The right to be forgotten in the light of the consent of the data subject

Cesare Bartolini*, Lawrence Siry

University of Luxembourg

Abstract

Recently, the Court of Justice of the European Union issued decision C-131/12, which was considered a major breakthrough in Internet data protection. The general public welcomed this decision as an actualization of the controversial "right to be forgotten", which was introduced in the initial draft for a new regulation on data protection and repeatedly amended, due to objections by various Member States and major companies involved in massive processing of personal data. This paper attempts to delve into the content of that decision and examine if it indeed involves the right to be forgotten, if such a right exists at all, and to what extent it can be stated and enforced.

Keywords: Data protection, General Data Protection Reform, consent.

1. Introduction

In May 2014, the Court of Justice of the European Union (CJEU) issued a decision[1] which has been regarded as the enforcement of the right to be forgotten in the scope of the European Data Protection Directive (DPD). Although the decision of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* does not explicitly mention a right to be forgotten, privacy advocates as well as the European Commission have stated that the CJEU did not create a new right, but simply applied the right to be forgotten, which was already present (although not explicitly mentioned) in the existing legal framework[2].

This statement seems quite provocative and oversimplified. Preliminarily, it should be observed that a right to be forgotten is not mentioned in the current DPD provisions, yet it has been statutorily introduced in the proposed General Data Protection Regulation (GDPR). The GDPR comes from the evolution of the DPD interpretation in the light of technological developments since its adoption in 1995. However, whether

*Corresponding author

Email addresses: cesare.bartolini@uni.lu (Cesare Bartolini), lawrence.siry@uni.lu (Lawrence Siry)

[1] European Court of Justice. *Decision C-131/12, ECLI:EU:C:2014:317.* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131. May 2014.

[2] See Section 6 *infra*.

the right to be forgotten is just the interpretational evolution of the principles that are within the DPD, or it represents a *quid pluris* in the law, is debatable. In other words, could a judge really enforce the right to be forgotten under the current legislation? Or is the statement that the CJEU affirmed the right to be forgotten just an exaggeration?

Indeed, there has been a significant evolution in the interpretation of data protection legislation. The DPD provisions concerning the right to rectification[3] and the right to object[4] have been interpreted extensively and grouped under a general category of the rights of the data subject (DS) over his or her data[5], because these rights are not a novelty introduced by the DPD, but stem from the already-existing principles that form the basis of data protection in Europe. On the other hand, however, the "right to be forgotten and to erasure", as it is being introduced by the reform, has its own provisions and regime which are not yet in force. The Court is probably applying an evolutive interpretation of existing principles, but stating that it has officially introduced the right to be forgotten is perhaps too much, especially considering that (as will be detailed in Subsection 6.2) the content of the decision appears to differ from that of the right to be forgotten.

Perhaps the *Google Spain* case can be better seen as a development in the interpretation of the DPD provisions concerning consent. Existing EU law does not provide the "right to be forgotten", but those provisions may still offer a basis to enforce it.

In general, the processing of personal data requires that the DS agrees by giving his or her informed consent. Additionally, the GDPR introduces the right to be forgotten, which requires the controller to erase the personal data. Both consent and the erasure request are based on the intent of the DS. On one side, giving one's consent is the door that opens up the lawfulness of the processing of personal data; on the other side, the willingness to be forgotten (in the terms of the GDPR) is the lock that makes further processing unlawful. At a first glance, one could say that exercising the right to be forgotten is an operation that is inverse to giving consent: essentially, a *withdrawal of consent*. This seems to be a much more reasonable ground to affirm a right to be forgotten, due to the complex juridical nature of consent which opens it to different interpretations. In other words, if the right to be forgotten already exists between the lines of the DPD, it might be in the shape of a withdrawal of consent.

The matter, however, is very delicate, because the DPD is unclear whether it is

[3] Article 6(1), subparagraph d, Directive 95/46/EC.

[4] Article 14, Directive 95/46/EC.

[5] There are actually two different classifications for the various provisions of the DPD. Some early comments (Elgesem, D. "The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data". In: *Ethics and Information Technology* 1.4 (Dec. 1999), pp. 283–293) tended to interpret the various rights of the DS separately depending on their *purpose*, regarding the provisions as being structured into several *layers*. The first layer concerns the quality of the data, whereas a separate layer concerns the legitimacy of the processing, including the right to object. This classification is still being followed by some sources (European Union Agency for Fundamental Rights. *Handbook on European data protection law*. Apr. 2014). Other commentators (Cate, F. H. "The EU Data Protection Directive, Information Privacy, and the Public Interest". In: *Iowa Law Review* 80.3 (May 1995), pp. 431–443) have embraced a different interpretation according to which the Directive confers upon the DS the right to exercise a control over his or her personal data, a right which is further detailed into a set of specific powers. The latter classification appears to have been welcomed in the draft Regulation, where all rights pertaining to the DS are provisioned under Chapter III "Rights of the data subject".

possible to withdraw, or revoke, one's consent once it has been freely given. And even if that were possible, there is no provision explaining what happens when the consent is withdrawn or revoked.

In addition to that, some provisions within the DPD confer on the DS the right to object to the processing of personal data. While there is clearly a connection between the right to object and the right to withdraw consent, it is arguable whether they are actually the same right. If they are not, and the right to be forgotten is not based on the withdrawal of consent, then maybe it can be found as an application of the right to object.

This paper delves into the judicial concepts of consent and the right to object, looking for similarities and differences in comparison to the right to be forgotten, to discover whether the seeds of such a right can be found in either of these legal concepts.

According to the analysis in the following, the short answer is no. It doesn't seem possible to infer the right to be forgotten, as it is formulated in the current draft of the GDPR, from the right to object, nor from a more generic withdrawal of consent. In other words, we argue that since no right to be forgotten exists, the Google Spain decision (which does not mention the right to be forgotten) addresses the matter from a different perspective. Also, the content of the decision does not match the obligations provisioned in Art. 17 of the GDPR (as explained in Subsection 6.1). If this analysis is correct, then the CJEU must rely on something else to issue the decision; and that could be the right to object instead.

In the following, Section 2 gives an introduction to the legal concept of consent, describing its nature and doctrinal analysis in both Civil Law and Common Law systems. Section 3 compares the concept of consent in data protection against the right to object stated in the DPD and in Member State laws to determine whether the right to object can be used as a basis to assert that a right to be forgotten exists under current legislation. After arguing that the right to object is not the equivalent of withdrawal of consent, Section 4 tries to find a generalized right to withdraw consent among the provisions of the DPD. There does not appear to be any generalized means of withdrawing consent, but Member States are free to introduce it. Could such a right be considered equivalent to the right to be forgotten? Again, the analysis suggests that the two rights are not the same.

Then, Section 5 analyzes the reform proposal, trying to outline the right to be forgotten in the GDPR, its relationship with the withdrawal of consent, and the controversial problems related to it. Finally, Section 6 runs through the details of the Google Spain decision and, based on the previous analysis, tries to determine whether the statements about it enforcing the right to be forgotten can be maintained, or the decision is asserting something different.

2. Consent-based processing

Consent is crucial in data protection legislation, at any level. The focus of this section is an analysis of consent under a legal point of view, especially in the light of the protection of personal data.

