine. Mark Savage appealed against Google's refusal to the Data Protection Commissioner but this claim was also unsuccessful. The Data Protection Commissioner Helen Dixon argued that in this case the public interest and freedom of expression guaranteed under the Constitution trumped the right to privacy.[174] The politician sought judicial orders from Dublin Circuit Court against the Data Protection Commissioner and Google Ireland. The judgement has been reserved but the outcome will be of interest as it the first right to be forgotten case in Ireland [175]

Any personal information is not however legitimately capable of delisting, the right to be forgotten is facing freedom of expression and the right to information. How to balance between these rights? The risk is to give Google the role of judge and party in the processing of applications for dereferencing. To avoid abuses, it was necessary that the Article 29 Working Party (Art. 29 WP), an independent European advisory on data protection and privacy, bring some clarification. Its organisation and tasks are defined by Articles 29 and 30 of Directive 95/46/EC and by Article 14 of Directive 97/66 / EC. Art. 29 WP played an

[170] 'European privacy requests for search removals' – Transparency report (Google, 13 June 2016) <https://www.google.com/transparencyreport/removals/europeprivacy/> accessed 13 June 2016.
[171] 'Ibid.
[172] Ibid
[173] See page 49.
[174] Saurya Cherfi, 'Politician brings landmark « right to be forgotten » case against Google after being branded homophobe online' The *Irish Independent* (Dublin, 4 May 2016).
[175] 'First « right to be forgotten case comes before Irish Court' *Irish Legal News* (5 May 2016).

important role in the implementation of the Right to Be Forgotten.[176] Indeed, in November 2014, the G29 developed guidelines[177] for the implementation of the right to delisting, to harmonise the settlement of disputes between the search engines to those who requested the data removal on these engines. The G29 has developed a common interpretation of the judgment and common criteria for the investigation of complaints.

In order to reconcile the right to delisting and the right to information and freedom of expression, the right to be forgotten is surrounded by safeguards to preserve a balance between the rights and freedoms weighed: the right to delisting is not an absolute right. Each request must be assessed on a case-by-case basis, *in concreto* and is not automatic. In addition, the delisting does not necessarily lead to the removal of the content. The content subject to the removal request thus remains available on the website and can be located on the basis of different keywords. In practice, only those with a clear and definite link with the European Union, citizen or resident of a EU member country are intended to make use of this right. However, the content being accessible from any country, that right must be global: the delisting should be effective on all extensions of a domain name, European or not.

3.3 Adoption of the data protection reform: the reinforcement of the right to be forgotten

This reform of EU data protection rules, consists of two elements: the General Data Protection Regulation and the Data Protection Directive for the police and criminal justice sector, is part of the implementation of the Digital Single Market Strategy.

On 15 December 2015, after years of complicated negotiations, the European Parliament, the Council and the Commission finally reached an agreement on the new data protection rules. In April 2016, the General Data Protection Regulation[178] was adopted by the Council and the

[176] European Commission, 'Article 29 Working Party' (ec.europa.eu, 6 October 2015) http://ec.europa.eu/justice/data-protection/article-29/index_en.htm accessed 25 July.
Article 29 Data Protection Working Party, Guidelines on the implementation of the CJEU judgment on « Google Spain and Inc v. Agencia espanola de proteccion de datos (AEDP) and Mario Costeja Gonzales », WP 225, 26 November 2014.

[177] Article 29 Data Protection Working Party, Guidelines on the implementation of the CJEU judgment on « Google Spain and Inc v. Agencia espanola de proteccion de datos (AEDP) and Mario Costeja Gonzales », WP 225, 26 November 2014.

[178] Regulation (EU) No 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[2016] OJ L119/1.

European Parliament entered into force in 2016 and shall apply in May 2018 in all member states of the European Union. It is interesting to note that a Regulation must be implemented in its entirety, throughout the European Union, contrary to the directive. Indeed the latter sets goals for all EU countries but each country is free to develop its own measures to achieve them and to transpose the directive into its national law.

