TILBURG UNIVERSITY LAW SCHOOL

BLOCKCHAIN AND THE RIGHT TO BE FORGOTTEN: A HAPPY “MARRIAGE”?

MASTER THESIS DISSERTATION

LL.M INTERNATIONAL BUSINESS LAW
2018/2019

JOSÉ MIGUEL MOREIRA MORENO

SUPERVISOR: OMOLOLU BAJULAIYE, LL.M

TILBURG, AUGUST 2019

Index

Introduction

The rise of Smartphones in the past few years, which enabled us to have everything at the distance of a click, has completely revolutionized the way people live, shop, and interact with each other. People find themselves permanently online, generating enormous amounts of data, which has caused the famous KYC (Know Your Customer) model to shift to a KYD (Know Your Data) model. As some might say, "The world's most valuable resource is no longer oil, but data"[1] moreover, in this data-driven world, the most valuable companies are no longer oil companies but technology companies such as Alphabet, Amazon, Apple, Facebook, and Microsoft. All this massive quantity of data that is collected is what makes possible for companies and governments to extract information, set patterns and draw conclusions, provided that they own the right analytical tools as it is substantially known that they do.

Big Data presents not only significant economic opportunities but big responsibilities and issues too. Companies are collecting vast quantities of data, but data, per se, is not where the value resides. Big data analytic tools allow the extraction of valuable information from the different metrics that are registered. The applications are limitless, from sales conversion ratios to the rationalization of processes through evidence-based decision mechanisms[2]. Big data also allows the identification of new opportunities and the pursuit of those in which real economic value is present. Its potential increases exponentially when combined with correlated technologies such as machine learning algorithms. However, it also poses some risks. The major one is compliance with existent regulations – the GDPR is vital to this extent – but also the accuracy of the system. Cases have happened where conclusions have drawn inaccurate conclusions or outcomes

[1] 'The world's most valuable resource is no longer oil, but data' (The Economist, 6 May 2017) <www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>accessed 19 April 2019

[2] Andrew O'Connell and Walter Frick, "You've Got the Information, But What Does it Mean? Welcome to 'From Data do Action'" (2014) HBR, 1.

which have led to some discriminatory[3] situations[4]. Consequently, human action is required in order to improve the algorithms' performance and eliminate bias.

Privacy and Data Protection were indeed hot topics back in May 2018. The General Data Protection Regulation (GDPR)[5] entered into force as of May 25th, 2018 and it brought challenges for companies, public authorities and all those that have to be compliant with it according to the GDPR[6]. Nevertheless, recent scandals such as Cambridge Analytica[7][8][9] and other massive data leaks brought this discussion into the community as a whole, raising both awareness and apprehension surrounding this prominent subject. As a result, big technology companies like Facebook and Google have been in the "eye of the hurricane" ever since. Firstly, Facebook took part in the Cambridge Analytica Scandal and other leaks of user data – e.g., recently, more than 540 million Facebook[10] records were exposed on Amazon cloud servers[11] -, raising concern about the way these companies effectively use our data and to whom they transmit it to. As a result of Facebook's malpractice handling user data, the Federal Trade

[3] Emily Barwell, 'Big Data – Understanding the Risks' (*Lexology,* 4 April 2018) <https://www.lexology.com/library/detail.aspx?g=bd810ed1-af5b-44b4-bc68-577e23e21ab4> accessed 18 July 2019. "A female doctor was locked out of a changing room because the automated security system had profiled her as a male as it had associated the title "Dr." with a men."

[4] James Vincent, 'Google 'fixed' its racist algorithm by removing gorillas from its image-labeling tech' (*The Verge*, 12 January 2018) <https://www.theverge.com/2018/1/12/16882408/google-racist-gorillas-photo-recognition-algorithm-ai> accessed 18 July 2019. In 2015, the image recognition algorithm used by Google was classifying black people as "gorillas".

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016].

[6] *Ibid*, L119/32, arts. 2 and 3

[7] Richard Water, 'Facebook sued by US regulator over Cambridge Analytica scandal' (Financial Times, 19 December 2018) <www.ft.com/content/683554b2-03c2-11e9-99df-6183d3002ee1> accessed 22 April 2019

[8] Aliya Ram, 'Facebook appeals against UK fine over Cambridge Analytica' (Financial Times, 21 November 2018) <www.ft.com/content/2af83cd4-eda3-11e8-89c8-d36339d835c0> accessed 22 April 2019.

[9] Hannah Murphy and Khadim Shubber, 'Facebook under criminal investigation over data deals' (Financial Times, 14 March 2019) <www.ft.com/content/d7e5a96c-45f6-11e9-b168-96a37d002cd3> accessed 22 April 2019.

[10] Julia Carrie, 'Hundreds of millions of Facebook records exposed on public servers – report' (The Guardian, 3 April 2019) < www.theguardian.com/technology/2019/apr/03/facebook-data-public-servers-amazon> accessed 22 April 2019

[11] Jason Silverstein, 'Hundreds of millions of Facebook user records were exposed on Amazon cloud server' (CBS News, 4 April 2019) <www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/> accessed 22 April 2019

Commission (FTC) approved a fine of 5 Billion US dollars[12]. Although it represents the most severe fine imposed in the United States of America against a tech company – unlike in Europe – the decision was also subject to some criticism. The democrat Representative David Cicilline called it a "slap on the wrist"[13] while Senator Richard Blumenthal urged for the need to accomplish "deep structural reforms"[14]. Secondly, Google being fined in France by the Commission Nationale de l'Informatique et des Libertés (hereinafter, CNIL) in 50 million Euros for, allegedly, failing to comply with its GDPR obligations, namely, failure to provide enough information to users about its data consent policies and how their information is used[15].

Another exciting subject has certainly been Blockchain Technologies[16]. With respect to Blockchain, a lot has been said and written and we find ourselves living the "hype", which can be perfectly summarized by Dan Ariely's words regarding Big Data: "Big Data is like teenage sex: everyone talks about it, nobody really knows how to do it, everyone thinks everyone else is doing it, so everyone claims they are doing it…"[17]. Nevertheless, Blockchain has multiple potential and realistic applications, ranging from personal identification to banking or even supply chain management, and some even advocate that it is the most significant innovation since the creation of the Internet[18]. Without getting into much detail, one of the key characteristics that make Blockchain so exciting is the immutability, i.e., once data is stored on the Blockchain, it cannot be changed. On the other hand, GDPR grants individuals in certain circumstances the Right to Erasure of their data or, how it is commonly known, the Right to be Forgotten[19]. Although

[12] Cecilia Kang, 'F.T.C. Approves Facebook Fine of About $5 Billion' (New York Times, 12 July 2019) <https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html> accessed 17 August 2019.

[13] *Ibid*.

[14] *Ibid*.

[15] Jon Porter, 'Google fined €50 million for GDPR violation in France' (The Verge, 21 January 2019) <www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil> accessed 22 April 2019

[16] PwC Global Blockchain Survey, <www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html> accessed 22 April 2019. 84% of the respondents answered that they are actively involved with Blockchain. However, 45% believe trust could delay adoption.

[17] Dan Ariely's Facebook post (6 January 2013).

[18] Mark Fenwick, Wulf A. Kaal and Erik P.M. Vermeulen, 'Legal Education in the Blockchain Revolution' (2017) <https://ssrn.com/abstract=2939127> accessed 20 July 2019.

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016], L119/43, art. 17 (GDPR)

these two realities, at least in theory, seem diametrically opposed, they coexist. How shall this situation be addressed?

Within this apparent contradiction lies the research question of this thesis: What are the implications of the “Right to be Forgotten” in a Blockchain technology solution?

Surely that it is not an easy task the one that is being tried to accomplish here because this technology is in constant adaptation, which makes it a moving target. However, that is what makes it so challenging and at the same time rewarding. In order to be able to answer the main research question, there is a set of sub-research questions that must be answered too. First of all, is it possible to reconcile the right to be forgotten with the immutability of the blockchain? In case of an affirmative answer, how can that be achieved? Secondly, the GDPR assigns different roles and responsibilities. How are these roles distributed in a DLT scenario?

Regarding the methodology used, a doctrinal approach will be followed, where the main sources are the General Data Protection Regulation (GDPR), the Treaty of the European Union (hereinafter, TEU) and the European Union Charter of Fundamental Rights (hereinafter, the Charter). In addition, relevant scientific articles, news, consultancy reports, and online blogs will also be taken into consideration. Since many countries are still waiting for further developments – possibly an European level answer to the problem - a comparative study will not be performed. Nevertheless, CNIL’s (Commission Nationale de l’Informatique et des Libertés) recently published report/guidance will also be used as an important source, mainly in Chapters 3 and 4, where the relation between Blockchain and the Right to be Forgotten will be discussed, as well as the different proposed solutions. The advantage of using a multitude of different types of sources is a more comprehensive view of the subject. On the one hand, an analysis limited to the letter of the law would be clearly insufficient taking into account the importance of the different contributions, such as the doctrine and the case law, play in the construction of the legal science in its entirety. On the other hand, an analysis dissociated from the letter of the law would not suffice as it would be in complete disregard of the cornerstone of the legal system.

Concerning the thesis' structure, this brief introduction precedes the first chapter and explains the importance of the topic and why this thesis is relevant and contributes to the body of knowledge already existent regarding this matter. The first chapter looks at a summary explanation of the General Data Protection Regulation, its background, and, in more detail, what is the Right to be Forgotten, the principles and values that have presided its creation but also its limitations. Furthermore, the Google Spain[20] case from the Court of Justice of the European Union (hereinafter, CJEU) will also be briefly analysed. In the second chapter, Blockchain technology is introduced and the main features are outlined. In the third chapter, the relationship between Blockchain and the Right to be Forgotten is explored in more detail. In the fourth chapter, the core of this thesis, consists of a critical analysis of the proposed solutions and this thesis' view on the topic. To conclude this study, the resulting findings will be presented and the research question that prompted this master thesis will be answered.

[20] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] CJEU

Chapter 1: General Data Protection Regulation and the Right to be Forgotten

1.1 Historical Evolution

In order to fully understand the reach of the GDPR, it is fundamental to conduct a brief historical review on the evolution of European legislation on this matter. Data protection in Europe began in the 1970s at an individual level, in Germany, followed by Sweden, France, the Netherlands and the United Kingdom.[21] Later, in 1981, the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108, which became the first and, up until now, the only diploma at an international level. Only in 1995, the European Commission felt the need to harmonise the legislation which had spread throughout European countries, and adopted the Directive 95/46/EC[22]. The Directive 95/46/EC would be in force until 25 May 2018, the date when it was repealed by the GDPR[23]. The Directive 95/46/EC[24], which contributed to the development of the internal market within Member States, had already established some principles that would also be incorporated in the GDPR later on, such as the principles of "fair and lawful processing"[25], "purpose limitation and specification"[26], "data minimisation"[27], among others. Nonetheless, Member States have a margin of discretion when transposing Directives which lead to different levels of protection in different countries, but to unequal degrees of enforcement and sanctions as well[28]. Therefore, after years of intense debate and discussion, the EU adopted the GDPR back in 2016, which became effective on 25 May 2018 after a two year

[21] European Union Agency for Fundamental Rights and Council of Europe '*Handbook on European data protection law*' (2018), 18.

[22] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[23] GDPR, L 119/86, art. 94

[24] Remember that Directives, unlike Regulations, do not apply directly and need to be transposed into the national legislation of each Member State.

[25] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] L281/40, art. 6 (1)(a).

[26] *Ibid*, art. 6 (1)(b).

[27] *Ibid*, art. 6 (1)(c).

[28] European Union Agency for Fundamental Rights and Council of Europe *'Handbook on European data protection law'* (2018), 30.

transition period. Last but not least, it is worth mentioning that one of the main goals of the GDPR is to support the Digital Single Market, by creating a level playing field in all Member States through harmonization[29] across a wide range of different areas, such as payments, VAT, consumer protection rules and geoblocking[30].

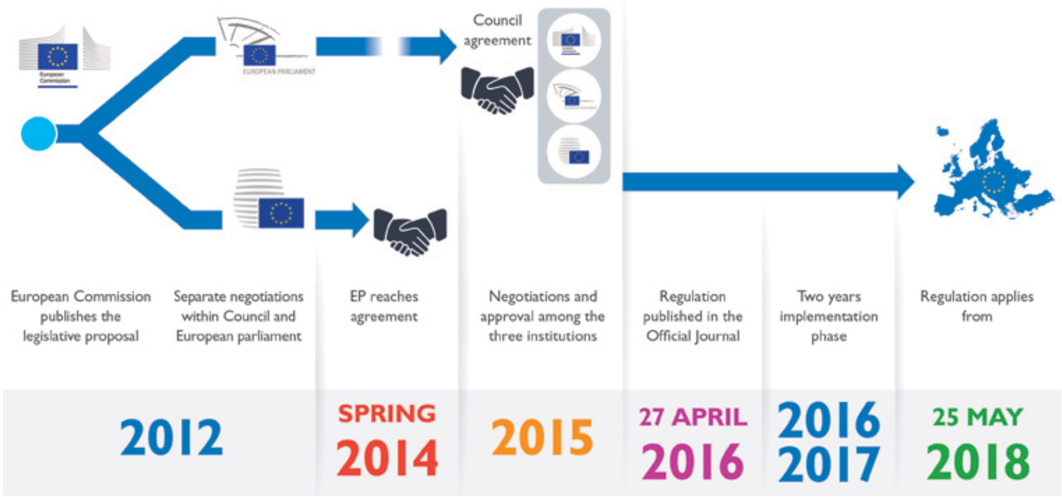

Council agreement
European Commission publishes the legislative proposal
Separate negotiations within Council and European parliament
EP reaches agreement
Negotiations and approval among the three institutions
Regulation published in the Official Journal
Two years implementation phase
Regulation applies from
2012
SPRING 2014
2015
27 APRIL 2016
2016 2017
25 MAY 2018

Diagram #1[31].