2.1. Data protection and consent

When the DPD[6] was adopted in 1995, it represented an evolution in the concept of personal data and the means to enforce its protection in a legislative environment. Starting from the 1970's, data protection law, with an origin rooted in Article 8 of the European Convention on Human Rights (ECHR)[7], had developed to a limited degree in Europe[8]. Additionally, in 1981, with the adoption of the Council of Europe's Convention 108[9], the idea of data protection as a right worthy of protection began to emerge. Over this time span, the first sparks of the computer revolution were ignited.

By then, the legal concept of data protection followed two completely different tracks, one in Europe and another in the United States. This is due in part to the fact that the United States did not adhere to the ECHR, and in part to the long evolution that privacy had already gone through in US courts and doctrinal analysis. Whereas in the United States the protection of personal data was born as a branch of the wider concept of privacy, and to date it is still seen as one of its aspects and protected under a common law tort[10], in Europe it had evolved as a concept of its own, separately from the concept of privacy. It had become the individual's right that personal information about him or her be collected and processed in a fair way and with a close relationship to the alleged purpose of the processing. However, early legislative measures could not take into account the massive collection and ubiquitous availability of any sort of personal data which would be stored in huge data centers and could allow a detailed profiling

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

[7]ECHR, Article 8 - Right to respect for private and family life.

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[8]*Hessische Datenschutzgesetz*.

[9]Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – CETS No.: 108.

[10]There has been a significant and controversial evolution in the American privacy doctrine. Prosser, W. L. "Privacy". In: *California Law Review* 48.3 (Aug. 1960), pp. 383–423 categorizes privacy torts into four main families, of which only the fourth has a net relationship with data protection. A brief survey can be found in Bartolini, C. *Privacy in the information society and the principle of necessity*. Saarbrücken, Germany: LAP Lambert Academic Publishing, Feb. 2013. However, it has been argued by Bloustein, E. J. "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser". In: *N.Y.U. Law Review* 39.6 (Dec. 1964), pp. 962–1007 that Prosser, in his milestone analysis, only focused on the monetary impact of the privacy intrusion, i.e., only when the identity of the plaintiff has a monetary value, whereas the interest protected by the privacy torts, as it had been originally suggested in Warren, S. D. and Brandeis, L. D. "The right to privacy". In: *Harvard Law Review* IV.5 (Dec. 1890), pp. 193–220, is related to human dignity and not to property. According to McClurg, A. J. "A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling". In: *Northwestern University Law Review* 98.1 (2003), pp. 63–143, pp. 107–113, this mistake has led US courts to associate the privacy tort with the right of publicity, thus denying protection in all situations where the plaintiff's identity didn't have a commercial value. Similarly, Barbas, S. "The Death of the Public Disclosure Tort: A Historical Perspective". In: *Yale Journal of Law & The Humanities* 22.2 (2010), pp. 171–215 provides a detailed historical analysis of the evolution of privacy in the United States, observing how the contrast between the freedom of expression and privacy has been won by the former in courts.

and traceability of individuals[11]. During the Eighties, computers reached a degree of maturity that allowed any company or institution to have some computing power; computer-based processing of personal data therefore started to gain some attention. The Nineties saw the growth of the Internet, and with it the perception of the risks it carried along for the users' identities. Under these premises, the DPD was approved.

2.2. Consent: a requirement of processing

One of the critical aspects of the DPD is that of the *consent* of the DS. In the majority of situations, without the DS's consent, a data controller is not entitled to perform any of the operations that fall under the collective term of "processing" in the language of the DPD.

Consent, however, is not the sole basis on which data processing can be founded. Article 7 of the DPD defines the conditions under which processing of personal data is to be considered lawful. The DS's intent is meaningful only under subparagraph a (processing under the DS's consent for specific purposes), and subparagraph b (when required for the execution of, or prior to entering, a contract to which the DS is party). These two subparagraphs numerically cover the majority of real-world processing. They also differ from the other subparagraphs from the perspective of the interests involved. Subparagraphs c through f address situations in which there is a preeminent interest (legal or public). Instead, under subparagraphs a and b the interests of the DS are not in a subordinate position with respect to those of the data controller. Therefore, the situations in which the user's intent is relevant not only represent a numerical majority, but also a sharper conflict between interests which are on the same level. The legislator solved this conflict in favor of the data subject, by requiring his or her consent before processing.

2.3. Legal nature of consent

Defining consent from a legal point of view is no easy task. Although consent addresses a rather intuitive concept[12], it appears to be quite complex from a classificatory perspective. The consent of the right-holder is generally studied by doctrine[13] in the context of personality rights, in particular with respect to personal identity and healthcare.

---

[11] Actually, the risks of massive data collection and the possibility for public institutions to control individuals through such knowledge had already been envisioned by Rodotà, S. *Elaboratori elettronici e controllo sociale*. Vol. 2. Quaderni dell'Irsta. Strada Maggiore 37, 40125 Bologna, Italy: Il Mulino, 1973, but this vision wasn't embraced by early legislation or Convention 108.

[12] O'Shea, T. *Consent in History, Theory and Practice*. Tech. rep. `http://autonomy.essex.ac.uk/consent-in-history-theory-and-practice`. University of Essex: Essex Autonomy Project, Mar. 2011 observes that "[a]t its simplest, to consent is to give permission or reach agreement for some activity to occur", and in this meaning it predates any formal approach to express consent.

[13] See for example Faden, R. R. and Beauchamp, T. L. *A History and Theory of Informed Consent*. 200 Madison Avenue, New York, New York 10016, USA: Oxford University Press, 1986; Goldstein, J. "For Harold Lasswell: Some Reflections on Human Dignity, Entrapment, Informed Consent, and the Plea Bargain". In: *The Yale Law Journal* 84.4 (Mar. 1975), pp. 683–703; Popovici, A. "Personality Rights - A Civil Law Concept". In: *Loyola Law Review* 50.2 (2004), pp. 349–358. A deep analysis by Gisclard, T. "Consent in Licenses of Personality Rights". In: *European Review of Private Law* 22.3 (2014), pp. 345–370 covers the various means of granting and withdrawing consent in a comparative perspective.

Generally speaking, its legal nature can be argued, seeing it either as an act with intentional or unintentional legal consequences[14]. However, the matter appears to be of mostly theoretical relevance. Especially in the light of the data protection legislation, the relationship with defects of consent is independent of the contractual or non-contractual nature of the consent.

Consent operates differently in the first two subparagraphs Article 7 of the DPD. In subparagraph b, the preeminent interest of the parties, and the processing of personal data is secondary. This requirement is not present in subparagraph a, where it rather appears that the data controller has an interest in processing the DS's personal data without an explicit contractual request on the DS's side. Subparagraph a has no relationship whatsoever with the (present or future) existence of a contract. The initiative for the processing of personal data seems to reside more on the data controller under subparagraph a, whereas it can equally be on either party under subparagraph b. This might imply that the legal nature of consent is mostly contractual under subparagraph a, where the DS has to agree on a request by the data controller, and non-contractual under subparagraph b, where it appears more like a required clause of a contract (therefore the contractual intent resides in the contract and not in the consent to personal data processing).