The General Data Protection Regulation updates and modernises the principles of the 1995 Directive on data protection. It brings changes for citizens, businesses and data protection authorities. It strengthens existing rights of the citizens and allows them to have more information on the processing of their data. The right to be forgotten is reinforced as it is explicitly provided by article 17. A new right, the right to portability is created. Minors are also subject to a specific protection. The Regulation simplifies procedures for businesses, gives them the possibility to have one single interlocutor representing all data protection authorities and provides them with a toolbox of compliance (for example code of conduct, certification). The obligations of the controller are also listed. They must provide transparent and easily accessible information to data subjects about the processing of data concerning them.[179]

The Regulation affirms and strengthens the skills of the data protection authorities, especially repressive powers with the ability to impose administrative penalties of up to 4 percent of their turnover of the company concerned. The European Data Protection Authorities will have the competence to make joint decisions. This new cooperation between protection authorities will be accompanied by a new independent European body, the European Committee for Data Protection Supervisor (EDPS) to arbitrate disputes between the authorities. This entity, which will take over the G29, will be able to hear and investigate complaints, monitor and ensure that the Data Protection rules are applied by EU institutions. [180]

The Data Protection Directive[181] for the police and criminal justice sector was also adopted in April 2016, will entered into force in May 2016 and be applied in May 2018. It protects data

[179] Council of the European Union, 'The general data protection regulation' (consilium.europa.eu, 27 May 2016) <http://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-regulation/> accessed 21 June 2016.

[180] 'European Data Protection supervisor' (ec.europa.eu) <http://ec.europa.eu/justice/dataprotection/bodies/supervisor/index_en.htm> accessed 27 July 2016.

[181] Directive (EU) No 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of

regarding victims and suspects in the context of a criminal investigation and harmonise laws to facilitate cross-border cooperation to combat terrorism and crime more effectively. [182]

3.4 Data protection laws, including the right to be forgotten, necessary for the implementation of the EU Digital Single Market

The following quotation from the Vice President for the Digital Single Market summarises succinctly the goals of the EU Digital Single Market:

> *"Today's agreement is a major step towards a Digital Single Market. It will remove barriers and unlock opportunities. The digital future of Europe can only be built on trust. With solid common standards for data protection, people can be sure they are in control of their personal information. And they can enjoy all the services and opportunities of a Digital Single Market. We should not see privacy and data protection as holding back economic activities. They are, in fact, an essential competitive advantage. Today's agreement builds a strong basis to help Europe develop innovative digital services. Our next step is now to remove unjustified barriers, which limit cross-border data flow: local practice and sometimes national law, limiting storage and processing of certain data outside national territory. So let us move ahead and build an open and thriving data economy in the EU – based on the highest data protection standards and without unjustified barriers."*[183]

The President of the European Commission, Jean-Claude Juncker, has listed the strategy of the digital single market among the political priorities of his mandate. The EU digital single market aims to destroy the barriers Europeans are currently facing when they use online services and tools. Online markets remain national. Indeed, only 15% of citizens shop online from another EU country.[184] Therefore the strategy of the project is to 'create a free and

---

criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] L 119/89.

[182] 'EU Data Protection Reform, major step towards a digital single market' (Bmisystem, 18 January 2016) < http://www.bmi-system.com/eu-data-protection-reform-major-step-digital-single-market/> accessed 27 July 2016.

[183] European Commission, Press release 'Agreement on Commission's EU data protection reform will boost Digital Single Market', 15 December 2015.

[184] European Council, 'Digital Single market for Europe' (consilium.europa.eu) <http://www.consilium.europa.eu/en/policies/digital-single-market-strategy/> accessed 27 July 2016.

secure digital single market'.[185] The strategy is constituted of three main objectives: make it easier for people to shop online and businesses to across borders, improve the conditions for digital networks and expand the development of the European digital economy. [186] The new data protection rules in the EU are part of this second goal. The 'trust in digital services' handling of personal information and the improvement of cyber-security[187] are indispensable to build the digital single market.