Source: DLA Piper[32]

Simultaneously, the European Convention on Human Rights (hereinafter, ECHR), which was enacted in 1950 and entered into force in 1953, establishes on Article 8 the “Right to respect for private and family life”. Besides not including the right to personal data protection as a separate right, it is considered to be part of the situations protected under Article 8 as evidenced by the many cases[33] decided by the European Court of Human Rights (hereinafter, ECtHR).

In terms of primary EU Law, i.e., the treaties – Treaty on European Union (hereinafter, TEU) and the Treaty on the Functioning of the European Union

[29] Linklaters, “The General Data Protection Regulation, A Survival Guide”, version 2.0, 11.

[30] ‘New EU rules on e-commerce’ <https://ec.europa.eu/digital-single-market/en/new-eu-rules-e-commerce> accessed 20 August 2019.

[31] This diagram illustrates the procedural timeline between 2012 and 2018.

[32] “EU General Data Protection Regulation” <www.dlapiper.com/en/us/focus/eu-data-protection-regulation/background/> accessed 28 April 2019.

[33] Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland no 931/13 (ECtHR, 27 June 2017).

(hereinafter, TFEU) – did not have any reference regarding fundamental rights and consequently data protection rights[34]. In order to solve this situation, the CJEU, through its interpretations, integrated them as general principles of EU Law. However, the decisive step happened when the EU enacted the Charter of Fundamental Rights of the European Union in the year of 2000. The Charter represented an innovation in the sense that it provided individual treatment for the right to "protection of personal data", separated from the right to "respect for private and family life". Even though the first was viewed as being included in the latter, this individualization of the right to protection of personal data represents and acknowledges the evolution that this right has been facing. Especially when considering the development of a social model based on information, internet, computers, and other technologies, all of them contributing to much faster processing of personal data. Furthermore, as a symbolic gesture, this was an important action from the part of the EU, setting the ground for the further developments already mentioned. The Charter, which started as a political document, became legally binding in 2009 when the Treaty of Lisbon came into force and raised[35] the Charter to the level of primary[36] EU Law[37].

1.2 What is personal data?

First of all, it is essential to understand the object of this diploma – what is personal data after all? Up until now, there is no universal definition for personal data, therefore it seems appropriate to take the GDPR definition as a working definition, due to the fact that we are working with EU Law. Therefore, "personal data" can be described as: "any information relating to an identified or identifiable natural person ('data subject')"[37]. It seems, however, quite insufficient to perceive the real extension of what can be qualified as personal data but, fortunately, the GDPR provides an answer to this question:

[34] European Union Agency for Fundamental Rights and Council of Europe '*Handbook on European data protection law'* (2018), 27.
[35] Treaty of Lisbon [2007] C 306/12, art. 1.
[36] Consolidated Version of the Treaty on European Union [2012] OJ C 326/19, art. 6/1.
[37] Furthermore, when the Treaty of Lisbon came into force, it also amended the TFEU. See article 16.
[37] GDPR, L 119/33, art. 4 (1).

> an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; [38]

Personal data is essentially any element or characteristic that refers to one's individuality, to the elements that characterize that person and that allow him/her to be identified as such. This is also true when dealing with pseudonymised data and therefore the same reasoning should be followed, due to the fact that it is possible to establish the connection between the pseudonymized data and the natural person to whom it belongs. The following logic step is to determine when a natural person is identifiable or not, taking into account "all the means reasonably likely to be used, such as singling out, either by the controller[39] or by any other person to identify the natural person directly or indirectly."[40] When doing so, i.e., to ascertain whether such means are reasonably likely to be employed, should be weighed "the costs and the amount of time required for identification, taking into consideration the available technology at the time of processing and technological developments."[41] On the other hand, the GDPR explicitly states that neither the principles of data protection nor the GDPR itself shall be applied to anonymous data given the fact that it is not possible to trace back and identify the data subject[42].

In summary, a set of anonymised data cannot be linked back to the data subject, whereas a set of pseudonymised data can still be traced back to a specific data subject through the use of additional information. The difference is relevant as it determines the qualification of a set of data as personal data or non-personal data.

1.3 Scope of Application

[38] The GDPR sets forth a more demanding regime to process sensitive personal data. See *Ibid*, L 119/38, art. 9.

[39] Ascertain who assumes the role of controller for GDPR purposes is of crucial importance due to the obligations that the GDPR prescribes to the controller.

[40] *Ibid*, L 119/5, Recital 26.

[41] *Ibid.*

[42] *Ibid*.

Regarding the material scope of the GDPR, it is defined both through a positive and a negative delimitation. It applies to the processing of personal data, whether this is fully automated, partially automated or done by any other means which form part of a filing system[43] or are intended to do so[44]. Yet it provides in the same article the situations in which it is not applicable, such as: "in the course of an activity which falls outside the scope of Union law[45]; by the member States when carrying out activities which fall within the scope of Chapter 2 of Title V of TEU[46]; by a natural person in the course of a purely personal or household activity[47]; by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding and the prevention of threats to public security[48]."

Concerning the territorial scope, the GDPR comprehends a more significant number of situations, when compared to the Directive it replaces, due to its broader scope. GDPR applies to but not exclusively processing of personal data "in the context of activities of an establishment"[49] within the European Union, regardless of whether the processing takes place within the Union. The definition of establishment is also given by the GDPR itself, being "the effective and real exercise of activity through stable arrangements"[50], irrespective of its legal form. Moreover, GDPR is also applicable to situations where organisations are not established in the EU and their processing activities are related to: "the offering of goods or services, irrespective of whether a payment of the data subject is required to such data subjects in the Union"[51], this means, no payment is necessary, and "the monitoring of their behaviour as far as their behaviour takes place within the Union[52]." Finally, GDPR must be applied when Public International Law dictates that a Member State law is applicable[53].

[43] GDPR, L 119/33, art. 4 (6).
[44] *Ibid*, L 119/32, art. 2 (1).
[45] *Ibid*, L 119/32, art. 2 (2)(a).
[46] *Ibid*, L 119/32, art. 2 (2)(b).
[47] *Ibid*, L 119/32, art. 2 (2)(c).
[48] *Ibid*, L 119/32, art. 2 (2)(d).
[49] *Ibid*, L 119/32, art. 3 (1).
[50] *Ibid*, L 119/4, Recital 22.
[51] *Ibid*, L 119/33, art. 3 (2)(a).
[52] *Ibid*, L 119/33, art. 3 (2)(b).
[53] *Ibid*, L 119/33, art. 3 (3).

Such a vast scope of application reflects the effort made by the EU in assuring data protection as a fundamental right, and it has many practical implications, such as the obligation to designate a representative in the Union when Article 3(2) GDPR is applicable[54]. Similar aspects and several others that we can find throughout this piece of legislation influence the way undertakings do business, as they provide incentives or, on the contrary, discouragement to act in a certain way, as it happens with tax reforms.

1.4 Data Controllers and Processors

In the Google Spain case, the Audiencia Nacional, the Spanish High Court, decided to refer a set of questions to the CJEU for a preliminary ruling. The most important question was whether or not Google should be regarded as a controller[55]. Due to its practical duties and obligations, the definition of the data controller is highly relevant in the context of data protection, hence the significance of the CJEU ruling.

Currently, the GDPR defines a "controller"[56] as:

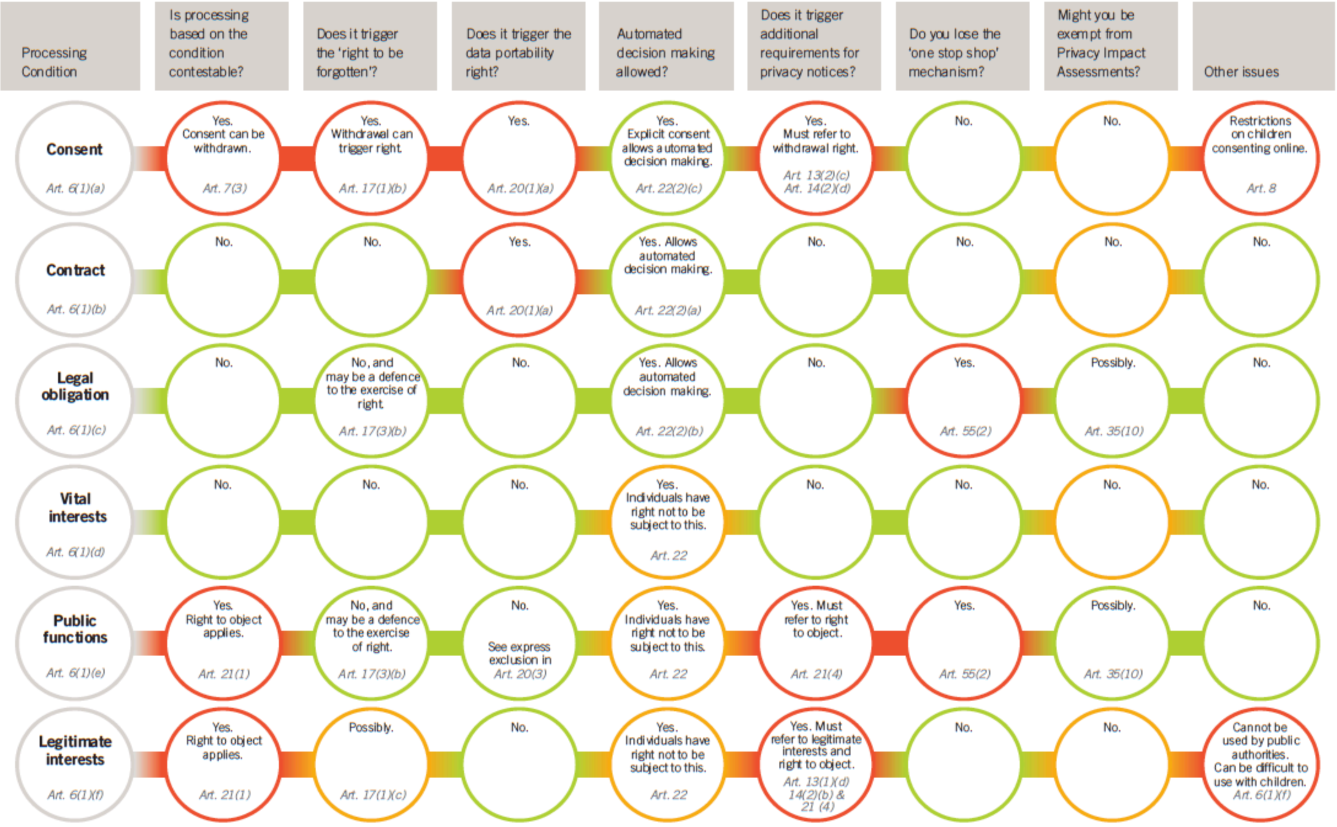
> the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

However, when personal data is processed in a context of purely personal or household activity, that individual should not be deemed as a "controller" under the GDPR due to the fact that his/her actions are comprehended within the exemptions provided for in Article 2 (2)I GDPR and therefore the GDPR is not even applicable.

Meanwhile, a "processor" is "a natural or legal person, public authority agency or other body which processes personal data on behalf of the controller." [57] Any processing activity must satisfy, at least, one statutory processing

[54] *Ibid*, L 119/48, art. 27 (1).
[55] Article 29 Working Party, "Opinion 1/2010 on the concepts of "controller" and "processor"" [2010].
[56]GDPR, L 119/33, Art. 4 (7).
[57] *Ibid*, L 119/33, Art. 4 (8).

condition of those listed on GDPR, Article 6. It is also important to highlight that certain processing conditions provide higher guarantees than others from a controller's perspective – as illustrated in diagram –2 - as they affect the obligations imposed by the GDPR and the individual's rights[58] – e.g., if the processing is based solely on consent, it is likely that the right to be forgotten will be triggered since consent can be withdrawn at any moment.



Processing Condition	Is processing based on the condition contestable?	Does it trigger the 'right to be forgotten'?	Does it trigger the data portability right?	Automated decision making allowed?	Does it trigger additional requirements for privacy notices?	Do you lose the 'one stop shop' mechanism?	Might you be exempt from Privacy Impact Assessments?	Other issues
Consent Art. 6(1)(a)	Yes. Consent can be withdrawn. Art. 7(3)	Yes. Withdrawal can trigger right. Art. 17(1)(b)	Yes. Art. 20(1)(a)	Yes. Explicit consent allows a utomated decision making. Art. 22(2)(c)	Yes. Must refer to withdrawal right. Art 13(2)(c) Art. 14(2)(d)	No.	No.	Restrictions on children consenting online. Art. 8
Contract Art. 6(1)(b)	No.	No.	Yes. Art. 20(1)(a)	Yes. Allows automated decision making. Art. 22(2)(a)	No.	No.	No.	No.
Legal obligation Art. 6(1)(c)	No.	No, and may be a defence to the exercise of right. Art. 17(3)(b)	No.	Yes. Allows automated decision making. Art. 22(2)(b)	No.	Yes. Art. 55(2)	Possibly. Art. 35(10)	No.
Vital interests Art. 6(1)(d)	No.	No.	No.	Yes. Individuals have right not to be subject to this. Art. 22	No.	No.	No.	No.
Public functions Art. 6(1)(e)	Yes. Right to object applies. Art. 21(1)	No, and may be a defence to the exercise of right. Art. 17(3)(b)	No. See express exclusion in Art. 20(3)	Yes. Individuals have right not to be subject to this. Art. 22	Yes. Must refer to right to object. Art. 21(4)	Yes. Art. 55(2)	Possibly. Art. 35(10)	No.
Legitimate interests Art. 6(1)(f)	Yes. Right to object applies. Art. 21(1)	Possibly. Art. 17(1)(c)	No.	Yes. Individuals have right not to be subject to this. Art. 22	Yes. Must refer to legitimate interests and right to object. Art. 13(1)(d) 14(2)(b) & 21 (4)	No.	No.	Cannot be used by public authorities. Can be difficult to use with children. Art. 6(1)(f)

Diagram #2.