Additionally, the DPD requires that the DS "must be given accurate and full information"[15], and that the consent to data processing be given in a free and informed way[16]. Article 10 contains provisions concerning information that must given to the DS, applicable in all cases of collection of personal data, regardless of the specific purpose of the processing. Finally, consent is defined[17] as freely given and informed

[14]The reference is to a concept widely used in civil law countries. The German law places a strong emphasis on the concept of *Rechtsgeschäft*, which is a juridical act in which the declaration of will (*Willenserklärung*) forms the basis of the legal consequences. According to Fauvarque-Cosson, B. and Mazeaud, D. *European Contract Law: Materials for a Common Frame of Reference: Terminology, Guiding Principles, Model Rules*. European Private Law. München: Sellier, 2008, p. 82, the concept is opposed to that of the real act (*Realakt*), where there is no declaration of intent, but the mere presence of an act is sufficient to produce the legal effect, and the juridical quasi-act (*geschäftsähnliche Handlungen*) where the legal effect is the consequence of a declaration, regardless of the underlying intention. In Italy, a similar concept is focused around the notion of *negozio giuridico* (Santoro-Passarelli, F. *Dottrine generali del diritto civile*. 9th ed. Eugenio Jovene, 1997, p. 126), where the will is producing the legal effects, together with the *cause* of the act, which is its social and economic function. The distinction is fundamental in the law theory of those system, because the law reacts depending on whether an act is relevant independently of the intent of having the legal consequences of that act, or it is made purposefully to enact those legal consequences. In the former case, the mere occurrence of the act is enough to trigger the legal consequences, independently of the actor's real intent; in the latter case, the intent of the actor is the trigger for the legal consequences, so that a vitiated intent may prevent them from occurring. Common law systems generally don't know a similar juridical figure, which descends from Roman law; the classical common law theory founding the validity of a contract is *consideration*, which is the expectation of a counterperformance by the other party. The European principles of contract law at Article 2:102 use the concept of *intention* that gives relevance to the party's will in a way similar to civil law systems (see Lando, O. and Beale, H., eds. *The Principles Of European Contract Law, Parts I And II*. Kluwer Law International, Nov. 1999, p. 144–145).

[15]Recital 38 of the DPD.

[16]Recital 70 of the DPD.

[17]Article 2, subparagraph h: "'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

indication about the agreement to being processed[18]. Together, these provisions imply that the contractual or non-contractual nature is not particularly relevant: in any case where the consent is given under a defective situation, the processing is unlawful.

Under a doctrinal analysis, consent may be seen as a form of acquittance: giving up one's right that would prevent a conflict of interest, deciding not to exercise that right thus allowing the other's interest to prevail[19]. In general, in the presence of conflicting interests, a party giving consent implies an acquiescence of a right in favor of the other party's interest[20]. When the conflicting interests are on the same level, unless a right holder accepts the other party's intrusion in his own private rights, any activity by the other party is illegitimate. The user's consent opens up the possibility for the other party to pursue its interest, within the limits of the consent released.

However, the concept of consent as surrender is inappropriate in the scope of the protection of personal data[21]. The DS does not simply abandon the right over his or her personal data by giving is consent[22]. Consent has a more procedural function as far as data protection is concerned. By giving consent, the DS maintains a degree of control over the processing, as well as remedies in case of unlawful processing[23]. The DS becomes actively involved in a dynamic relationship with the data controller to ensure that the processing is lawful, within the limits of the consent, and fair[24].

---

[18]The legislative expression is significant. "Freely given" denotes that consent must be given in the absence of coercion or violence, whereas "informed" means that the data subject should be aware of what he or she is consenting to, what data will be processed, and the reason why. In case the consent is not freely given or lacking sufficient information, it would be vitiated, and the data subject might request that the controller cease all processing.

[19]Under this perspective, consent is not a passive tolerance of the other party exercising the conflicting interest. Rather, it is a conscious decision that can be expressed in an implicit manner. According to Faden and Beauchamp, *A History and Theory of Informed Consent*, p. 235, "[c]onsents and refusals are actions[,] acts of autonomous authorizing [or] declining to authorize".

[20]Santoro-Passarelli, *Dottrine generali del diritto civile*, p. 53, reckons that "the revocable consent of the person to exposition or publication [...] stands as a statement that in the concrete situation there exists no interest in privacy". Hurd, H. M. "The moral magic of consent". In: *Legal Theory* 2.02 (June 1996), pp. 121–146, p. 123 argues that consent can operate in two different ways: it can transform the morality of another's conduct, so that an action that would normally be wrong becomes right when endorsed by the other party's consent; and it allows another to do a wrong act, meaning that the act does not become right by virtue of consent, but rather the consent defeats any rights that the actor not do the wrong act, thus waiving a defense. Ibid., p. 131 compares the behaviour of the consenting person to that of an accomplice, in the sense that consent, by act or omission, provides an aid to the actor's actions; also, the mental state of the consenting person is not the same of the wrongdoer, just as the accomplice's behaviour is not supported by the same degree of culpability required to actually commit the offense.

[21]Although, in the early years of personal data protection, the concept of acquittance was considered adequate. According to Robbers, G. "Der Grundrechtsverzicht. Zum Grundsatz 'volenti non fit iniuria' im Verfassungsrecht". In: *Juristische Schulung* 25.12 (Dec. 1985), pp. 925–931, p. 928, an individual can waive the protection of his or her own personal data by giving consent to their transfer and processing, on the basis of Articles 1 and 2 of the German Fundamental Law.

[22]Reimer, S. "Die datenschutzrechtliche Zustimmung". MA thesis. Universitätsring 1, 1010 Wien, Austria: Universität Wien, 2010: "there is always an exercise of the fundamental right and not a waiver of the right itself".

[23]Resta, G. "Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali". In: *Rivista critica del diritto privato* 18.2 (2000), pp. 299–333, pp. 304–306.

[24]Geiger, A. "Die Einwilligung in die Verarbeitung von persönlichen Daten als Ausübung des Rechts auf informationelle Selbstbestimmung". In: *Neue Zeitschrift für Verwaltungsrecht* 8.1 (Jan. 1989). `https:`

Under Common Law, consent is seen as a procedural justification. Simply put, if a person consents to another person doing something to him or her, and later claims that the (consented) behaviour consisted of a wrongdoing, the given consent can be used by the defendant as a means of defence[25]. Again, while the classification may be appealing in a general context, this does not appear to be a satisfactory assumption regarding consent in personal data protection. First, acquiring the DS's consent is not sufficient to guarantee that the data controller will not incur in liability, as there are a number of principles and rules (proportionality, necessity and so on) that further restrict the limits of data processing, regardless of consent. Second, by consenting, the DS establishes an active relationship involving the processing of personal data.

Regardless of the contractual or non-contractual nature of consent, for the purposes of personal data protection it behaves as a condition precedent to the processing, i.e., the lawfulness of any processing activity is subject to the consent of the DS[26], and (with respect to subparagraph b) the contract cannot be executed by any of the parties without the consent. More specifically, it acts as a *condicio iuris*[27], because the requirement is introduced by the law and not by the parties. Also, although operating in the sole interest of one of the parties (the DS), it doesn't appear that the condition can be renounced by the DS, since it is the expression of a public interest in a fair and lawful processing of personal data. In other words, the DS would not be entitled to generically give up his or her control over any future processing and personal data by the data controller.