A search engine is a high-powered computer tool capable in a few milliseconds to cross any type of globally collected information on the simple keystroke of the first and last name of a person. For a long time, no one had reacted to this flagrant violation of privacy laws, until the CJEU finally offered the following reasoning: Google performs daily processing of personal data within the meaning of the 95 European Directive. It is responsible for it and must comply with this directive as soon as the persons concerned are EU nationals, that the information is available within the Union and that Google, established in the EU, handle commerce over the Internet in the EU. Therefore, in the Google Spain ruling, the CJEU held on the territoriality of EU laws, on the applicability of EU data protection laws to a search engine and on the right to be forgotten.
The legal framework relative to privacy and data protection, which already existed before this famous ruling, represented a basis for the recognition of the right to be forgotten.

The Data Protection Regulation represents a very important reform of the EU data protection laws. It strengthens the rights of European citizens and gives them more control over their personal data. For instance, the obligation to collect a clear consent from the individuals for the proceeding of personal data is guaranteed. It defines the rights of individuals and defines the obligations of the people performing data processing and those who are responsible for this treatment. It simplifies the formalities for companies and offers them a unified legal framework. But above all, the new Regulation introduces formally and explicitly the right to be forgotten. The question that arises is whether this data protection Regulation will successfully manage to find the adequate balance between the interests of the different stakeholders involved.

[185] Ibid.
[186] Ibid.
[187] Ibid.

3.5 France's will to implement the right to be forgotten

Building on the idea that the CJEU guaranteed the right to be forgotten to the EU citizens through its decision of May 2014[188], this section seeks to underline that the CJEU did not 'create' a right unknown to European countries. For some of them, such as France, this milestone decision seemed to have been highly expected. The principle of the right to be forgotten is not new in France. For decades, France has been giving importance to it and in this regard may be considered as an anchor country in the implementation of the right to be forgotten. The first law dealing with this complex issue is the Data Protection Act of 6 January 1978[189]. For the first time, France recognised implicitly a right to be forgotten. In Article 6-5), the law specifies that the retention period may not exceed the duration necessary for the purposes for which the data were collected and processed. Moreover, Article 40 of the same Act provides that 'any individual providing proof of identity may ask the data controller to rectify, complete, update, block or delete personal data relating to them that are inaccurate, incomplete, equivocal, expired, or whose collection, usage, disclosure or retention is prohibited'.[190]

A number of initiatives and proposals to regulate the digital right to be forgotten have been made in France, with mixed success, but each one incontestably contributed to create a conducive framework to facilitate the landmark ruling of the CJEU in the Google Spain case.[191] Therefore this section will closely examine the main French initiatives in relation to the right to be forgotten as well as case law clearly aligning itself on the European Union's position.

3.5.1 The legislative proposal to regulate the digital right to be forgotten in France

Two senators, Anne-Marie Escoffier and Yves Détraigne, filed on the 6th of November 2009, a legislative proposal to "better ensure the right to privacy in the digital age"[192] and to transform the "*homo sapiens*" to "*homo numericus*", both "free and informed" about their

[188] *Google Spain Costeja* (n 2).
[189] Act n° 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties, available at <https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf>.
[190] Ibid.
[191] *Google Spain Costeja* (n 2).
[192] Legislative proposal No. 2387 passed by the Senate to better ensure the right to privacy in the digital age (Proposition de loi n°2387 adoptée par le Sénat visant à mieux garantir le droit à la vie privée à l'heure du numérique) [24 March 2010] available at http://www.assemblee-nationale.fr/13/pdf/propositions/pion2387.pdf.

personal information and the use that is made online. The text proposes thus mandating "a clear, accessible and specific information" towards users about the duration data retention, and the purpose of collecting their personal data (Articles 5 and 6). [193] The other key measure of this legislative proposal is to regulate the right to be forgotten on the Internet. Article 8 calls for "the easiest practice of the right to delete data" by making it free and feasible electronically. Article 13 of this proposal offers the ability to refer the matter more easily and efficiently to civil jurisdictions, particularly in case of impossibility for people to exercise their right to delete data. Finally, article 2 of the text intends to clarify the status of the IP address by viewing it as a personal data.[194]