Source: Linklaters[59]

The GDPR also represents a change in comparison with the Directive as it places direct obligations from which processors were previously exempt, for instance, to maintain a record of processing carried out on behalf of a controller[60]; cooperate

[58] Linklaters, "The General Data Protection Regulation, A Survival Guide", version 2.0, 19.

[59] *Ibid*.

[60] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] L 119/51, art. 30 (2).

with national supervisory authorities[61]; to appoint a data protection officer in certain cases[62]; and to comply with the rules on transfers of personal data outside the EEA[63].

This legal framework, as well as the general features that characterize the existent arrangement between controllers and processors, can be better understood through an analogy with a different reality, yet very popular, a football team. In a football team, the "controller" would be the coach, determining the tactics, i.e., why, how, and which personal data will be processed, whereas the "processor" in this analogy would assume the role of a player, acting accordingly to the instructions given by the coach. As well as in a real football team, both of them are accountable, *mutatis mutandis*, to superior authorities. The coach and the players are accountable to the president of the club, in representation of the supporters, while the controller and the processor are supervised by the national[64] data protection authorities[65], which might impose administrative fines[66] for violations of the GDPR. Processors and controllers are also held accountable by the private right of action given to individuals to compensate them for any suffered material or non-material damages[67].

In conclusion, processors are now more accountable than ever, but the most liable were and still are the controllers.

[61] *Ibid*, L 119/51, Art. 31.

[62] *Ibid*, L 119/55, Art. 37.

[63] *Ibid*, L 119/60, Art. 44.

[64] *Ibid*, L 119/71, Arts. 60 to 70, for a general framework for cooperation between supervisory authorities and the role of action of the GDPR consistency mechanism and the European Data Protection Board.

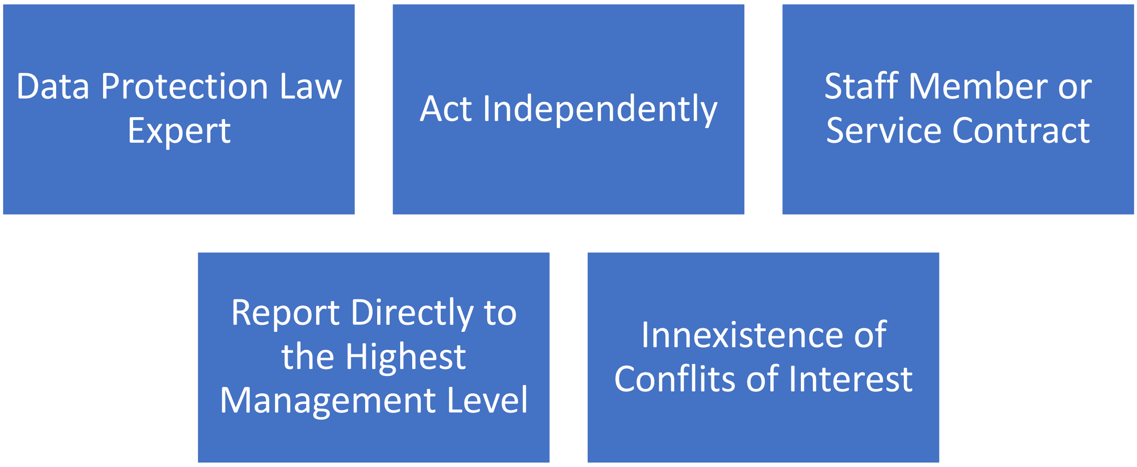
[65] Truly independent supervision is an essential component of EU data protection law. See *Ibid*, L 119/66, Art. 52; Charter of Fundamental Rights of the European Union [2012] OJ C 326/397, art. 8 (3); and also: Case C-362/14, *Maximilliam Schrems v. Data Protection Commissioner* [GC] [2015] CJEU; Case C-518/07, *European Commission v. Federal Republic of Germany* [GC] [2010], para. 25, CJEU; Case C-614/10*, European Commission v. Republic of Austria* [GC] [2012], paras 59 and 63, CJEU; and Case C-288/12, *European Commission v. Hungary* [GC] [2014], paras 50 and 67, CJEU.

[66] GDPR, L 119/82, arts. 83 and 84.

[67] *Ibid*, L 119/81, Art. 82.

1.5 Innovations: Data Protection Officers and Data Breach Notifications

Data Protection Officers[68] (DPOs) are one of the main innovations brought by the GDPR, however, there is no definition of DPO in the GDPR. DPOs are persons who advise and monitor compliance with data protection rules in organisations. As part of their role, they also work as a contact point between the organisation and the supervisory authority[69]. Section 4 of the GDPR is especially devoted to DPOs[70], providing us with the framework for this new role, such as the criteria to be taken into account when appointing a DPO, the duties and tasks, the relationship with controllers and processors, among other aspects. The designation of a DPO is only mandatory[71] when specific requirements, which are provided for in Article 37 of the GDPR, are met. However, it is essential to bear in mind that a voluntary designation will trigger the application of all the provisions of the GDPR.


Data Protection Law Expert
Act Independently
Staff Member or Service Contract
Report Directly to the Highest Management Level
Innexistence of Conflits of Interest

DPO's characteristics[72]

Diagram #3

[68] Article 29 Working Party, "Guidelines on Data Protection Officers ('DPOs')" [2017].
[69] GDPR, L 119/56, art. 39.
[70] However, there are some dispersed considerations regarding DPOs in other parts of the GDPR.
[71] *Ibid*, L 119/55, Art. 37.
[72] *Ibid,* L 119/55, Section 4.

Another significant change introduced by the GDPR[73] was the obligation to notify data breaches. Personal data breaches are defined by the GDPR as:

> a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.[74]

In case of a personal data breach, controllers shall without undue delay – not later than 72 hours – notify it to the supervisory authority unless it does not represent a risk to the rights and freedoms of natural persons[75]. Nevertheless, in case of high risk, the data breach shall be communicated to the data subject too[76]. Whenever the data breach occurs at the level of a processor's activity, the processor has a duty to notify the controller[77], which will subsequently convey the information as previously mentioned.

1.6 Right to Erasure (Right to be Forgotten)

The right to erasure, which is also frequently referred to as the right to be forgotten, is codified into the GDPR in Article 17 and it is one of the greatest innovations of this recently introduced piece of legislation. Although the right is not limited to search engines, it was brought into the spotlight when the Court of Justice of the European Union, in 2014, ruled against Google. The case commonly known as *Google Spain* opposed Mr. Mario Costeja González and the Agencia Española de Protección de Datos (AEPD) to Google Inc and its subsidiary Google Spain SL. It all started back in 5 March 2010 when Mr. Costeja González filed a complaint to the AEPD against Google Inc and Google Spain.

The AEPD decided in favour of Mr. Costeja González, ordering Google Inc to remove the solicited personal data, which consisted of outdated information regarding past financial difficulties[78] relating to Mr. Costeja González, from its

[73] See also, Article 29 Working Party, "Guidelines on Personal data breach notification under Regulation 2016/679", WP250, [2017].

[74] GDPR, L 119/34, Art. 4 (12).

[75] *Ibid*,L 119/52, art. 33.

[76] *Ibid*, L 119/52, Art. 34.

[77] *Ibid*, L 119/52, Art. 33 (2).

[78] Mr. Costeja González's name appeared for a real-estate auction related with the recovery of social security debts. Mr Costeja González requested that information to be removed both from the daily newspaper "La Vanguardia" and Google Search's results.

search engi–e - Google Sear–h - index and to prevent future accesses to that very same data[79]. Google Spain and Google Inc. brought two separate actions against that decision before the Audiencia Nacional (the National High Court) which decided to join the actions[80].

The Audiencia Nacional decided to refer a set of questions for a preliminary ruling to the CJEU as a way of eliminating its concerns about EU law interpretation, namely regarding Directive 95/46/EC.

Summarizing[81], the CJEU considered that the activity carried out by the operator of a search engine "is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name". The reason why that is likely to happen is that Google enables a "structured overview" due to its list of results, "which, without the search engine, could not have been interconnected or could have been only with great difficulty"[82]. The court also made reference to the fact that the interference with those rights cannot be merely justified by the operator of the search engine's economic interest[83], which is tremendously important to understand which rights must and which ones must not be taken into consideration. In that sense, the court referred that, on a case by case judgement, the interest of users potentially interested in having access to that information has to be weighed up against the data's subject fundamental rights under Articles 7 and 8 of the Charter[84]. Also, the search engine operator is obliged to remove the links to web pages from the list of results, when the search is carried out on the basis of an individual's name, even when its publication on those pages is lawful[85].

Part of the reason why Google Spain decision was so important is because search engines were regarded as data controllers and clarified the existence of a right to be forgotten. It has serious implications for every internet actor, not only

[79] Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] CJEU

[80] *Ibid*, para. 18.

[81] For further developments, Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] CJEU, available at:<http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5050217 >

[82] *Ibid*, para. 80.

[83] *Ibid*, para. 81.

[84] *Ibid*.

[85] *Ibid*, para. 88.

search engines. In addition, it also emboldened not just the Court or the Regulators, but the data protection paradigm in general[86]. The Right to be Forgotten is much broader than the right to delisting from search engines.

As part of the intention to give back to individuals control over their personal data and ensuring that people's privacy is sufficiently protected[87], the right to be forgotten was then explicitly codified in the GDPR, more precisely, in Article 17. The requests shall be addressed to the data controller, who is responsible for the erasure of the data if one of the grounds provided in Article 17 (1) is deemed applicable. Besides, the controller shall take all the reasonable steps to inform other controllers, who might have linked, copied or replicated such data, that the data subject has requested its erasure[88]. Nevertheless, this is not an absolute right and therefore it is subject to limitations, such as the exemptions provided for in article 17 (3) of the GDPR. Hence, data does not have to be erased when it is at stake the exercise of freedom of expression and information[89]; to fulfil a legal obligation[90]; for reasons of public interest, research, statistic, as long as the appropriate safeguards are ensured[91]; and relating to the exercise[92] of legal claims[93].

Consequently, as it has already been mentioned, the conception and application of the right to be forgotten is not peaceful and, therefore, there are some concerns in the existent literature and case law, from which it is pertinent to examine in more detail the relationship between the right to be forgotten and the freedom of expression.

[86] This idea was expressed in David Smith's oral contribution to 'EU Internet Regulation after Google Spain' report of proceedings (27/3/2015) from the University of Cambridge, <https://www.cels.law.cam.ac.uk/sites/www.law.cam.ac.uk/files/images/www.cels.law.cam.ac.uk/documents/google_spain_conference_report_-_16.12.2015.pdf> accessed 26 June 2019.
[87] Hans Graux, Jef Ausloos and Peggy Valcke, "The Right to be Forgotten in the Internet Era" [2012].
[88] GDPR, L 119/44, arts. 17 (2).
[89] *Ibid*, L 119/44, art. 17 (3)(a).
[90] *Ibid*, L 119/44, art. 17 (3)(b).
[91] *Ibid*, L 119/44, arts. 17 (3)(c)(d) and 89 .
[92] The term "exercise" here is broadly considered, comprising "establishment, exercise, and defence", as provided in Article 17 (3)(e) GDPR.
[93] *Ibid*, L 119/44, art. 17 (3)(e).

1.7 Right to be Forgotten and Freedom of Expression

When one reads or researches about the right to be forgotten, it certainly will not go unnoticed the great variety of papers and posts discussing the relationship and interference between these two rights, and how the first one is likely to harm the latter. The response is particularly intense in the United States[94], where Constitutional Law, namely, the First Amendment[95], strongly protects such speech from possible limitations as speech[96] on the Internet received the highest level of First Amendment protection[97]. Therefore, the right to be forgotten it is frequently appointed as a new kind of online censorship[98] and "a path to a far less open Internet."[99]

The fact is that Google[100] developed an online form[101] where people can solicit the removal of their personal data by identifying themselves and indicating the URL's which contain the content that they wish to see removed. Google has even created a transparency report, which also displays, among other relevant data, both the number of "Delisting Solicitations"[102] and the total number of URLs solicited to be delisted[103]. The report also provides success rate of the decided

[94] Justia Law. (2019). *Florida Star v. B.J.F., 491 U.S. 524 (1989)*. [online] Available at: https://supreme.justia.com/cases/federal/us/491/524/ [Accessed 4 May 2019].
Where the Supreme Court has long held that information, even if distasteful, has a right to be disseminated if true. In this particular case, the Supreme Court overturned compensatory and punitive damages awarded by a Florida court to a sexual assault victim who saw her name published in a local newspaper, considering that the interest at stake could not justify the inroads made against the freedom of the press.

[95] The First Amendment comprises both the right to speak and the right not to speak.

[96] Franz Werro, "The Right to Inform v. The Right to be Forgotten: A Transatlantic Clash" [2009] in "Liability in the Third Millennium" 285, 286, <https://ssrn.com/abstract=1401357> accessed 4 May 2019.

[97] Justia Law. (2019). *Reno v. American Civil Liberties Union, 521 U.S. 844 (1997)*. [online] Available at: https://supreme.justia.com/cases/federal/us/521/844/ [Accessed 4 May 2019].

[98] Peter Fleischer, "Foggy thinking about the right to oblivion" (Peter Fleischer: Privacy…? 9 March 2011) <http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html> accessed 5 May 2019.