Additionally, the DPD requires that consent be given by the DS, but does not mention anything about the time at which it must be given. Any processing carried out prior to obtaining the consent is certainly unlawful, but doubts may arise over what happens when the DS gives consent to the processing: whether the consent also operates as a date of commencement, with an *ex nunc* lawfulness of the processing, leaving the data controller liable for any processing that occurred previously; or if it operates retroactively, with an *ex tunc* effect, giving lawfulness to previous processing, or at least to the part of it which was carried out within the boundaries of the subsequent consent. The Directive is not explicit about this. In the absence of any provisions, unless the DS expressly requests that data processing is allowed only for the future, it would be

---

`//beck-online-beck-de.proxy.bnl.lu/?typ=reference&y=300&z=NVWZ&b=1989&s=35&n=1`, pp. 35–37 highlights two aspects of the DS's right of control over his or her own personal data. As a defensive right it grants protection to individuals against unlimited collection, storage, use and disclosure of their personal data; as a positive guarantee, the right to informational self-determination for the individual confers the power to basically decide on disclosure and use of personal data.

[25]Beyleveld, D. and Brownsword, R. *Consent in the law*. Legal Theory Today. 16C Worcester Place, Oxford OX1 2JW, UK: Hart Publishing, Jan. 2007, pp. 59–63. The authors further distinguish consent in two subcategories. The former is the one expressed in the text, where "the consenting agent, A, is precluded from raising a complaint about the conduct of the recipient agent B"; in the latter, consent is given with respect to a rule-set, which one party prospects to the other (as may be the case of a contract), and the person who gives the consent "is precluded from denying that he or she is bound by the rules (the rights and obligations) to which he or she has consented".

[26]It is worth repeating that this statement only embraces processing based on consent (subparagraphs a–b of Article 7).

[27]A *condicio iuris* is a condition that is automatically applied to a juridical act by the law and not by the parties' will. The fact that the DS's consent determines the lawfulness of the processing is not a consequence of the will of the parties, so it is not a voluntary condition.

logical to assume that, once consent is given, it pertains to all processing carried out within the alleged purposes, regardless of whether it was previously illegitimate.

The matter is far from having a merely theoretical interest. In fact, a lot of service providers on the Internet start collecting data about their users as soon as they start surfing their web sites, either by collecting data about the users' location, IP address, providers, user agent, navigation preferences, search queries, and so on, or by storing *cookies* onto the user's computer, to maintain data across different visits and keep profiling users in the future. It is generally recognized that storing a cookie onto a user's browser is a form of data processing from the point of view of the DPD[28]. In most cases, this "up-front" processing is carried out without requesting any consent by the user, and thus is performed unlawfully from the perspective of the DPD. Later, if the user subscribes to that service (and is therefore required to give consent to the data processing), those data are silently merged with all subsequent ones. In doing this, the DS has silently acquiesced and made lawful something that had already happened and was unlawful prior to his or her consent.

The function of consent in personal data protection has been debated as well[29]. While the original idea of consent as an expression of the autonomy of the DS might be considered appropriate in the past[30], the recent technological developments have made it inefficient. It has been observed that autonomy is based on three factors: intentionality, understanding and controlling influences[31]. A different approach[32] is centered around the duties of the data processor, that is, obligations stemming from the law or ethical regulations[33]. Finally, a third approach to consent is based on the DS's rights: the acquisition of consent must be respectful of the fundamental rights of the DS, in the light of his or her autonomy[34]. However, it has also been noted that acquiring the "in-

[28]The use of cookies has been viewed as a threat for a long time. The issue came to the attention of the general public when the online advertising company DoubleClick Inc. planned to acquire the marketing company Abacus Direct, because DoubleClick, by means of its cookies, had collected information on over 100 million Americans (Rubinstein, I. S. et al. "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches". In: *The University of Chicago Law Review* 75.1 (2008), pp. 261–285). Over time, users have developed some attention to cookies, but cookie techniques have evolved as well in response to the heightened attention (Hoofnagle, C. J. et al. "Behavioral Advertising: The Offer You Can't Refuse". In: *Harvard Law & Policy Review* 6.2 (Aug. 2012), pp. 273–296).

[29]An accurate analysis of several approaches to consent is offered by Kosta, E. *Consent in European Data Protection Law*. Vol. 3. Nijhoff Studies in European Union Law. Plantijnstraat 2, 2321 JC Leiden, The Netherlands: Brill, Mar. 2013, pp. 130–140.

[30]Faden and Beauchamp, *A History and Theory of Informed Consent*, *passim*.

[31]This view is challenged by Kosta, *Consent in European Data Protection Law*, p. 138. When consent is provided by means of a checkbox, there is no guarantee the the DS has actually read or understood the data protection policy.

[32]Manson, N. C. and O'Neill, O. *Rethinking Informed Consent in Bioethics*. University Printing House, Shaftesbury Road, Cambridge, CB2 8BS, United Kingdom: Cambridge University Press, Apr. 2007.

[33]According to Kosta, *Consent in European Data Protection Law*, p. 138, this concept is questionable as well, because most modern services processing personal data do not rely on a personal relationship between the DS and the data controller, but are based on standard forms and documents.

[34]This is the view endorsed, among others, by Ibid., pp. 138–139; Rouvroy, A. and Poullet, Y. "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy". In: *Reinventing Data Protection?* Ed. by Gutwirth, S. et al. Springer Netherlands, 2009. Chap. 2, pp. 45–76; Brownsword, R. "Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality". In: *Reinventing Data Protection?* Ed. by Gutwirth, S. et al. Springer Netherlands, 2009.

formed consent" of the DS is no longer a viable solution to protect his or her personal data[35].

Questions arising from the legal nature and effects of consent are interesting from a doctrinal perspective, but the real significance of the matter is related to the withdrawal of consent[36]. The DPD does not provide a general provision for withdrawing already-given consent. Therefore, legitimate questions would include whether it is possible for a DS to withdraw consent, thus preventing data processing. In case withdrawal is possible, to what extent should it be allowed? What is the legal nature of the withdrawal? How should the withdrawal occur and what would its effects be? And, what should happen to data already collected and processed?

3. The right to object

The DPD does not include a general right of the DS to withdraw consent, as there are no provisions whatsoever requiring Member States to implement the right to withdraw consent once it has been given freely and based on fair and complete information[37]. This section analyzes the relationship between the right to be forgotten and the right to object, trying to determine if, while not explicitly provided by the Directive, the former can be inferred from the latter.

3.1. The right to object in the DPD

The DPD provides a right of objection to data processing under certain circumstances. Of course, the right to object to personal data processing has a strong relationship with the right to be forgotten. Indeed, if the DPD granted a generalized right to object to the processing of personal data, such a right could be used to prevent the data controller to perform any further processing involving that subject. However, based

Chap. 2, pp. 83–110, because it "safeguards the central role to the consent of the data subject", in line with Europe's strong protection of human rights.

[35]According to Schermer, B. W. et al. "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection". In: *Ethics and Information Technology* 16.2 (Mar. 2014), pp. 171–182, "consent overload, information overload, and the absence of meaningful choice leads to 'consent desensitisation'. Users no longer make active, informed choices when confronted with a consent situation, but instead simply provide consent when consent is asked". Acquisti, A. "Nudging Privacy: The Behavioral Economics of Personal Information". In: *IEEE Security & Privacy* 7.6 (Dec. 2009), pp. 82–85 suggests a "soft-paternalism" solution, by designing systems in such a way that they "nudge" individuals, offering them "the option of more informed choices".

[36]In a comparative analysis on the possibility to withdraw consent in personality rights, Gisclard, "Consent in Licenses of Personality Rights" observes that "[t]he existence of a right of withdrawal is highly controversial in many countries, even in those where the law specifically confers on the person the right to withdraw her consent".