3.5.2 The initiative of the French Data Protection Commissioner to include the right to be forgotten in the Constitution

In November 2009, Alex Türk, the former French Data Protection Commissioner, held a public debate demanding the inclusion of the right to be forgotten in the Constitution. The President of the National Commission for Data Protection and Liberties (CNIL) also declared that a law would not be enough: "It's a start, but it is essential to start negotiations on the issue between the United States and European Union to move towards a global device". [195] For Alex Türk, the challenge of the right to be forgotten is to "reproduce a natural function, forgetfulness, which makes life bearable."[196]

3.5.3 Towards a common charter to social networks and search engines

On the 13 of October 2010, a charter known as 'Code of Good Practice on the Right to be Forgotten on Social Networks and Search Engines'[197] was signed in Paris. The ten signatories actors[198] were collaborative sites (mainly social networks, blogs, and forums) and search

---

[193] Emilie Bulot, 'Gros plan sur le droit à l'oubli numérique' (*Anis*, March 2010) <http://www.anis.asso.fr/Gros-plan-sur-le-droit-a-l-oubli-numerique-2010.html> accessed 4 August 2016.
[194] 'Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique' (senat.fr, 2010) https://www.senat.fr/rap/l09-330/l09-3302.html accessed 4 August 2016.
[195] Emilie Bulot (N 194).
[196] Jean-Baptiste Chastand, 'La délicate question du droit à l'oubli sur Internet' *Le Monde* (Paris, 12 November 2009).
[197] Secrétariat d'Etat à la Prospective et au Développement de l'économie numérique, 'Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche' (13 October 2010).
[198] *Action innocence, Confédération nationale des associations familiales catholiques, E-enfance, Union nationale des associations familiales, Copains d'avant, Pages jaunes, Skyrock, trombi.com, Viadéo, Microsoft France (MSN, Windows live, Bing)*

engines.[199]

The main aim of this text, initiated by the former Secretary of State in charged of the Development of the Digital Economy, Nathalie Kosciusko-Morizet, was to give individuals control on their private data accessible on the Internet.[200] The signatories undertook to improve the transparency of the use of data published by the users on the Internet.[201] In addition, the users were able to delete or modify the data they published through a virtual "Complaint Desk" and delete their account easily. Finally, these websites had to ask users for the permission to transfer their data to third parties or to external applications (quizzes, games...). Finally, through this charter, the signatories search engines had to collaborate with publication websites to preserve the privacy of Internet users and facilitate the eventual non-indexation of certain contents.[202]

However this Charter suffers from two handicaps and therefore has a modest application. Firstly, the charter is non-binding nature, as it is a code of conduct to which we voluntarily subscribe. Thus it has a limited effect on the maintenance and protection of the rights provided. Secondly, Google and Facebook, two companies among the most concerned with data protection, abstained from signing.[203] Facebook, with 1.13 billion active users in 2016 on a daily basis[204], is the first social network in the world. Its importance in terms of right to oblivion is the nature, often very personal, of the data published by its users. Similarly, Google is the undisputed leader of search engines. Its market share in France rose to 93.37% over the year 2015.[205] Far behind, two other Americans, Bing and Yahoo, covered

---

[199] 'Charte du droit à l'oubli numérique : mieux protéger les données personnelles des internautes' (Portail du gouvernement, 18 October 2010) <http://archives.gouvernement.fr/fillon_version2/gouvernement/charte-du-droit-a-l-oubli-numerique-mieux-proteger-les-donnees-personnelles-des-interna.html> accessed 4 August 2016.

[200] Dimitri Seddiki, 'Premiers enseignements du « droit à l'oubli »' (Village de la Justice, 1 October 2014) <http://www.village-justice.com/articles/Premiers-enseignements-droit-oubli,17868.html> accessed 4 August 2016.