[99] Jeffrey Rosen, "Symposium Issue: The Right to be Forgotten" [2012] SLR 64, 88.

[100] Companies such as Facebook and Google are the most targeted since Google enjoys a dominant position as search engine and its transparency report evidences that the most requested website for the erasure of links is Facebook.

[101] The form is available at: <www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf>

[102] The "delisting solicitations" correspond to the amount of requests. The number of URLs represent the added total amount of ULRs of all the delisting solicitations combined.

[103] Up to date, 2 May 2019, the numbers are respectively (800.128) and (3.116.465). For more updates, please consult <https://transparencyreport.google.com/eu-privacy/overview>

cases since the date of GDPR's implementation: up until now, the success rate is of 44,5% total URLs all around the globe delisted vs 55,5% URLs not delisted.

Whether the right to be forgotten violates freedom of expression, not only in the US but in every other country where the freedom of expression is somehow protected – most likely it will be at constitutional level -, will very much depend on the way this right it is applied and enforced in practice. In fact, the GDPR[104] provides the need for a fair balance between the right to be forgotten and other rights such as access to information and freedom of expression, not to mention that the European Treaties[105] and the Charter[106], raised to the level of primary EU law by the Treaty of Lisbon, recognize it as fundamental right. Furthermore, the fact that Google and other undertakings carry an assessment on whether personal data must be erased, does not preclude the right to lodge a complaint with a supervisory authority[107] nor the right to an effective judicial remedy against a controller or processor[108] or even against a supervisory authority[109].

Thus, it is not possible to conclude that the European legislator was unaware of that mutual interference, on the contrary, all the different values were transposed into the GDPR. Moreover, after the Google Spain case ruling, the Article 29 Working Party adopted guidelines[110] for the implementation of the CJEU decision, with the aim of helping undertakings and supervisory authorities when handling complaints. Google specifically mentions that they "have carefully developed criteria in alignment with the Article 29 Working Party's guidelines" and that in a decision not to delist pages due to its public interest content, several factors are taken into account:

> including – but not limited to – whether the content relates to the requester's professional life, a past crime, political office, position in public life, or whether the content is self-authored content, consists of government documents, or is journalistic in nature.[111]

[104]GDPR, L 119/44, arts. 17 (3)(a) and 85.

[105] Consolidated Version of the Treaty on European Union [2016] OJ C 202/19, art. 6.

[106] Charter of Fundamental Rights of the European Union [2012] OJ C 326/398, art. 11.

[107] GDPR, L 119/80, art. 77.

[108] *Ibid*, art. 79.

[109] *Ibid*, art. 78.

[110] Article 29 Working Party, "Guidelines on the implementation of the CJEU judgment on "*Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*", C-131/12 [2014].

[111] Transparency Report: Search removals under European privacy law <https://transparencyreport.google.com/eu-privacy/overview>, accessed 5 May 2019.

In that regard, a peremptory statement that the right to be forgotten always infringes the core of the right to freedom of expression it is not legitimate. Instead, it must be assessed on a case-by-case basis and will depend on how it is effectively applied. In that sense, quoting scholar Jeffrey Rosen to illustrate this living uncertainty, as we are still in an embryonic state of law enforcement:

> It's possible, of course, that although the European regulation defines the right to be forgotten very broadly, it will be applied more narrowly. Europeans have a long tradition of declaring abstract privacy rights in theory that they fail to enforce in practice.[112]

Rosen's quote illustrates the decisive role played by the Courts' interpretation on this matter. The Right to be Forgotten may seem too broad in abstract, however, one cannot disregard that it needs to meet certain requirements to be applicable and that the Article 17 of the GDPR previews some exemptions, among them, the exercise of freedom of expression and information.[113] Hence the importance of the courts interpretation. As in other conflicting rights where a Court is called upon to decide, everything hinges on how broad the Court defines what constitutes an exercise of freedom of expression and information. The same reasoning is equally applicable to other exemptions such as "reasons of public interest in the area of public health"[114] In practice, the opposite situation might happen, that the exemptions are too broad and, consequently, are raised so often that the right to be forgotten is often considered inapplicable.

[112] Jeffrey Rosen, "Symposium Issue: The Right to be Forgotten" [2012] 64 SLR 88, 92.
[113] GDPR, L 119/44, art. 17 (3)(a).
[114] *Ibid*, art. 17 (3)(c).

Chapter 2: Blockchain

2.1 Blockchains' Background

Regarding, decentralized ledger technologies (DLTs), and Blockchain in particular, the aim of this thesis is to look beyond the hype, building on top of the existent body of knowledge. The starting point is to understand how Blockchain emerged and why it became so popular.

In order to understand the development of this technology, it is necessary to go back to the year of 2008. In September 15th 2008, Lehman Brothers collapsed and filed for bankruptcy, resulting in trillions of dollars lost in market capitalization, thousands of employees lost their jobs, resulting in the global financial crisis. In November 2008, right after this catastrophic scenario, Satoshi[115] Nakamoto proposed Bitcoin, the first peer-to-peer electronic cash system, which did not require financial institutions as intermediaries. Instead of relying on a centralized authority such as a bank, to act as a trusted third party, Bitcoin managed to use this decentralized peer-to-peer network, where the participants do not need to know each other or trust each other to interact to solve the double-spending problem.[116] After Bitcoin, others have followed, such as Ethereum, Ripple and, more recently, Libra. Given the exponential growth experienced in the number of ICOs (Initial Coin Offerings), Blockchain became known as the technology underlying Bitcoin and the other existent cryptocurrencies.

Afterwards, the world began to realize that Blockchain had many other potential applications in the financial industry, but also in supply chain management, agriculture and food security, insurance, healthcare, digital identities and public registries.

[115] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2009), <https://bitcoin.org/bitcoin.pdf> accessed 16 July 2019.

[116] Marcella Atzori, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?" [2015] <https://ssrn.com/abstract=2709713> accessed 15 May 2019.

2.2. Organizations’ Evolution

Blockchain is frequently mentioned as a way to bypass intermediaries, cut transaction costs and streamline processes. It is also pointed out that in enables true peer-to-peer communications and transactions. This is the result of a paradigm shift in the way companies typically organize themselves.

Traditional companies used to be organized in a vertical and hierarchical structure, where several levels of management separate the senior management from the workers in the first stage. However, this structure is too heavy to implement changes. In response, some companies began adopting flatter models of organization[117], reducing hierarchy levels. Thereafter, some companies embraced an even flatter form of organization, the platform structure[118]. The disruption brought by this phenomenon across a range of industries was so intense that the term “platform economy” was created. Uber and Airbnb are perhaps the most famous examples but there are other highly relevant names, some of them operating in other geographies as it is the case of Go-Jek in Asia. Uber[119] and Lyft[120] were recently admitted to the Stock Exchange – NYSE and NASDAQ respectively – with valuations of several billions of dollars, albeit having massive losses both in their quarter and annual reports.

However, platforms still represent a single point of failure. Their level of decentralization is higher than the level of traditional companies, but it does not amount to full distribution. Platforms are still intermediaries that match offer and demand. On the contrary, in a fully distributed Blockchain[121], instead of paying Uber or Airbnb a fee for using their platforms, users would transact with each other directly. In Bitcoin, for example, users still pay a fee to the miners but ideally

[117] E.g., Netflix.

[118] Mark Fenwick, Joseph A. McCahery, Erik P.M. Vermeulen, ‘The End of ‘Corporate Governance’: Hello ‘Platform Governance’’ (2018) <https://ssrn.com/abstract=3232663> accessed 21 July 2019.

[119] ‘Uber IPO’ (*Financial Times*)< https://www.ft.com/content/b3e70e9e-5c4d-11e9-9dde-7aedca0a081a> accessed 21 July 2019.

[120] Sara Salinas, ‘Lyft pops in trading debut settles to modest gains’ (*CNBC*, 29 March 2019) < https://www.cnbc.com/2019/03/29/lyft-ipo-stock-starts-trading-on-public-market.html> accessed 21 July 2019.

[121] Mark Fenwick, Wulf A. Kaal and Erik P.M. Vermeulen, ‘Why Blockchain’ Will Disrupt Corporate Organizations’ (2018) <https://ssrn.com/abstract=3227933> accessed 21 July 2019.

the amounted transaction costs would be lower[122]. Diagram #4 is a keen representation of how technical progress has enabled more social connectivity and decentralization between 1980 and 2020.

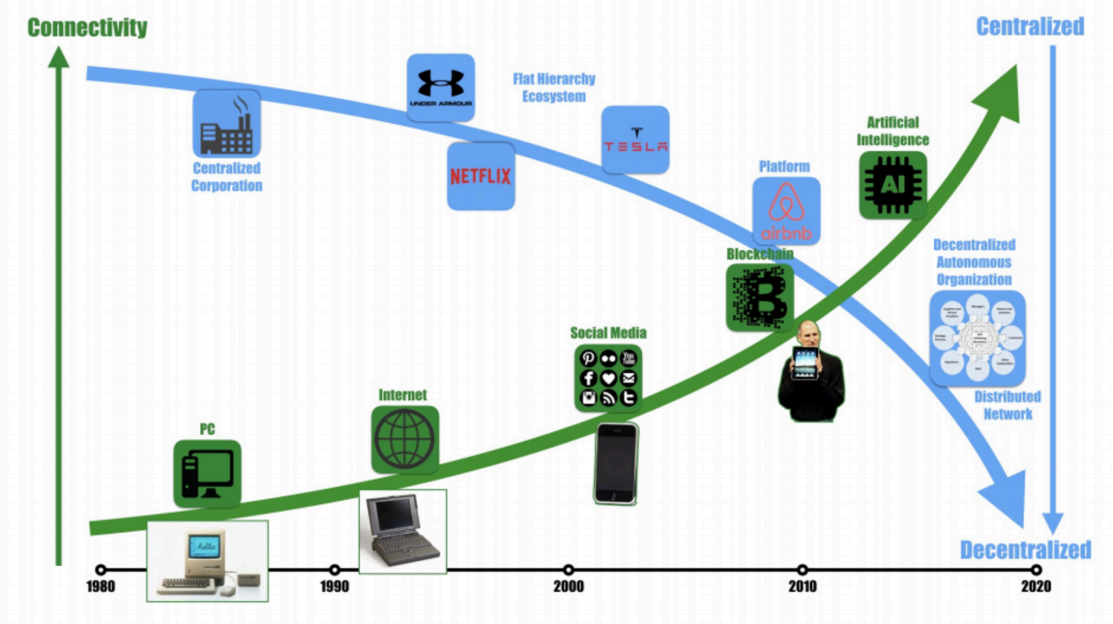


Figure 1: Time Series 1980–2020 societal connectivity and platform decentralization.

Diagram #4

Source: Mark Fenwick, Wulf A. Kaal and Erik P.M. Vermeulen, 'Legal Education in the Blockchain Revolution'[123]

2.3 What is a Blockchain? How does it work?

A Blockchain is a "shared and distributed ledger or database that maintains a continuously growing list of blocks"[124]. The term "Blockchain" is indicative of the way it works: every block is stored in a linear, chronological order, forming a chain of blocks. Every block contains data, whether it is records of

[122] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2009) <https://bitcoin.org/bitcoin.pdf> accessed 21 July 2019.

[123] Mark Fenwick, Wulf A. Kaal and Erik P.M. Vermeulen, 'Legal Education in the Blockchain Revolution' (2017) <https://ssrn.com/abstract=2939127> accessed 21 July 2019.

[124] Quoted in Daniel Drescher, 'Blockchain Basics: A Non-Technical Introduction in 25 steps' (2017) (as cited in Mark Fenwick and Erik P. M. Vermeulen, 'A Primer on Blockchain, Smart Contracts & Crypto-Assets' (2019).

transactions, facts or other information[125]. Each node maintains a copy of the ledger, which is updated in real time as new blocks are created and validated.

It is a distributed technology to the extent that it does not require a central registry system or a single responsible in charge of the system. Instead, the technology relies on a distribution of responsibility among the participants, also called "nodes", which are all connected with each other and store the data simultaneously. In this distributed reality, there is no hierarchical structure between nodes as it happens in a centralized system.

Blockchain is often said to be "immutable". However, this terminology is misleading because, even though it is very difficult to tamper with the chain, it is not impossible. A famous case where advantage was taken of security vulnerabilities was the DAO (Decentralized Autonomous Organization) hack. It is important to bear in mind that the issue did not arise from Ethereum itself, rather it occurred in one application built on Ethereum software, the DAO. It happened in June 2016[126] and 30% of the funds were stolen as a result. The idea behind the DAO project was a virtual venture capital fund, created by Slock.it, and governed by the investors through the DAO structure[127].

2.3 Consensus Protocols

In a traditional centralized database there is a centralized structure responsible for registering the relevant transactions. One must trust the central authority in charge of the record keeping process[128] since the accuracy of the records is intrinsically linked to the responsible(s)' actuation. Therefore, if that individual or organization is trustworthy is of paramount importance. In the same

[125] Mark Fenwick and Erik P. M. Vermeulen, 'A Primer on Blockchain, Smart Contracts & Crypto-Assets' (2019), <https://ssrn.com/abstract=3379443> accessed 3 June 2019.
[126] David Siegel, "Understanding the DAO Attack" (*Coindesk*, 25 June 2016) <https://www.coindesk.com/understanding-dao-hack-journalists> accessed 19 July 2019.
[127] Osman Gazi Güçlütürk, "The DAO Hack Explained: Unfortunate Take-off of Smart Contracts (Medium, 1 August 2018) < https://medium.com/@ogucluturk/the-dao-hack-explained-unfortunate-take-off-of-smart-contracts-2bd8c8db3562>, accessed 3 June 2019. "The attacker(s) managed to recursively call the split function and retrieved their funds multiple times before getting to the step where the code would check the balance. On 16 June 2016, the attacker managed to retrieve approximately 3.6 million Ether from the DAO fund abusing this loophole, which is known as "recursive call exploit".
[128] Jake Frankenfield, 'Consensus Mechanism (Cryptocurrency)' (*Investopedia*, 25 June 2019) < https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp> accessed 21 July 2019.

way there is a single point of control, there is also a single point of failure. Public blockchains, however, facilitate peer-to-peer transactions between peers that do not know each other without involving an intermediary in the operation. Therefore, it is essential to find a mechanism which enables the parties to trust the system, even though they do not trust each other directly, so that they can transact. That is precisely the role fulfilled by the different consensus protocols on the market.