[37]Eventually, the European Data Protection Supervisor (EDPS) sanctioned that the possibility of withdrawing one's consent is implicit in the DPD (see European Data Protection Supervisor. *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*. `http://europa.eu/rapid/press-release_EDPS-14-6_en.htm`. Mar. 2014, p. 15, note 39). However, this statement has been released almost twenty years after the DPD was in force, and in the light of the new reform proposal, which explicitly allows to withdraw consent at any time. The timing of such a statement raises legitimate doubts as to whether this was the real intention of the DPD since its origin.

on the formulation of the right to object in the DPD and in the legislation of Member States, the right to object does not seem to extend to encompass a full-fledged right to be forgotten.

In its premise, the DPD requires that the DS should have the right "to object to processing in certain circumstances"[38]. As for the nature of these circumstances, other recitals provide some clarifications. When data are processed for the purpose of marketing, this right should be granted "at no cost and without having to state his reasons"[39]. On the other hand, when the data processing is not based on the DS's consent, but for example for public interests, the DS should have the more limited right "on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself"[40]. This specific protection is further softened because "Member States may nevertheless lay down national provisions to the contrary"[41]. Such premises are actually matched in the Directive provisions, which allow the DS to object to data processing carried out under public interests or the legitimate interests of the data controller or third parties[42]. In any situation where the data are processed for the purpose of direct marketing, the right to object to the processing must be granted at any time and free of charge[43]. In other words, the DPD does indeed grant the DS the right to object, but in a limited scope which can be further narrowed by national legislation.

3.2. Implementation by Member States

Member States have not drifted much from the right to object of the DPD.

UK legislation grants the DS a generalized right "to require the data controller [...] to cease, or not to begin, processing" if it can "cause substantial damage or substantial distress"[44]; if the processing takes place for the purposes of direct marketing, then it can be prevented at any time[45]. Similarly, Italy grants the DS a right of opposition to data processing "for legitimate reasons", or in any case of direct marketing[46].

The Spanish law confers a slightly stronger protection to the DS. The data protection law[47] does not include a provision on the right of objection, but defers it to a ruling[48], which grants the right to object under conditions which are essentially the same as those in the DPD; additionally, however, the DS may object to the processing

[38] Recital 25.
[39] Recital 30.
[40] Recital 45.
[41] *Ibid.*
[42] Article 14: "Member States shall grant the data subject the right: (a) to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data".
[43] Article 14, subparagraph b.
[44] UK Data Protection Act, Section 10.
[45] UK Data Protection Act, Section 11.
[46] Italian *d.lgs.* 196/2003, art. 7, subparagraph 4.
[47] Spanish *Ley orgánica* 15/1999.
[48] Spanish *Ley orgánica* 15/1999, article 17(1) and Spanish *Real Decreto* 1720/2007, article 34.

when its purpose is the taking of a decision based solely on an automated processing of personal data.

In Portugal, a right of opposition is granted under stricter conditions, because it requires "serious and legitimate reasons related to his or her personal situation" and the opposition must be justified. In any case of data processing for the purpose of direct marketing, the right of opposition is exercisable without any conditions or justification[49]. Similarly, the German law entitles the DS to object to data processing if "the data subject's legitimate interest outweighs the controller's interest"[50], or without any requirements in case the processing is for advertising, marketing or opinion research[51].

Luxembourg grants more or less the same right, in which the DS can issue an "*opposition justifiée*" to processing "for capital and legitimate reasons pertaining to his or her peculiar situation", or in case of direct marketing. However, an additional provision expressly allows the DS to object before data are disclosed *for the first time* to third parties for marketing purposes[52].

Lithuanian law allows the DS to object to data processing that is carried out by public authorities or in the interests of the data controller or third parties (in the form of a written notice and "legally motivated"), or ("without providing reasons") for purposes of direct marketing or survey[53].

3.3. The right to object and the right to be forgotten

Summarizing this overview, both the European Directive and Member State laws grant the DS some means of objecting to personal data processing, but this right can be exercised only if any of the following is true:

- he or she has a legitimate interest which outweighs those of the data controller, or the processing can potentially cause damage or distress, or, more generically, there are compelling and legitimate reasons to object. In this case, the DS may be required to provide a justification for the objection to be valid;
- the processing is carried out for the purpose of direct marketing, or in some cases for market research. The DS can object to such processing at any time and without justification;
- Member States can grant the right to object in situations not taken into account by the DPD, but this rarely occurs.

[49] Portuguese *lei* n.° 67/98, article 12.

[50] German *Bundesdatenschutzgesetz*, Section 20(5).

[51] German *Bundesdatenschutzgesetz*, Section 28(4).

[52] Luxembourgish *loi du* 2 *août* 2002, art. 30, subparagraph c.

[53] Lithuanian *Įstatymas* Nr. I-1374, article 27. Interestingly, the article, in its official English translation found at `http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=435305`, is titled "Data Subject's Right to Withhold His Consent to the Processing of His Personal Data", possibly placing the withholding of consent in relationship with the right to object. While this may appear weird from the perspective of other Member State laws, it is perfectly in line with the spirit of the Lithuanian law, especially in the light of article 14(1), according to which "Personal data may be processed for the purposes of direct marketing only after the data subject gives his consent". In other words, Lithuania places more emphasis on the DS's consent, regulating the processing of personal data for marketing purposes on an *opt-in* basis.

In addition to this, the DPD allows the DS the right to rectification or erasure of incomplete or inaccurate data[54]. However, this provision clearly has a more limited scope than the right to object, because it operates only when data are inaccurate or incomplete, but also does not prevent the controller to carry on with the data processing, in contrast with the right to object where further data processing is prohibited if the objection meets the requirements.

Therefore, neither in the DPD nor in national legislation is there any general provision granting the DS the right to object. The right to object cannot be used as a generalized means to prevent the data controller from processing the DS's personal data. More notably, it does not appear that the right to be forgotten (as it is defined in the GDPR, thus allowing the erasure of the data and the propagation of the erasure request) can be inferred on the basis of a general application of the right to object. Various differences emerge between the two, concerning both the *prerequisites* and the *effects*.

Concerning the prerequisites, the right to be forgotten does not have any specific requirements to be exercised, because the DS can simply withdraw his or her consent, thus enacting the provisions of Article 17(1), subparagraph b of the GDPR. The right to object, instead, can be exercised only if either of the following conditions is met:

- an *objective* requirement, related to the purpose of the data processing (direct marketing, and sometimes other purposes);
- a *subjective* requirement, meaning that the DS must allege some proof of damage or distress, or have some legitimate grounds to object.

Concerning the effects, the right to object simply states that the processing "may no longer involve those data"[55], whereas the right to be forgotten entitles the DS to obtain the erasure of the data and the propagation of the request[56].

4. Withdrawing consent

Given that the right to be forgotten does not exist on the basis of the right to object, another basis for it might be found in the withdrawal of consent. The question, then, becomes whether such a right actually exists.

4.1. Withdrawing consent under European legislation

The DPD does not explicitly grant the DS the right to withdraw consent[57]. However, this does not mean that this right does not exist in the Directive. Member States

[54] Article 6(1), subparagraph d.

[55] Article 14(1), subparagraph b of the DPD.