[201] Charte du droit à l'oubli numérique : mieux protéger les données personnelles des internautes' (Portail du gouvernement, 18 October 2010) <http://archives.gouvernement.fr/fillon_version2/gouvernement/charte-du-droit-a-l-oubli-numerique-mieux-proteger-les-donnees-personnelles-des-interna.html> accessed 4 August 2016.

[202] Ibid.

[203] Giles Tremlett, Angelique Chrisafis and Kate Connolly, 'Forget me not : campaigners fight for control of online data' *The Guardian* (London, 4 April 2013).

[204] 'Number of daily active Facebook users worlwide as of second quarter 2016 (in millions)' (The Statistics Portal, 2016) < http://www.statista.com/statistics/346167/facebook-global-dau/> accessed 4 August 2016.

[205] 'Parts de marchés des moteurs de recherche en France' (Le Journal du Net, 25 July 2015) http://www.journaldunet.com/ebusiness/le-net/1087481-parts-de-marche-des-moteurs-de-recherche-en-france/ accessed 4 August 2016.

respectively only 4.13% and 2.72% of the requests on the search engines.[206] It is therefore understandable why Microsoft signed the Charter without difficulty.

The reluctance of Google is undoubtedly linked to issues of territoriality and transfer of data outside the European Union.[207] Facebook instead argued that it was trying to define its "own standards".[208] In summary, the 'Code of Good Practice on the Right to be Forgotten on Social Networks and Search Engines' signed in 2010 suffered from its lack of ambition and lack of real will of the most concerned digital actors.

3.5.4. A Bill 'For a Digital Republic'

A bill entitled 'A Bill for a Digital Republic'[209] is currently under discussion in Parliament since December 2015. The bill, initiated by the current Secretary of State in charge of digital technology, Axelle Lemaire, grants new rights to Internet users. Several measures promote the free disposal of personal data and are relevant to the right to be forgotten. The latter, already granted to Europeans since 2014, will be improved for French minor children, more vulnerable to the risks linked to the use of powerful technologies. They will be able to delete personal data through a specific accelerated procedure. Moreover, 'revenge porn', which consists of uploading intimate photos or videos without the consent of the persons concerned, will be liable of two years imprisonment and a 60,000 euros fine.[210]

The bill deals also with the concept of 'numerical death'.[211] A person will be able to organise the conditions of conservation and communication of her personal data after her death, like transmitting guidelines and designating a person responsible for their execution.

---

[206] Ibid.
[207] Laurent Checola, ' « Droit à l'oubli » sur Internet : une charte signée sans Google ni Facebook' *Le Monde* (Paris, 13/10/2010) available at < http://www.lemonde.fr/technologies/article/2010/10/13/droit-a-l-oubli-sur-internet-une-charte-signee-sans-google-ni-facebook_1425667_651865.html>.
[208] Christian Delporte, 'Droit à l'oubli : la Charte de NKM ronronne' *Libération* (Paris, 15 October 2010) available at http://www.liberation.fr/medias/2010/10/15/droit-a-l-oubli-la-charte-de-nkm-ronronne_686567.
[209] 'Projet de loi pour une République numérique [26 Janvier 2016] available at http://www.assemblee-nationale.fr/14/ta/ta0663.asp.
[210] Benjamin Hue, 'Loi sur le Numérique: revenge porn, droit à l'oubli, mort numérique…Ce qui va changer' (RTL, 26 January 2016) < http://www.rtl.fr/actu/politique/loi-sur-le-numerique-revenge-porn-droit-a-l-oubli-mort-numerique-ce-qui-va-changer-7781542323> accessed 5 August 2014.
[211] Benjamin Hue, 'Loi sur le Numérique: revenge porn, droit à l'oubli, mort numérique…Ce qui va changer' (RTL, 26 January 2016) < http://www.rtl.fr/actu/politique/loi-sur-le-numerique-revenge-porn-droit-a-l-oubli-mort-numerique-ce-qui-va-changer-7781542323> accessed 5 August 2014.