The Proof-of-Work (PoW) protocol is the most famous protocol because it is used by many of the most famous cryptocurrencies, including Bitcoin. In order to add a new block to the chain, a miner has to solve a set of complex mathematical problems – an encrypted puzzle - before all the other miners, which is then verified by the other miners before adopting it. In spite of its high reliability, this protocol is highly inefficient when it comes to spending resources. Given the race to solve the puzzle – the proof-of-work - and be rewarded for it with a new bitcoin, miners compete heavily[129]. The more miners involved, the harder it is to solve the mathematical puzzle, and hence the high energy costs[130]. Moreover, the number of processed transactions per second is substantially lower when compared to players in the market like Visa or Mastercard, in which is known as the scalability problem[131].

Proof-of-Stake (PoS), however, it is described[132] as a low cost alternative because it requires lower resources in comparison with the Proof-of-Work mechanism. It is not dependent of the work performed by the miner, rather it is on a validator's[133] stake in the network[134]. The chances of each validator in the network being chosen to forge a new block varies according to the deposit that

[129] Andrew Tayo, 'Proof of work, or proof of waste?' (*Hackernoon*, 14 December 2017) <https://hackernoon.com/proof-of-work-or-proof-of-waste-9c1710b7f025> accessed 21 July 2019.

[130] For a more complete view on this subject. Luke Fortney, 'Bitcoin Mining, Explained' (*Investopedia*, 25 June 2019) <https://www.investopedia.com/terms/b/bitcoin-mining.asp> accessed 21 July 2019.

[131] Andrew Gazdecki, 'Sidechains: How to scale and Improve Blockchains, Safely' (*Forbes*, 27 November 2018) <https://www.forbes.com/sites/forbestechcouncil/2018/11/27/sidechains-how-to-scale-and-improve-blockchains-safely/#314c7e084418> accessed 21 July 2019.

[132] Jake Frankenfield, 'Consensus Mechanism (Cryptocurrency)' (*Investopedia*, 25 June 2019) < https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp> accessed 21 July 2019.

[133] Proof-of-Stake does not have miners, it has validators. Consequently, new blocks are not mined but forged.

[134] Vbuterin, 'Proof of Stake FAQ' (*GitHub*, 20 March 2019) <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#what-is-proof-of-stake> accessed 21 July 2019.

validator has made – the stake. The higher the stake, the higher the chances. It can be argued that this algorithm is not fair because it favours the rich but this argument can also be refuted because proof-of-stake, unlike proof-of-work, does not allow economies of scale. Thereafter, once a node is chosen to validate the following block, the validator proceeds to the verification of the transactions within the block. After the verification is successfully completed, the new block is added to the chain. The stake also works as a safety measure because the validator has a financial incentive to act with integrity. Otherwise, the validator will lose part of the stake, which will give rise to financial losses.

Another protocol which has recently been discussed is the Zero-Knowledge Proof (ZKP). ZKP is a protocol where one party can provide other parties with the data they need without actually revealing the data itself[135]. What it does is convey to the other parties that they are not being lied to, by minimising that probability. However, that probability will never reach zero. Some cryptocurrencies, such as Zcash, already utilise a variant of this protocol, the zk-SNARKs. The Dutch bank "ING"[136] built another variation called "Zero Knowledge Range Proof"[137], which proves that a given number is comprehended within a certain range without actually revealing the number. One potential application is to demonstrate that one's salary is sufficient to get a loan.

The first two protocols were highlighted here due to their massive adoption. Proof-of-stake, however, is already an example of the alternatives to PoW that Blockchain developers are considering. ZKP is another interesting consensus protocol because of the privacy that it ensures, which can be useful, especially concerning personal data issues.

[135] For a very brief explanation in video format: Simply Explained – Savjee, 'Zero Knowledge Proof – ZKP' (*Youtube*, 14 January 2019) <https://www.youtube.com/watch?v=OcmvMs4AMbM> accessed 21 July 2019.

[136] 'ING launches Zero-Knowledge Range Proof solution, a majpr addition to blockchain technology' < https://www.ingwb.com/themes/distributed-ledger-technology-articles/ing-launches-major-addition-to-blockchain-technology> accessed 22 July 2019.

[137] Tommy Coens, Coen Ramaekers, and Cees van Wijk, 'Efficient Zero-Knowledge Range Proofs in Ethereum' < https://www.ingwb.com/media/2122048/zero-knowledge-range-proof-whitepaper.pdf> accessed 22 July 2019.

2.4 Public vs Private vs Consortium

Concerning Blockchain's design, there is an ongoing discussion over which kind is superior and, as a consequence, must be adopted. On one hand, there are those who advocate in favour of the public and permissionless[138] version of the technology, as it is the one that better embodies decentralization as a philosophy. These are often deemed as "the purists"[139]. In a public and permissionless[140] blockchain, also referred to as a "trustless" network, there is no entity in control of the blockchain. Trust in the system is ensured through the combination of a cryptographic fingerprint – a hash – and a consensus protocol[141].

On the other hand, there are those who consider this vision to be utopic and claim that more pragmatism is needed in order for Blockchain to be adopted and become a mainstream technology. Those prefer a permissioned[142] version/solution of the technology. This can assume the form of a private or a consortium blockchain. The first is controlled by a single entity or individual, where control is clearly centralised. The latter is controlled by a group of approved individuals, where control is distributed among the different participants. This type of Blockchain is very useful for companies interested in collaborating with each other – e.g. for a certain industry – to ensure that all the participants have access to the same information. Unlike public and permissionless blockchains, authorization is required to participate in the system and participants in the network know each other. For this way of thinking – private or consortium - only thus can Blockchain technology be embraced by the masses.

[138] Rahul Sharma, "Public vs Private Permissioned Ledgers and Blockchain Standards", (Forbes, 11 June 2019) < https://www.forbes.com/sites/forbestechcouncil/2019/06/11/public-vs-private-permissioned-ledgers-and-blockchain-standards/#42a996e9550b>, accessed 17 June 2019. ("It's important to note that permissioned – some of the public networks like Stellar and Sovrin are public permissioned networks.")

[139] Accenture, 'Editing the Uneditable Blockchain: Why Distributed Ledger Technology Must Adapt to an Imperfect World' (2016). The pdf can be downloaded at <https://www.accenture.com/us-en/insight-editing-uneditable-blockchain> accessed 5 July 2019.

[140] E.g. Bitcoin and Ethereum.

[141] Mike Orcutt, 'How secure is blockchain really?' (*MIT Technology Review*, 25 April 2018) <https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/> accessed 21 July 2019.

[142] E.g. R3 (Corda) or Hyperledger.

However, both sides believe in this prediction of massive adoption of Blockchain.

The tension between purists and pragmatists is not limited to Blockchain design as evidenced by the DAO hack. Related to that incident, the first argued that "code is law" and, therefore, the actions were legitimate as they were enabled by the code itself. Moreover, they considered that data on the blockchain is perceived as immutable and it should be kept as such, since doing the contrary would constitute a precedent for further situations and harm the Ethereum blockchain in the long term. The latter considered that the community should intervene as the hacker should not be allowed to profit from that situation. Secondly, that it was not a bailout but a mere return of funds to the original owners. As a result, a vote for a hard fork proposal was put in place, a majority was reached and a division happened. As of that moment, two different Blockchains came into existence: the anti-fork Ethereum Classic (ETC) and the pro-fork Ethereum (ETH)[143].

[143] Antonio Madeira, "The Dao, the Hack, the Soft Fork and the Hard Fork", (CryptoCompare, 12 March 2019) < https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/>, accessed 3 June 2019.

Chapter 3: The Right to be Forgotten applied to Blockchain

3.1 Is the GDPR applicable to data stored on a blockchain?

By analysing the GDPR, one will certainly conclude that the GDPR was designed to deal with organisations that operate in silos. All the obligations, duties or exercise of rights were tailored to be directed at a centralized structure, person or entity. On the other hand, Blockchain is a decentralized form of governance. The question is if the GDPR is still applicable to data stored on a blockchain.

A considerable part of the core rules and principles[144] of the GDPR were already present in the Directive 95/46/EC it replaces. The Directive 95/46/EC did not succeed in avoiding fragmentation across the European Union. Hence the need to implement the GDPR. Regulations unlike Directives are directly applicable and therefore more adequate to ensure a consistent legal framework throughout the Union. Differences in the level of protection are seen as obstacles[145] to the free flow of personal data and, consequently, as obstacles to the development of the single market. The GDPR provides a unified legal framework, whose aim is to ensure a level playing field to remove those obstacles and assure an equivalent level of protection in all Member States[146].

In order to determine whether or not a certain set of data falls within the scope of the GDPR, it is necessary, in the first place, to take a look at the definition of 'personal data' provided by the GDPR itself. In that sense, as previously mentioned, it will be considered 'personal data' if a natural person can be 'identified, directly or indirectly' and 'in particular by reference to an identifier such as a name, an identification number, location data' among others.

In addition, it has also been demonstrated that while pseudonymized data still amounts to personal data, since it is possible to trace it back to the person to whom it belongs. However, that reasoning is no longer true in respect to anonymized data given the fact that it does not allow the establishment of that connection.

[144] Such as fair and lawful processing, data minimization or purpose limitation.

[145] GDPR, L 119/2, Recital 9.

[146] *Ibid*, Recital 10.

Consequently, the answer to the question of whether or not data stored on a blockchain amounts to personal data resides on how that very same data is stored on the blockchain. Therefore, it is not possible to provide a "one size fits all" answer, it depends. When data which allows the identification of a natural person directly or indirectly is stored in its original form, it will certainly be qualified as personal data. On the other hand, data can also be stored through some encryption form or by making use of a hash function[147]. Both these cases are considered pseudonymisation[148] techniques rather than anonymization. In the first scenario, 'the holder of the key can trivially re-identify each data subject though decryption of the dataset'[149]. With respect to hashing, even though it cannot be reversed – in contrast with what happens with encryption – it still constitutes a form of pseudonymisation since it is possible to link the data to the data subject – e.g. comparison between possible input values and the values in the dataset or even a brute force[150] attack[151]. In fact, Article 29 Working Party points out that believing that a pseudonymised dataset is anonymised – when it is not - is one of the most common mistakes made by data controllers[152].

Thus, taking into the fact that pseudonymisation is not enough for 'personal data' to be disregarded as 'personal data' and, in addition, that the standard for data to be considered anonymized is high, it is reasonable to conclude that in a large variety of situations GDPR will be indeed applicable.

3.2 Immutability vs Right to be Forgotten

The core of this thesis lies in this point: how to solve the apparent contradiction between the right to be forgotten – provided for in Article 17 GDPR – and the so called immutability of Blockchains. It is fair to say that, at least at

[147] Michèle Finck, 'Blockchains and Data Protection in the European Union' (2017) <https://ssrn.com/abstract=3080322> accessed 18 June 2019.
[148] Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' [2014], 19.
[149] *Ibid.*
[150] *Ibid*.
[151] According to a definition given by Kaspersky, a brute force attack is a trial and error approach where the hackers hope is to guess the relevant information correctly. It can be a password, a username, a key. In order to accelerate the process, hackers have developed different tools to do the job faster. "What's a Brute Force Attack?" <https://www.kaspersky.com/resource-center/definitions/brute-force-attack> accessed 18 July 2019.
[152] *Ibid*, 21.

first glance, they seem to be in profound conflict. If the GDPR is applicable – as already demonstrated that it is – how can immutability be reconciled with the right to be forgotten? This is of huge relevance and might get you to question even if it is worth adopting the technology. Yet, it is worth remembering that the GDPR does not regulate technologies per se[153], in abstract, rather it takes into account how technology is used in a specific context involving personal data.

Immutability in Blockchain is given by the append-only feature, this is, data can only be added to the blockchain, not removed from it. Therefore, data stored this way it is stored in perpetuity as long as it exists. This is why frequently it is referred that, once something is stored on a Blockchain, it is like "it is set in stone". This is, unless the ledger has been corrupted, which is considered to be of an enormous difficulty due to the cryptographic security mechanisms previously described.

Immutability is often thought of as one of Blockchain's most cheered characteristics. However, this is where the friction point with the right to be forgotten emerges – not only the right to be forgotten or even GDPR-related issues, but this thesis is mainly focused on it – and the discussion begins.

On the other hand, Article 17 of the GDPR provides individuals with the right to have their data forgotten in certain circumstances. The problem is that the meaning of the term "forgotten" is yet to be clarified. Does data have to be effectively erased as suggested by a literal reading of the term? Or is it enough to conceal it, as long as the same practical effect is achieved?[154]

Some would argue that, when dealing with this kind of technologies, "*code is law"* and, therefore, this question should not even be posed because these are two different plans. They propose the same approach in relation to smart contracts as a way of dismissing the application of Contract Law. Consequently, if code is law, anything performed under the code would be legal. However, from a legal perspective,– as referred by Zetzsche, Buckley and Arner[155] - this is a

[153] CNIL, 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data' (*CNIL*, 6 November 2018) < https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data> accessed 24 June 2019

[154] Allyson Haynes Stuart, 'Google search results: buried if not forgotten' (2013) <https://ssrn.com/abstract=2343398> accessed 21 June 2019.