[56] It appears that the right to be forgotten has a wider scope and effect than the right to object, and the latter is rather a subset of the former. The legislative provisions support this view, because one of the reasons to exercise the right to be forgotten is the right to object granted by Article 19 of the GDPR, which essentially corresponds to the right to object as defined in the DPD. However, there is a major difference in the "new" right to object, and that is an *inversion of burden of proof*: whereas in Article 14 of the DPD it is the DS that must allege "compelling legitimate grounds" to object, Article 19 of the GDPR requires the data controller to demonstrate "compelling legitimate grounds [...] which override the interests [...] of the data subject".

[57] See Subsection 3.1 *supra*.

can also implement it, since the spirit of the DPD allows them flexibility in raising the level of protection of the DS.

Some references to the DS's entitlement to withdraw his or her consent can be found in the Electronic Privacy Directive (EPD)[58], an integration of the DPD with respect to electronic communications[59]. The EPD grants the DS the right, limited to certain specific categories of personal data, to actually withdraw the consent that was previously given. Namely, this right can be exercised only with respect to data related to traffic over telecommunication networks[60], and geolocalization or location data[61]. For these types of data, consent can be withdrawn "at any time"; but, apart from them, the EPD does not explicitly confer DSs a generalized right to revoke their consent.

Can this limited right be used to infer a generalized right to withdraw consent, implicitly granted by the DPD? If such were the case, then one might wonder why the DPD grants a generalized right implicitly, and later the EPD explicitly states it for certain categories of personal data. Since the two directives are several years apart, it might be argued that the legislative technique was different between them, so that the former contains an implicit right to withdraw one's consent while the latter provides a further specification on the withdrawal of consent for certain types of data[62]. However, even if these were the intentions of the European Commission, the Member States' different approaches suggest that the DPD does not provide a general right to withdraw consent, not even implicitly[63].

4.2. Differences in Member State laws

Some national laws have a single law implementing both the DPD and the EPD. Under the law of these Member States, the right to withdraw one's consent is present

[58]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[59]The field of application of the EPD is more restricted than that of the DPD, since it is limited to data protection in the electronic communication sector (thus not covering more "traditional" contexts such as non-electronic archives or general principles in data processing), but it provides a more detailed regime in that scope. Simply put, the DPD entered into force when the Internet was in its early stages, and after a few years the need for additional protection in electronic communications had already emerged. See `https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Legislation`.

[60]Recital 26 and Article 6(2) of the EPD.

[61]Recital 35 and Article 9 of the EPD.

[62]This idea has been expressed by the European Data Protection Supervisor, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, p. 15: consent "may be withdrawn, in which case any personal data pertaining to the data subject should be erased". See also footnote 37 *supra*.

[63]The opinion is debated. In particular, "[t]he Data Protection Directive does not mention a general right to withdraw consent at any time", but despite the text of the DPD provisions "such a right exists and [...] it must be possible for the data subject to exercise it at his or her discretion" (European Union Agency for Fundamental Rights, *Handbook on European data protection law*, p. 60). However, this appears more to be the outcome of the developments in the interpretation of the DPD. This seems to be confirmed by the very same source: "[t]here should be no requirement to give reasons for withdrawal and no risk of negative consequences over and above the termination of any benefits which may have derived from the previously agreed data use". This statement sounds more like a suggestion for the interpretation of the law, hinting at the fact that there currently is no express right to withdraw consent, but it should be either provided, or at least enforced through an extensive interpretation of the DPD.

in the scope of the EPD, but not in that of the DPD. Essentially, these States grant the right to withdraw consent with respect to specific types of data, without offering a general provision on a generalized right to withdraw consent for all personal data. It would appear inconsistent for the same law to grant the right explicitly in some sectorial contexts and implicitly as a general rule. In other words, when data protection law legislation includes some provisions about the right to withdraw one's consent regarding some specific type of data, these appear more as an exceptional provision than the expression of a more generic right which can be derived implicitly from the general principles of the law.

For example, Italy revised its data protection law in 2003, superseding the previous law and implementing both the DPD and the EPD within the same act. This statute provides that the DS has the right to withdraw consent to the processing of certain categories of personal data, namely traffic data[64] and location data[65], and in both cases it is stated that the consent is "revocable at any moment"[66].

Most Member States have separate implementing legislation for the DPD and the EPD. Concerning these, the situation may vary depending on whether the transposition of the DPD contains provisions on consent withdrawal or it does not. In the latter case, the same uncertainties expressed above with respect to the relationship between the two directives can be repeated for the national law. For example, such is the case with the United Kingdom, where data protection is separate from the provisions on privacy in electronic communications, which is contained in a regulation[67]. While the latter correctly allows the DS to withdraw consent to the processing of certain types of data (namely location, traffic and marketing), the Data Protection Act does not provide any hint whatsoever as to the possibility of withdrawing consent in a generalized way. This possibility might or might not be inferred implicitly from the general principles of the law[68].

Other States have separate legislative instruments for the two directives, but still the general data protection law covers withdrawal of consent to some extent. Germany is

[64] Italian *d.lgs.* 196/2003, art. 123(3).

[65] Italian *d.lgs.* 196/2003, art. 126(1).

[66] However, the Italian doctrine generally assumes that consent to the processing of personal data is revocable. See, for example, Santoro-Passarelli, *Dottrine generali del diritto civile*: "the *revocable* consent of the person to exposition or publication [...] stands as a statement that in the concrete situation there exists no interest in privacy" (emphasis added); Messinetti, D. "Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali". In: *Rivista critica del diritto privato* 16.3 (1998), pp. 339–407 and footnote 79 *infra*.

[67] UK regulation 2003 No. 2426, The Privacy and Electronic Communications (EC Directive) Regulations 2003.

[68] However, concerning the UK legislation, it has been argued that it would be very unlikely that a general right to withdraw one's consent can be found within the folds of the Data Protection Act. In particular, in Curren, L. and Kaye, J. "Revoking consent: A 'blind spot' in data protection law?" In: *Computer Law & Security Review* 26.3 (May 2010), pp. 273–283, the authors note that in the parliamentary debates a right to withdraw one's consent was assumed to be present; however, due to the wording of the law (and of the directive it transposed), interpreting it in the sense of a general right to withdraw a previously given consent would lead to an inherent contradiction in the law. Alternatively, it would be possible to operate on Article 8 of the ECHR to infer a right of withdrawal, but apart from the fact that this would seem a very feeble connection, it could be pointless because the DS could contractually give up his right to withdraw consent if such a situation were envisioned in a contract.

one of these: the *Bundesdatenschutzgesetz* does not provide a general right to withdraw consent, nor does it have any reference to traffic or location data (which are in the scope of the EPD and not of the DPD). However, with respect to data processing for commercial purposes, "the controller ensures that the declaration of consent is recorded and the data subject can access and revoke it at any time with future effect"[69]. Again, it would appear problematic to assume that this is the expression of a more general principle to withdraw one's consent to any processing regardless of the type of data involved, especially in the light that data processing for marketing purposes is on a lower level compared to the rights of the DS, as is shown already in the DPD which grants a generalized right to object to such processing[70].

An outstanding exception to this scenario is the Spanish *ley orgánica* transposing the DPD. Since there is no relationship between *ley orgánica* 15/1999 and the EPD, it makes no reference to traffic data or location data. However, the Spanish data protection law contains an explicit provision allowing the DS to revoke previously given consent "when there are justified grounds for doing so"; the law also details the temporal effect of the revocation, so that it "does not have retroactive effect"[71]. Additional provisions state that "consent for the communication of personal data may also be revoked"[72], and that the inclusion of data in publicly accessible data bases require a consent "which may be revoked at any time"[73].