[155] Dirk A. Zetzsche/ Ross P. Buckley/ Douglas W. Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2017) EBI Working Paper Series <https://ssrn.com/abstract=3018214> accessed 21 June 2019.

weak argument. It is not because something is written in code rather than in plain text language that it will be legitimized by the Law[156]. Otherwise, it would be an open door to circumvent the application of any piece of Legislation and breach the fundamental values that compose the judicial system[157].

Another line of thought could also reach the same conclusion that the right to be forgotten is not applicable, but following a different trajectory. Arguing that Blockchain and Decentralized Ledger Technologies fall under the "umbrella" of the exemption provided for in Article 17 (2) GPDR: '*taking account of available technology and the cost of implementation*', rather than being considered a no-law zone. In that sense, "Blockchains' inherent limitations", might be a relevant factor since, by nature, Blockchains' architecture and features are often not compatible. By doing so, the immutable chain would be compromised, which would consequently undermine the purpose of adopting Blockchain as a solution since the very beginning. Nevertheless, one might question: if there are blockchain solutions that claim they have found a way of coping with not only GDPR but other regulations as well – and apparently they did – should different standards be used? Isn't that a way of indirectly promoting and, in a certain way, rewarding the non-compliance? Is the aspiration of a fully decentralized scenario – the holy grail of decentralization - enough to justify it?

Differently, an editable blockchain is also being discussed and available in the market. Due to Accenture's backup and development, this proposal has gained traction and Accenture's was even awarded with a patent for their solution. The feature of editability is provided by a new variation of the chameleon hash function[158]. Modification of the blocks is enabled through the use of the chameleon hash key to unlock the link between the block that must be changed and its successor, as illustrated in diagram #5. But, thanks to this mechanism, it is possible to substitute the existent block with a new one without breaking the chain, as it would happen traditionally. Accenture affirms that their invention is

[156] *Ibid*, 'If someone writes code under which the person is entitled to steal others' money, the code will not legitimize theft'.

[157] Here, generally speaking and regardless of which legal system is being considered in a specific case.

[158] Accenture, 'Editing the Uneditable Blockchain: Why Distributed Ledger Technology Must Adapt to an Imperfect World' (2016). The pdf can be downloaded at <https://www.accenture.com/us-en/insight-editing-uneditable-blockchain> accessed 5 July 2019.

designed to preserve the virtues of immutability as well since it is possible to identify which blocks have been changed because of a scar that evidences the alteration and cannot be removed, even by trusted third parties.

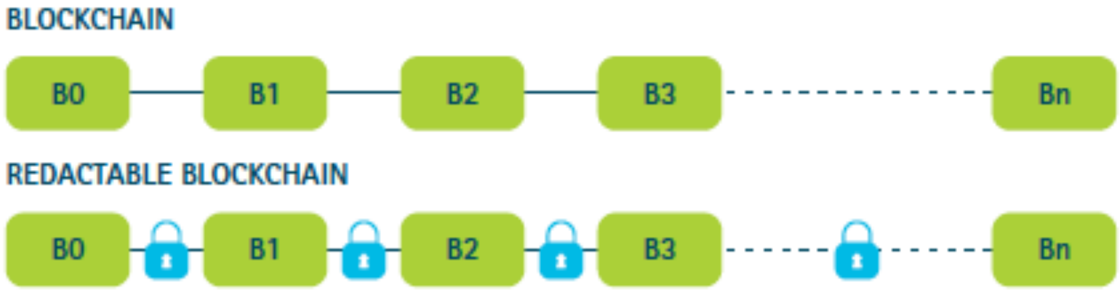


Diagram #5

Source: Accenture[159]

Accenture claims that distributed ledger technologies must adapt to an imperfect world and, in that sense, pragmatism is required. In fact, in their paper, a section is entirely devoted to privacy rights in general, and the right to be forgotten in particular, in an attempt to demonstrate the relevance of the topic and the impacts of being non-compliant. Furthermore, by comparing Blockchain to the Internet in its early days, Accenture draws the parallel between these two to illustrate the kind of development that Blockchain might experience if massively adopted – and, in their view, the way to massive adoption is done by embracing the editable blockchain. They argue that, without this feature that enables modifications or data to be taken away from the ledger, there is an imperative for coders to write perfect code every time - which does not meet reality. Also, an alternative situation of mischief might happen, with undesirable data ending up stored in perpetuity in a Blockchain. Often, when one thinks about it, a wrong credit rating score and the consequences it might have on a certain person is frequently given as an example. However, Accenture illustrates not only with human situations, but with mischief behaviour as well. Situations where somebody, deliberately, acts in order to create harm or trouble, for instance, in 2013, it was discovered pornography[160] embedded in metadata on Bitcoin's

[159] *Ibid*.

[160] *Ibid*.

blockchain. It would not be problematic if it was not for its immutability. Additionally, it is argued that the editable blockchain saves both time and resources, especially, as transactions become more complex. More adoption represents more transactions per second, and more transactions per second entail more processing power, and also larger storage capacity. Hence the need to preserve time and resources in order to achieve scalability[161], a major issue[162] with blockchain solutions.

Additionally, the adoption of this solution requires the designation of a person or a group in charge of managing the system. The challenge then will be to design the appropriate governance structure to deal with this situation, transposing the best practices in traditional corporate governance to this particular situation. This is, which checks and balances need to be put in place; who has permission to make changes; in which circumstances, among other questions.

3.3 Transposing data controllers and processors to Blockchain

In relation to the application of the GDPR, another issue arises: who assumes the different roles listed in the GDPR? Sometimes, defining data controllers, processors or joint controllers may be a hard task to achieve in concrete cases. Furthermore, difficulty has increased exponentially due to decentralization, especially in public and permissionless blockchains, where participants do not know each other and come and go whenever it suits their needs. In that sense, the French Data Protection Authority – *Commission nationale de l'informatique et des libertés (CNIL)* – has already issued guidance[163] on the interplay between these two and realities, having dedicated special attention to the qualification of the participants in the blockchain[164].

[161] *Ibid*.

[162] Connor Blenkinsop, 'Blockchain's Scaling Problem, Explained' (*CoinTelegraph*, 22 August 2018) <https://cointelegraph.com/explained/blockchains-scaling-problem-explained> accessed 18 July 2019.

[163] CNIL, 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data' (*CNIL*, 6 November 2018) < https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data> accessed 24 June 2019

[164] That guidance will not be addressed here, but in the next chapter instead to avoid unnecessary repetitions.

Being able to determine who assumes these roles when facing a decentralized structure is absolutely essential. In order to fully understand the reach and practical relevance, it is useful to perform a comparative exercise between the existent reality and an alternative where those roles do not exist.

As an example, these are two very pertinent questions one might ask: to whom do data subjects turn to in order to exercise their rights? Who is held responsible in cases where sanctions are applied?

These two very basic questions, however, do not have two correspondent easy answers. Yet, without them, it is not possible to ensure data subjects a complete protection of their lawfully granted rights, and certainly not enforce them. In this regard, data protection authorities taking the lead, as CNIL did in France, must be praised. Such measures actively contribute to put the topic in the order of business and consequently generate more discussion around it, propelling us to find new solutions.

The CNIL's guidance and the aforementioned questions will be looked at in greater detail in the next chapter.

Chapter 4: Critical analysis

Despite the technological character of this analysis, the main focus cannot be disregarded, that is, this is a juridical analysis of the reality in question. Thus, it is now time to subsume the facts to the applicable law and see which solutions are compliant and which are not.

Starting with the qualification of the participants in the blockchain, the CNIL's guidance will be used as the basis for the discussion. It is obvious that the GDPR was clearly designed having in mind a paradigm of centralization (namely, centralized data management) where exist well-defined roles, which is basically the way traditional companies have been organized so far. In that sense, it is fair to say that when the GDPR was enacted and more recently came into effect, it was already outdated. Blockchain, as the underlying technology of Bitcoin, became famous precisely because of the decentralization it brought into the market, as a way to bypass intermediaries.

From CNIL's perspective, a participant is a data controller when: (i) is a natural person and that the personal data processing operation is related to a professional or commercial activity; (ii) is a legal person and that it registers personal data in a blockchain. In a private or consortium case, this will often be the case but, in a public blockchain, to what extent is this still true? According to Article 29 Working Party Guidelines, 'the concept of a controller is a functional concept'[165] (…) 'and thus based on a factual rather than a formal analysis'.

That being said, several participants would be considered data controllers under CNIL's orientations. Yet, a very valid question is if each data controller, individually, is able to exercise an effective control over how data is processed, 'determining the purposes and the means'. The lack of a centralized decision structure points in the direction of a negative answer because, if an individual cannot control and influence the ledger on his own, how is it possible to affirm that he/she determines the purposes and the means of processing like a data controller does? A possible counterargument is: even if they do not determine it individually, they can still be considered joint controllers under Article 26 GDPR

[165] Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor" [2010].

due to the collective nature of their actions. Again, a more in-depth reasoning is necessary. If it is true that the allocation of responsibilities does not necessarily have to be equally split, it is also true that an agreement on that topic must be achieved. Article 26 (1) GDPR prescribes that 'they shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this regulation'[166]. However, it presumes some sort of collective action, such as the one found in a contractual arrangement, which is not the case. Instead of having participants acting together, in explicit and coordinated manner, participants act individually and usually there is no coordination between them. As referred by Michèle Finck, 'they don't determine the modalities of data processing of other nodes'[167]. Reason for which, in comparison, the interpretation of the Article 29 Working Party, based on the factual elements and circumstances of the case, is preferable given that it reflects better the reality it pretends to regulate.

Nevertheless, some forms of organization can be found, namely, mining pools, where different miners get together and cooperate in order to increase their chances of finding a block[168]. Working on their own, miners' chances of finding a block and be rewarded for their work would be substantially lower. This way, even though miners do not receive the total amount, the trade-off is that they receive a portion of that same total, on a more regular basis, according to the way the division was structured, proportional or not[169]. The irony in this form of organization is patent since public blockchains are perceived by the public as fully decentralized and hailed for it, and find themselves moving towards a form of centralization, the mining pools.

Therefore, the question of whether or not, some economic agent may be considered a *data controller* under the GDPR when dealing with Blockchains cannot be answered with a rule of thumb. The functional approach proposed by Article 29 Working Party is not limited to theoretical discussion. On the contrary,

[166] GDPR, L 119/48, art. 26 (1).

[167] Michèle Finck, 'Blockchains and Data Protection in the European Union' (2017) <https://ssrn.com/abstract=3080322> accessed 24 June 2019.

[168] E.g. Bitcoin mining pools, many of them in China, where electricity is cheaper as this activity is very resource consuming.

[169] For more information regarding the different configurations that mining pool rewards can assume, 'What are Bitcoin Mining Pools?' < https://www.coindesk.com/information/get-started-mining-pools> accessed 17 June 2019.

it has massive practical implications as *data subjects* will turn to *data controllers* in order to exercise their lawfully granted rights. Moreover, it is also a way of assigning liability. Consequently, a case by case assessment is necessary. Where in a private and permissioned blockchain, identifying the participants and which role each one of them fulfills should not offer special difficulty, in a public blockchain, the scenario is not so clear and requires more thought. Although, it does not seem directly applicable, the truth is that the GDPR, as well as other laws, were designed for the typical centralized organizational structure. In this decentralized/distributed model, consensus can be reached in different manners, and it cannot be ruled out from the beginning the possibility that a court will conclude in favor of some sort of coordinated action. The rules are known by its participants, knowing the rules they decide to participate, all of them contribute to the maintenance of the system and, *mutatis* mutandis, it is possible that - in some cases - a court may consider this a form of joint control[170].

It is important to bear in mind that, from a juridical point of view, the practical difficulties of the enforcement shall not be mistaken with the potential applicability of the law to a concrete case. Some scholars, such as Zetzsche, Buckley and Arner, have already proposed some viable alternatives to provide companies and other organizations with more legal certainty, helping them navigate this new paradigm and avoid or limit potential liabilities. However, their solution of creating a legal structure within controlled entities of a conglomerate or a joint venture in case multiple parties are involved, is good for companies, but does not solve the issue of public permissionless blockchains. Notwithstanding, from a big company point of view, where potential damages can assume massive proportions, this prudent approach is recommended and it is very likely that a private or consortium blockchain is more adequate to their business needs. But, as technology and law mature in the light of new developments[171], the forecasts are that both regulating and providing legal advice on this matters will get easier.

[170] Dirk A. Zetzsche/ Ross P. Buckley/ Douglas W. Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2017) EBI Working Paper Series <https://ssrn.com/abstract=3018214> accessed 26 June 2019.

[171] Erik P.M. Vermeulen, 'Want to Understand Blockchains? Start Experimenting' (*Hackernoon,* 25 November 2017) < https://hackernoon.com/want-to-understand-blockchains-start-experimenting-bdc5aeaf2d07> accessed 19 July 2019. As a consequence of a fruitful dialogue

Meanwhile, in relation to the interplay with the right to be forgotten, the following must be said. The right to erasure or right to be forgotten, codified in Article 17 GDPR, is one of the hot topics regarding privacy and data protection due to its many friction points. However, it cannot be forgotten that this right is not absolute and it can only be exercised if, at least, one of grounds provided for in Article 17 (1) is applicable. Moreover, it is subject to many exemptions – article 17 (3).

Immutability is indeed one of the features that has made Blockchains so desirable. It is due to this characteristic that Blockchains are perceived as highly reliable and able to function without requiring the intervention of a trusted third party. Notwithstanding, immutability entails some difficulties too. Not only does it concern the right to be forgotten, but the right to rectification as well.