In short, the Spanish law explicitly grants the DS the right to *revoke* a previously-given consent. This right is different from the right of objection, which is nonetheless granted by the Spanish law[74].

Although the Spanish law cannot speak for all Member States nor for the EU, together with the other hints which are present in the different legislation, it can be argued that a right to revoke/withdraw one's consent can be envisioned, and that it is different from the right to object which is present in EU and national legislation. The main differences between the right to withdraw consent and the right to object are:

- the right to withdraw one's consent clearly requires that the DS has already given consent to the processing of his or her personal data, whereas the right to object does not have such a requirement;
- according to the DPD, the right to object to data processing must be implemented in Member State laws. On the other hand, based on the EPD, the right to withdraw consent is required only for certain categories of data;
- the right to object normally requires the DS to allege some proof of a potential harm that the data processing can cause, or at least justify the reasons for objecting, whereas the right to withdraw consent does not require any justification.

[69] German *Bundesdatenschutzgesetz*, Section 28(3a).
[70] See Subsection 3.1 *supra*.
[71] Spanish *Ley orgánica* 15/1999, article 6(3).
[72] *Ibid.*, article 11(4).
[73] *Ibid.*, article 28(1).
[74] See Subsection 3.2.

That said, the possibility for the DS to withdraw previously-given consent, in most cases, has not been granted by Member States as a generalized provision, but only against the processing of those types of data for which it is required by the EPD[75].

4.3. Effects of consent withdrawal

Since the DPD does not grant an explicit right to withdraw a previously given consent, it leaves some open questions about its legal nature and the effects that it has on personal data processing.

Both questions can be addressed by looking back at the legal nature of consent[76]. If the DS's consent acts as a condition precedent, the main question is how its withdrawal operates. Because personal data processing is lawful only in the presence of the DS's consent, once such consent is withdrawn no further processing is allowed. However, the definition of "processing" is rather wide, encompassing a large number of activities; a sample of activities embraced by the general term "processing" is given in the DPD[77]. These certainly include collection, recording, and storage. Therefore, once the consent is withdrawn, any further collection and storage of personal data is prohibited. The data controller is not allowed to retrieve any additional personal data about the DS, or make any use of those already acquired[78]. Undoubtedly, the overall spirit of the DPD implies that no further data can be collected once the consent is withdrawn.

The matter is more problematic when it comes to data that have already been collected. In other words, does the withdrawal of consent operate as a form of revocation, with an *ex tunc* effect, meaning that all existing data collected about the DS withdrawing his or her consent must be deleted? Or is it simply a termination, thus with an *ex nunc* effect, allowing the controller to maintain (but not process further) data already collected[79]?

In other words, the problem can be expressed as follows. Any personal data collected by the controller after the DS consented to the processing has been collected lawfully, and data are legitimately stored in the controller's databases. But when the DS withdraws consent, is the data controller allowed to maintain those data? Or must any further procrastination in erasing them be considered a violation?

---

[75] However, it appears that the right to object, as it is defined in the DPD, was initially foreseen as a right to withdraw consent. The evolution in the European Parliament discussions, starting from the initial drafts of the DPD back in 1990, over time led to a reduction of that right, eventually transforming it in the current right to object to data processing under certain circumstances. Curren and Kaye, "Revoking consent: A 'blind spot' in data protection law?", p. 277–278 carry on a detailed analysis of the changes that went on. This strengthens the conclusion that the DPD does *not* grant the right to withdraw one's previously given consent, not even implicitly. Yet, since nothing is stated against it either, Member States are free to implement it if they deem necessary, as did Spain.

[76] See Subsection 2.3 *supra*.

[77] Article 2, subparagraph b.

[78] Unless the processing is made lawful by other provisions in Article 7 which disregard the DS's consent, of course.

[79] According to Messinetti, "Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali", pp. 358–360, who as a general rule admits that consent may be withdrawn, the legal concepts of revocation and termination are inadequate in expressing the actual significance of an act contrary to a previous authorisaion regarding the DS's personal identity. This act can only partially be subsumed under the classical legal concepts which cause the interruption of an existing contract or legal relationship.

It should be stated in advance that prior to the GDPR there does not appear to be any definite answer to this question. However, some hints can be found in the same definition of "processing" provided by the DPD, particularly in the term "storage". If storage is intended as a static activity, i.e., the very fact that data are maintained somewhere is considered storage, then it should be argued that the controller is not allowed to maintain those data anymore. On the other hand, if the concept of storage is interpreted in a dynamic perspective, meaning the activity that takes the data and places them in a place where they will be maintained, then it should be concluded that there is no prohibition to maintain those data, as long as no further processing activity occurs.

Between these two visions, the latter would appear preferable, because it is more in line with the rest of the definition. Specifically, before the sample listing of a number of activities that are included within the definition of "processing", Article 2 defines processing as "any operation or set of operations". Once the data have been stored, no operation occurs in simply maintaining them statically.

However, this interpretation appears to raise more problems than it actually solves, at least on a practical basis. Indeed, copying the data or transferring them from one location to another would be considered data processing from the perspective of the DPD. Since most data centers make use of backup copies or occasionally update their architectures by migrating the data to a different hardware or software platform, it would be very difficult to state that they are not "processing" the data in doing so. However, this obstacle does not appear to be insurmountable, because this situation could easily fall within the boundaries of a legitimate processing on the basis of Article 7, subparagraph f ("legitimate interests pursued by the controller"). Ensuring the dependability of the controller's systems, or improving services by means of more adequate hardware and software platforms, can probably be considered a legitimate derogation to the DS's consent.

Another useful hint to understand the legal nature of withdrawal is the Spanish *ley orgánica*, which actually implements a generalized right to withdraw a previously given consent. The Spanish transposition clearly states that the withdrawal "does not have retroactive effect"[80]. Although this is still insufficient to completely settle the issue, it is easier to interpret the provision in the sense that the data controller is not forced to delete the lawfully obtained data. This interpretation would be more in line with the total exclusion of any retroactive effects.

If the withdrawal of consent has a non-retroactive effect, operating only by preventing any processing from that point on, then it is all the more unlikely that it can be equated to the right to be forgotten. The "right to be forgotten and to erasure", as its title implies[81], requires the controller to erase all data pertaining to the DS exercising it, *with full retroactive effect on data already collected*.

Concluding, although the answer is not certain, it would appear that not even the right to withdraw a previously given consent can be used as a means of exercising a right to be forgotten. It does not appear then, that the DPD or Member State legislation

[80] Spanish *Ley orgánica* 15/1999, article 6(3). See also footnote 71 *supra*.

[81] See footnote 83 *infra*.

actually provide any means to allow a DS to request a data controller the erasure of any personal data pertaining to him or her, unless some legitimate reason such as inaccurate data exists.

5. Reform proposal

The data protection reform proposal represents a major overhaul of the existing data protection regime, attempting to set a new level of data protection throughout all EU countries, addressing the emerging technologies which over the years have posed new challenges in the field of data protection. The general part of the reform is contained in a Regulation[82] which is currently being reviewed and amended.