With regards to the first argument that "code is law" and that the Law is not applicable, it could not be in more profound disagreement with the view of this thesis. The Law applies irrespective of the support in which such solution is contained. As referred by Zetzsche, Buckley and Arner, 'If someone writes code under which the person is entitled to steal others' money, the code will not legitimize theft'[172]. The consequences of this line of reasoning are perverse and dangerous. Considering the DAO event, in particular the hard fork discussion, it was referred back then that the community should not intervene since the actions were allowed by the code itself, and that by doing so it would open a precedent that could damage the Ethereum Blockchain in the long term. It is clear that the Law must prevail and that a situation like this cannot be allowed. The primary function of the Law is not to ensure efficiency measures or viable business models while sacrificing its core values. As mentioned by Diogo Pereira Duarte[173]:

> The pretension of replacing the Law, its language and its solutions, developed over millennia, as an intrinsically human reality, by the strict application of

and experimentation, the various stakeholders and participants in the ecosystem will foster new legal solutions, properly applying the Law to new technologies, as it is the case of Blockchain.

[172] Dirk A. Zetzsche/ Ross P. Buckley/ Douglas W. Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2017) EBI Working Paper Series <https://ssrn.com/abstract=3018214> accessed 26 June 2019.

[173] Diogo Pereira Duarte, '"Smart Contracts" e intermediação financeira', in António Menezes Cordeiro and Ana Perestrelo de Oliveira and Diogo Pereira Duarte (coord) *Fintech II – Novos Estudos sobre Tecnologia Financeira* (2019).

> programming, by the *code is law*, would be an unprecedented civilizational regression.[174]

The same reasoning applies to harmful consequences brought by immutability. The ‘garbage in, garbage out’ problem is an example of that. Immutability can be extraordinary but only to the extent of the quality of its data. When the information stored in a Blockchain is not accurate, the friendly view of immutability gives place to a problem in need for a solution. Therefore, the “code is law” view, where code is sovereign among the system participants, must be rejected. Code is not paramount and it cannot operate irrespective of the formally enacted laws.

Secondly, it has been promoted a solution where blockchains, due to its inherent limitations, do not have to comply with Article 17(1) GDPR since they are exempted by paragraph 2 of the same Article. However, such proposal results from a wrongful reading of Article 17(2) GDPR. The referred article prescribes that:

> where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

From this reading derive two essential conclusions: (1) the Article is referring to the duty that the controller has of informing other controllers, it is not referring to processors on his behalf; (2) the consideration of the “available technology and the cost of implementation” is in relation to that communication by the controller to other controllers, not an exemption that allows the controller to disregard the application of Article 17(1) GDPR. Therefore, this is not a valid solution to overcome this issue.

A third solution that has been proposed is the usage of both on-chain and off-chain storage. This solution does not appear to be present major problems complying with the law since personal data is either stored off-chain and only non-personal data is on-chain. Another possible off-chain solution is to use

[174] Free translation.

Blockchain merely to hold the proof that data is valid[175]. Therefore, if need be, data can easily be modified or deleted, as it is not stored on the blockchain itself. This way, immutability is preserved and GDPR compliance is achieved. With regards to technological arguments, it can be argued that off-chain storage is closer to an imperative than a choice, solving the necessity of storage and making scalability easier. While on the other hand, it can be argued that the durability provided by the chain is lost because data is no longer on chain. Be that as it may, this is a good question for thought and that is not possible to discuss in more depth in this thesis.

The last solution being analysed here is the debatable idea of an editable blockchain. This solution is indeed very controversial and it is even considered by some within the Blockchain community the destruction of this technology. In a first analysis, the great virtue of this technology is the immutability that it ensures. Consequently, an editable Blockchain appears to be a contradiction that renders the adoption of the Blockchain useless. Nevertheless, that is precisely the argument of its proponents, namely, the consulting firm Accenture. Accenture's view relies on the assumption that pragmatism is key in order for Blockchain to succeed as the idealistic view will not work.

In this thesis, solutions have been discussed, some public some private, some more decentralized than others. In this case, Accenture is proposing a model – for which they have been awarded a patent – that works as a private/consortium permissioned blockchain. Up to this point, there is nothing new. It has already been discussed here on this occasion. The innovation is the editability of the blockchain managed through the use of chameleon hashes. However, an entirely reasonable, yet powerful argument is mentioned, which is also related with the "garbage in, garbage out" problem. That argument is the inevitable human error inherent to any kind of human action, but also mischief and privacy laws, which are being discussed here. Consequently, if human error is unavoidable, this appears to be a useful – or even necessary – mechanism.

Hence, it is worth mentioning the conditions in which the modification or erasure is allowed. The governance structure that is required, i.e., the system

[175] Michèle Finck, 'Blockchains and Data Protection in the European Union' (2017) <https://ssrn.com/abstract=3080322> accessed 26 June 2019.

administrators and the permissions granted to each one of them, the circumstances in which they can be exercised has now become a vital element of the equation with the reintroduction of a trusted third party. The challenge here is not how to enforce the right to be forgotten anymore, but to guarantee that the system is not an open door for unauthorized changes, compromising the trust that is placed in this system. Concerning the system's different view on immutability, whether or not it will work, only time will tell. However, the system is clearly not immutable in the sense that a Bitcoin blockchain is immutable. Accenture's architecture is only immutable until it is not anymore. This means, as Accenture properly recognizes, that their Blockchain solution is only partially immutable. On one hand it is immutable. On the other hand, it allows modifications under certain circumstances. However, the real question is if the "scar" that is left everytime that the system is amended is enough to provide the same trust in the system that pure immutability does.

Notwithstanding, it is worth mentioning that this kind of technology – the editable blockchain – is only suitable for private blockchains, where the participants know each other. In contrast, it is not possible to apply it to public and permissionless blockchains such as the ones underlying cryptocurrencies – e.g. Bitcoin – given the fact that the immutability of the ledger, provided by the different consensus mechanisms put in place to ensure it, is indeed what creates trust in a trustless network[176]. From a legal standpoint, the editable blockchain enables its participants to be fully compliant because due to the combination of private network environment and editability. This proposal is fully aligned with the principles set forth in the GDPR – e.g. privacy by design - it has its merits regardless of all the debate around it.

Last but not least, reference has to be made to the evolution of cryptography techniques because as they become increasingly more sophisticated, standards will have to be redefined. For example, it is not hard to foresee a Court or Data Protection Authority considering that a given cryptographic technique is so sophisticated that it meets the requirements, when a data subject exercises his/her right to be forgotten.

[176] Ana Perestrelo de Oliveira, '"Direito ao apagamento dos dados ou "direito a ser esquecido"', in António Menezes Cordeiro and Ana Perestrelo de Oliveira and Diogo Pereira Duarte (coord) *Fintech II – Novos Estudos sobre Tecnologia Financeira* (2019).

Conclusion

Throughout this thesis, a variety of aspects regarding the relation between Data Protection, mainly the right to be forgotten, and Blockchain technology were analyzed. Yet, it is useful to identify its limitations beforehand in order to present a more accurate overview. This thesis was never intended to be an exhaustive analysis of the technological intricacies of this subject. Nonetheless, it is unquestionable the technological character of this topic and, therefore, it was performed in the best possible way. In that sense, the section regarding the consensus mechanisms is deliberately shorter than others which were more developed. This decision was made conscious that the reader will certainly find more clear and detailed information when researching about this topic in other papers or even generally searching on the Internet.

Another topic whose resolution is still pending is a more in-depth analysis of the role of controllers and processors, one that performs a thorough analysis on that matter, regarding the most common Blockchain architectures. However, that topic alone, which has tremendous practical relevance, has enough material for a complete study.

Still on the subject of recognizing the thesis' limitations, special consideration must be given to governance structures. Despite the importance of this topic, the challenging task of proposing the appropriate checks and balances for a governance structure would be material for another complete master thesis. In that sense, although it is a very interesting research question, any attempt to solve it in such a short space would not be adequate. Therefore, it is better to reserve it for another occasion.

At a certain point in their paper[177], Zetzsche, Arner and Buckley, referred that "Part of the thrill of blockchain to date has been its disregard of the law" and that was part of the reason that motivated the option for this topic when writing this thesis. Their statement does not do justice to all the developers, *latu sensu*, concerned with the legal implications of their actions and that have actively tried to find solutions to ensure compliance. However, the first aspect cannot be

[177] Dirk A. Zetzsche/ Ross P. Buckley/ Douglas W. Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2017) EBI Working Paper Series <https://ssrn.com/abstract=3018214> accessed 3 July 2019.

disregarded. As any law practitioner, law student or even an informed average person would know, the ignorance of the law or its wrong interpretation does not qualify as a defence for not complying, nor as an exemption for its penalties. As a matter of fact, that is expressly stated in the Civil Code[178], right next to other master basic rules of any legal system. Thus, it is precisely in this gap that this modest contribute is of use, in this recent area where many legal uncertainties still exist, and an additional effort is required, combining legal knowledge and creativity, to adapt the traditional legal framework to the most recent innovations.

This study started with an overview of the General Data Protection Regulation, which covered the general aspects, such as the historical evolution, the scope of application, the definition of personal data, and also the main innovations it introduced. Some correlated hot topics such as the duality between the right to be forgotten and freedom of expression were also addressed. The conclusion is that, even though limits to the fundamental right of freedom of expression have been largely debated in relevant literature over the years, it is always interesting to revisit this topic from a new prism, in the light of new developments such as new technologies. Which leads to the first set of conclusions. In first place, that the scope of application of the GDPR – material and territorial – is so vast, it touches so many areas and so many geographies, that it is comprehensible all the attention it has attracted before and after coming into effect. In second place, with regards to the interrelation between freedom of expression and the right to be forgotten, the intensity of the debate is much stronger in the United States than it is in Europe. As to whether or not the freedom of expression in its core as a fundamental right, whether entities like Google are transformed in censors-in-chief, will depend on how it is applied in practice. The own GDPR recognizes freedom of expression as an exception to the right to be forgotten, among others. Consequently, it is possible to conclude that the right to be forgotten it is not an absolute right[179].

Concerning the disruptive Blockchain technology, it is undeniable that society is in the presence of one of, if not the most, transformative technology that has been developed since the massification of the Internet. It has the potential to be used in a wide range of businesses and services, and even

[178] Article 6, from the Civil Code (*Código Civil*)

[179] GDPR, L 119/2, Recital 4.

reshape the way we conceive organizations in its more distributed form. There are even some authors challenging or, at least, questioning themselves if this kind of decentralized scenarios do not undermine our governmental bodies. In the chapter dedicated to it, an attempt was made to explain what the trendy blockchain is, how it works, the different types of blockchain. That explanation was included in order to grant some background and the basic knowledge necessary to proceed to the core of this thesis: the application of the right to be forgotten to blockchain technologies.

In that respect, the GDPR is indeed applicable to blockchain technology. The technology, per se, is in that regard neutral. What determines the applicability is the processing of personal data, hence, as long as personal data is being processed, the GDPR will be applicable.

Thereafter, it was followed by the critical analysis. This was a chapter that required much thought, demanding a critical view in order to evaluate the different argumentations, its coherence, its flaws, and separate those which make sense from those which do not.

Both public and private blockchains deserve credit. For the time being, private blockchains appear to be more “realistic”, more aligned with the company organization, easier to comply with the existent regulations and business demands and, consequently, seems more poised for mass adoption. However, this is only true in relation to an “enterprise-reality”, i.e., the form of organization adopted by traditional companies, influenced by the way this companies organize themselves and their activities, such as a bank or an oil company. One must not disregard public blockchains as they present huge potential for development. As a matter of fact, the true peer-to-peer networks, where individuals connect with each other directly will most likely happen in a public blockchain. Once technology is mature enough, once a proper governance model is sufficiently developed, it is expectable that more and more working solutions of this kind will appear.

Over the course of this thesis, the reader might get the idea that private blockchains are favored over public blockchains. That is not the real purpose of this work. When reading this thesis, one cannot disregard the context in which it was written. This thesis’ aim is to take into consideration the great variety of existent realities and look at them, today, from a legal perspective, meanwhile, setting the eyes in the future and acknowledging that further developments will arise. In that regard, if traditional corporations disregard the disruption by these new models[180], they might be surpassed and even become obsolete. History is full of examples of companies who were not fast enough or who did not move at all and that have gone bankrupt as a consequence. The platform economy[181] is already a flatter form of organization, more decentralized, and is facilitating peer-to-peer communication.

It is, hereby, rejected the view that it is either public or private blockchains, as if they were opponents and could not coexist. On the contrary, as previously referred, both public and private blockchains deserve credit. Each variant of the technology – public, private, or a hybrid – will be considered adequate or not depending on the matter in question. The conclusion is that a "one size fits all" approach is not correct. The syndicated loan between the bank BBVA[182], as the sole bookrunner, and Red Eléctrica Corporácion is a perfect example where theory meets practice and has to adapt to its demands. The solution adopted by the parties had to meet and combine the specificities of each phase. During the negotiation phase, every step was recorded in a private blockchain network (Hyperledger). Thus, all the nodes participating in it find themselves in the possession of the relevant information – the same as their peers. However, once the contract is signed (or was signed), "a unique document identifier is recorded in Ethereum's public blockchain network (specifically in its test network, 'testnet') to guarantee its immutability against third parties while safeguarding its confidentiality at all times"[183].

That being said, the conditions to answer the research question of this thesis - "What are the implications of the "Right to be Forgotten" in a Blockchain technology solution?" – are now gathered. Once more, there is not a "one size fits all" recipe, it depends. Interestingly, the solution lies in 4 questions that must be asked beforehand: (i) What is the problem that is trying to be solved? It is essential to consider this not only when addressing personal data but any

[180] Mark Fenwick, Wulf A. Kaal and Erik P.M. Vermeulen, 'Why Blockchain' Will Disrupt Corporate Organizations' (2018) <https://ssrn.com/abstract=3227933> accessed 2 July 2019.
[181] Mark Fenwick, Joseph A. McCahery, Erik P.M. Vermeulen, 'The End of 'Corporate Governance': Hello 'Platform Governance'' (2018) <https://ssrn.com/abstract=3232663> accessed 2 July 2019.
[182] 'BBVA signs world-first blockchain-based syndicated loan arrangement with Red Elétrica Corporación', <https://www.bbva.com/en/bbva-signs-world-first-blockchain-based-syndicated-loan-arrangement-with-red-electrica-corporacion/> accessed 2 July 2019.
[183] *Ibid*.

problem in general; (ii) Is Blockchain really necessary to solve this problem or is there a better solution available? Blockchain is indeed a technology breakthrough but, in many cases, it will not be the best solution to implement; (iii) Is personal data being processed? – and, in this regard, it is absolutely crucial to take into consideration the exemptions provided for in Article 17(3) GDPR as well as any other applicable legislations because they might determine that the right to be forgotten is not applicable. Consequently, in a case, where it is possible to be sure that this situation is completely off limits, that will determine if there is necessity to implement certain measures; (iv) if personal data is being processed – after the careful evaluation that has been just mentioned – which system architecture/which solution is more adequate, bearing in mind the necessity to comply with the different applicable regulations, including but not limited to the GDPR?

To conclude, the right to be forgotten does not have to be an insurmountable obstacle to the adoption of blockchain as a solution and neither does the immutability of the blockchain. Instead, during the conception and development of these and other kinds of tech solutions, it is wise to make use of an interdisciplinary group[184], where a member with a legal background is included, rather than a team entirely composed by people with a single background – e.g. engineering – that might come to a solution that is perfectly adequate from an engineer standpoint, but that faces obvious legal issues.

[184] Mark Fenwick, Wulf A. Kaal and Erik P.M. Vermeulen, 'Legal Education in the Blockchain Revolution' (2017) <https://ssrn.com/abstract=2939127> accessed 20 July 2019.

Bibliography

Articles

Allyson Haynes Stuart, 'Google search results: buried if not forgotten' (2013) <https://ssrn.com/abstract=2343398> accessed 21 June 2019.

Ana Perestrelo de Oliveira, '"Direito ao apagamento dos dados ou "direito a ser esquecido"', in António Menezes Cordeiro and Ana Perestrelo de Oliveira and Diogo Pereira Duarte (coord) *Fintech II – Novos Estudos sobre Tecnologia Financeira* (2019).

Andrew O'Connell and Walter Frick, "You've Got the Information, But What Does it Mean? Welcome to 'From Data do Action'" (2014) HBR, 1.

Diogo Pereira Duarte, '"Smart Contracts" e intermediação financeira', in António Menezes Cordeiro and Ana Perestrelo de Oliveira and Diogo Pereira Duarte (coord) *Fintech II – Novos Estudos sobre Tecnologia Financeira* (2019).

Dirk A. Zetzsche/ Ross P. Buckley/ Douglas W. Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2017) in *EBI Working Paper Series* <https://ssrn.com/abstract=3018214> accessed 21 June 2019.

European Union Agency for Fundamental Rights and Council of Europe, 'Handbook on European data protection law' (2018)

Franz Werro, "The Right to Inform v. The Right to be Forgotten: A Transatlantic Clash" (2009) in *Liability in the Third Millennium* 285, <https://ssrn.com/abstract=1401357> accessed 4 May 2019.

Hans Graux, Jef Ausloos and Peggy Valcke, "The Right to be Forgotten in the Internet Era" (2012).

Jeffrey Rosen, "Symposium Issue: The Right to be Forgotten" (2012) in *SLR*, 64.

Marcella Atzori, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?" (2015), <https://ssrn.com/abstract=2709713> accessed 15 May 2019.

Mark Fenwick and Erik P. M. Vermeulen, 'A Primer on Blockchain, Smart Contracts & Crypto-Assets' (2019), <https://ssrn.com/abstract=3379443> accessed 3 June 2019.

Mark Fenwick, Joseph A. McCahery, Erik P.M. Vermeulen, 'The End of 'Corporate Governance': Hello 'Platform Governance'' (2018) <https://ssrn.com/abstract=3232663> accessed 2 July 2019

Mark Fenwick, Wulf A. Kaal and Erik P.M. Vermeulen, 'Legal Education in the Blockchain Revolution' (2017) <https://ssrn.com/abstract=2939127> accessed 20 July 2019.

Mark Fenwick, Wulf A. Kaal and Erik P.M. Vermeulen, 'Why Blockchain' Will Disrupt Corporate Organizations' (2018) <https://ssrn.com/abstract=3227933> accessed 2 July 2019.

Michèle Finck, 'Blockchains and Data Protection in the European Union' (2017) <https://ssrn.com/abstract=3080322> accessed 18 June 2019.

Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2009) <https://bitcoin.org/bitcoin.pdf> accessed 16 July 2019.

Case Law

Case C-518/07, *European Commission v. Federal Republic of Germany* EU:C:2010:125

Case C-288/12, *European Commission v. Hungary* EU:C:2014:237

Case C-614/10*, European Commission v. Republic of Austria* EU:C:2012:631

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

Case C-362/14, *Maximilliam Schrems v. Data Protection Commissioner* EU:C:2015:650

Justia Law. (2019). *Florida Star v. B.J.F., 491 U.S. 524 (1989)*. [online] Available at: https://supreme.justia.com/cases/federal/us/491/524/ [Accessed 4 May 2019].

Justia Law. (2019). *Reno v. American Civil Liberties Union, 521 U.S. 844 (1997)*. [online] Available at: https://supreme.justia.com/cases/federal/us/521/844/ [Accessed 4 May 2019].

Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland no 931/13 (ECtHR, 27 June 2017).

Guidelines

Article 29 Working Party, "Guidelines on Data Protection Officers ('DPOs')" [2017].

Article 29 Working Party, "Guidelines on Personal data breach notification under Regulation 2016/679", WP250, [2017].

Article 29 Working Party, "Guidelines on the implementation of the CJEU judgment on "*Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*", C-131/12 [2014].

Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' [2014]

Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor" [2010].

CNIL, 'Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data' (*CNIL*, 6 November 2018) < https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data> accessed 24 June 2019.

Legislation

Article 6, from the Civil Code (*Código Civil*)

Charter of Fundamental Rights of the European Union [2012] OJ C 326/397

Consolidated Version of the Treaty on European Union [2016] OJ C 202/19.

Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995]

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016].

Treaty of Lisbon [2007] C 306/12.

Others

Accenture, ‘Editing the Uneditable Blockchain: Why Distributed Ledger Technology Must Adapt to an Imperfect World’ (2016). The pdf can be downloaded at <https://www.accenture.com/us-en/insight-editing-uneditable-blockchain> accessed 5 July 2019.

Aliya Ram, ‘Facebook appeals against UK fine over Cambridge Analytica’ (Financial Times, 21 November 2018) <www.ft.com/content/2af83cd4-eda3-11e8-89c8-d36339d835c0> accessed 22 April 2019.

Andrew Gazdecki, ‘Sidechains: How to scale and Improve Blockchains, Safely’ (*Forbes*, 27 November 2018) <https://www.forbes.com/sites/forbestechcouncil/2018/11/27/sidechains-how-to-scale-and-improve-blockchains-safely/#314c7e084418> accessed 21 July 2019.

Andrew Tayo, ‘Proof of work, or proof of waste?’ (*Hackernoon*, 14 December 2017) <https://hackernoon.com/proof-of-work-or-proof-of-waste-9c1710b7f025> accessed 21 July 2019.

Antonio Madeira, “The Dao, the Hack, the Soft Fork and the Hard Fork”, (CryptoCompare, 12 March 2019) < https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/>, accessed 3 June 2019.

‘BBVA signs world-first blockchain-based syndicated loan arrangement with Red Elétrica Corporación’, <https://www.bbva.com/en/bbva-signs-world-first-blockchain-based-syndicated-loan-arrangement-with-red-electrica-corporacion/> accessed 2 July 2019.

Cecilia Kang, ‘F.T.C. Approves Facebook Fine of About $5 Billion’ (New York Times, 12 July 2019) <https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html> accessed 17 August 2019.

Connor Blenkinsop, ‘Blockchain’s Scaling Problem, Explained’ (*CoinTelegraph*, 22 August 2018) <https://cointelegraph.com/explained/blockchains-scaling-problem-explained> accessed 18 July 2019.

David Siegel, “Understanding the DAO Attack” (*Coindesk*, 25 June 2016) <https://www.coindesk.com/understanding-dao-hack-journalists> accessed 19 July 2019.

David Smith oral contribution to ‘EU Internet Regulation after Google Spain’ report of proceedings (27/3/2015) from the University of Cambridge, <https://www.cels.law.cam.ac.uk/sites/www.law.cam.ac.uk/files/images/www.cels.law.cam.ac.uk/documents/google_spain_conference_report_-_16.12.2015.pdf> accessed 26 June 2019.

Emily Barwell, ‘Big Data – Understanding the Risks’ (*Lexology,* 4 April 2018) <https://www.lexology.com/library/detail.aspx?g=bd810ed1-af5b-44b4-bc68-577e23e21ab4> accessed 18 July 2019.

Erik P.M. Vermeulen, ‘Want to Understand Blockchains? Start Experimenting’ (*Hackernoon,* 25 November 2017) < https://hackernoon.com/want-to-understand-blockchains-start-experimenting-bdc5aeaf2d07> accessed 19 July 2019.

“EU General Data Protection Regulation” <www.dlapiper.com/en/us/focus/eu-data-protection-regulation/background/> accessed 28 April 2019

Hannah Murphy and Khadim Shubber, ‘Facebook under criminal investigation over data deals’ (Financial Times, 14 March 2019) <www.ft.com/content/d7e5a96c-45f6-11e9-b168-96a37d002cd3> accessed 22 April 2019

Jake Frankenfield, ‘Consensus Mechanism (Cryptocurrency)’ (*Investopedia*, 25 June 2019) < https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp> accessed 21 July 2019.

James Vincent, ‘Google ‘fixed’ its racist algorithm by remong gorillas from its image-labeling tech’ (*The Verge*, 12 January 2018) <https://www.theverge.com/2018/1/12/16882408/google-racist-gorillas-photo-recognition-algorithm-ai> accessed 18 July 2019.

Jason Silverstein, ‘Hundreds of millions of Facebook user records were exposed on Amazon cloud server’ (CBS News, 4 April 2019) <www.cbsnews.com/news/millions-facebook-user-records-exposed-amazon-cloud-server/> accessed 22 April 2019

Jon Porter, ‘Google fined €50 million for GDPR violation in France’ (The Verge, 21 January 2019) <www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil> accessed 22 April 2019

Julia Carrie, ‘Hundreds of millions of Facebook records exposed on public servers – report’ (The Guardian, 3 April 2019) < www.theguardian.com/technology/2019/apr/03/facebook-data-public-servers-amazon> accessed 22 April 2019

Linklaters, “The General Data Protection Regulation, A Survival Guide”, version 2.0.

Luke Fortney, ‘Bitcoin Mining, Explained’ (*Investopedia*, 25 June 2019) <https://www.investopedia.com/terms/b/bitcoin-mining.asp> accessed 21 July 2019.

Mike Orcutt, ‘How secure is blockchain really?’ (*MIT Technology Review*, 25 April 2018) <https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/> accessed 21 July 2019.

‘New EU rules on e-commerce’ <https://ec.europa.eu/digital-single-market/en/new-eu-rules-e-commerce> accessed 20 August 2019.

Osman Gazi Güçlütürk, “The DAO Hack Explained: Unfortunate Take-off of Smart Contracts (Medium, 1 August 2018) < https://medium.com/@ogucluturk/the-dao-hack-explained-unfortunate-take-off-of-smart-contracts-2bd8c8db3562>, accessed 3 June 2019.

Peter Fleischer, “Foggy thinking about the right to oblivion” (Peter Fleischer: Privacy…? 9 March 2011) <http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html> accessed 5 May 2019.

PwC Global Blockchain Survey, <www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html> accessed 22 April 2019.

Rahul Sharma, “Public vs Private Permissioned Ledgers and Blockchain Standards”, (Forbes, 11 June 2019) < https://www.forbes.com/sites/forbestechcouncil/2019/06/11/public-vs-private-permissioned-ledgers-and-blockchain-standards/#42a996e9550b>, accessed 17 June 2019.

Richard Water, ‘Facebook sued by US regulator over Cambridge Analytica scandal’ (Financial Times, 19 December 2018) <www.ft.com/content/683554b2-03c2-11e9-99df-6183d3002ee1> accessed 22 April 2019.

Simply Explained – Savjee, ‘Zero Knowledge Proof – ZKP’ (*Youtube*, 14 January 2019) <https://www.youtube.com/watch?v=OcmvMs4AMbM> accessed 21 July 2019.

The world’s most valuable resource is no longer oil, but data’ (The Economist, 6 May 2017) <www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>accessed 19 April 2019.

Transparency Report: Search removals under European privacy law <https://transparencyreport.google.com/eu-privacy/overview>, accessed 5 May 2019.

Vbuterin, ‘Proof of Stake FAQ’ (*GitHub*, 20 March 2019) <https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#what-is-proof-of-stake> accessed 21 July 2019.

‘What are Bitcoin Mining Pools?’ <https://www.coindesk.com/information/get-started-mining-pools> accessed 17 July 2019.