5.1. The right to be forgotten in the reform

The approval of the reform is facing difficulties and controversy. One of the most debated problems is precisely the enumerated right to be forgotten, explicitly stated in the title of Article 17[83]. This article has faced many changes and amendments from the original text back in 2011. In particular, Article 17 has been completely rewritten since its original formulation, and some parts of it have been removed and have become separate articles[84]. The original formulation was very clear[85], granting the DS the right to have any reference to data completely erased from publicly available communication

[82]The reform proposal is split into two documents, a Regulation (document 2012/0011) and a Directive (document 2012/0010). Whereas the GDPR contains the general provisions, and is basically the complete revision of the DPD, a separate directive is currently under preparation for data protection in criminal investigations by public authorities. The choice has been controversial. One of the key objectives of the reform is to make data protection consistent (European Commission. *Why do we need an EU data protection reform?* `http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf`. 2012). Doubts have been expressed as to the need to have two separate disciplines, especially given that the distinction underlying them (general data protection and criminal data protection) has been considered artificial and inconsistent. This structure has been "met with regret by Europe's data protection advocates" (Giurgiu, A. and Lommel, G. "A New Approach To EU Data Protection". In: *Die Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (KritV)* 97.1 (2014), pp. 10–27).

[83]The current formulation of Article 17 is titled "Right to be forgotten and to erasure".

[84]Hoboken, J. van. *The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember*. Tech. rep. European Commission, May 2013, p. 16.

[85]According to Ibid., draft 51 provided the DS with a very strong concept of the right to be forgotten, because Article 15(2) granted the DS the right to obtain the erasure not only of the personal data that he or she did not want to be publicly available anymore, but also to all references to them: "[t]he data subject shall have the right the right to obtain the erasure of any reference to data, which are erased pursuant to paragraph 1, from any publicly available communication service which allows or facilitates the search of or access to this data". This provision did not place a specific obligation upon the controller, so problems would arise as to who would be responsible for the erasure (or liable for a lack thereof). However, the formulation is very clear, because it explicitly states what the DS is entitled to. Later, GDPR draft 56, Article 15(2) more clearly placed the obligation to erase the data upon the data controller, stating that "[w]here the controller referred to in paragraph 1 has made the data public, it shall in particular ensure the erasure of any public Internet link to, copy of, or replication of the personal data relating to the data subject contained in any publicly available communication service which allows or facilitates the search of or access to this personal data". The text of draft 56 can be found at `http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf`.

The Commission formulation takes into account the technical difficulties the controller might have met in the exercise of such a right on the DS's part: "the controller [...] shall take all reasonable steps [...] to

services. However, this wording would have had unbearable consequences from a technical point of view, therefore it has undergone major changes[86].

Article 17(1) provides several situations where the DS has the right to be erased by the data controller. Of particular interest is subparagraph b, which allows the DS to withdraw his or her consent. In other words, based on the upcoming Regulation, withdrawal of a previously given consent is sufficient to have the right to have personal data erased by the controller. This is a generalized means of withdrawing consent and does not require any justification to be alleged to the erasure request; whereas the Spanish *ley orgánica* requires "justified grounds for doing so"[87]. Also, the right to withdraw consent is different from the right to object, which is *per se* another circumstance which legitimizes the removal request and is expressed in subparagraph c immediately following the consent withdrawal. It appears that the right to withdraw consent can be applied to data processing that is based on the DS's consent, whereas the right to object applies to data processing which is lawfully carried out regardless of the consent of the DS.

The right to withdraw consent is also contained in Article 7(3) of the GDPR, which states that "[the] data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal". After the withdrawal, any previous processing is still considered lawful, and the controller does not incur in liability (which occurs if the consent has never been given and data are processed nonetheless)[88].

Additionally, under the draft Regulation, the right to object is another possible basis for the right to be forgotten "pursuant to Article 19"[89]. In other words, the original right to object from the DPD is expanded, and under the new Regulation also requires the controller to erase all data pertaining to the objecting DS. Under this formulation, it appears that the right to be forgotten, as defined in the GDPR, is an extension of the original right to object.

In the light of the recent decision by the CJEU[90], the European Commission has stated[91] that Article 12 of the DPD, by allowing the DS to request the erasure of data

---

inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data" (Article 17(2)).

[86]The official released version of the document still dates back to January 2012. Some parliamentary reports and unofficial leaked documents provide a different formulation, and there are now two more articles (17a and 17b) concerning the right to be forgotten. However, the content of the first two paragraphs has not changed substantially from the 2012 version.

[87]Spanish *ley orgánica* 15/1999, article 6(3). See Subsection 4.2 *supra*.

[88]From a systematic perspective (see Subsection 4.3 *supra*), this is not sufficient to determine whether the withdrawal is a revocation which removes the original consent with an *ex tunc* and totally retroactive effects, or as a termination which does not remove the original consent but *ex nunc* ceases its effects. Both interpretations appear to be flawed with respect to the provision. The revocation and its *ex tunc* effect would imply a *fictio iuris* where the consent has never been given, therefore the intermediate processing should not be lawful. The termination is incompatible with the concept of "withdrawing" the consent, a "cessation" being more appropriate. An intermediate interpretation might be preferable, according to which the consent is actually revoked with retroactive effects, but the controller does not incur in any liability because it was based on legitimate expectations stemming from the DS's behaviour.

[89]Article 17(1), subparagraph c.

[90]See Subsection 6.1 *infra*.

[91]European Commission. *Factsheet on the "Right to be Forgotten" ruling*. `http://ec.europa.eu/justice/newsroom/data-protection/news/140602_en.htm`. June 2014.

that is no longer necessary, already contained the principle at the basis of the right to be forgotten, and "claims that the Commission has proposed something fundamentally new in the Data Protection Regulation are therefore wrong". While they are certainly born from a common background, the above seems to be an overstatement from a legal point of view. The right to be forgotten has a wider scope than the right to erasure of data which are no longer necessary. Since the right to be forgotten lacks a requirement (that data are no longer necessary), it can be exercised under more general conditions[92].

Article 17 contains a derogation which can prevent the erasure of the DS's personal data: withdrawing consent obtains erasure only if "there is no other legal ground for the processing of the data". *A contrario*, if there are other legal grounds for processing, the DS's request will not force the controller to erase the data[93]. The provision seems to refer to other circumstances in which the processing of personal data would be allowed even if the DS had never consented. In this case, the DS cannot obtain erasure, unless the requirements for the right to object also apply. In any case, the breadth of the derogation cannot be properly evaluated yet.

Most of the problems presented by Article 17, however, are related to paragraph 2, which deals with other parties that may have acquired the personal data for which the DS requests erasure[94]. This is a very common phenomenon in modern Internet networks called "bouncing", where a content published on some website is replicated (normally by users) on other websites. In these situations, the data controller must take any reasonable steps to inform other data controllers of the DS's request for erasure[95].

---

[92]The opinion that the DPD does not contain, even implicitly, the right to be forgotten, is dominant and preferable, maintained also (see Subsection 6.1 *infra*) by the Advocate General of the *Google Spain* case (Jääskinen, N. *Opinion of Advocate General Jääskinen*. `http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=416370`. June 2013): "the Directive does not provide for a general right to be forgotten" (par. 108; also par. 111: "Articles 12(b) and 14(a) *[the right to object]* of the Directive do[es] not provide for a right to be forgotten"), a right introduced in the reform not as "a codification of existing law, but an important legal innovation" (par. 110). Additionally, "any generalised right to be forgotten cannot be invoked [...] on the basis of the Directive even when it is interpreted in harmony with [Article 7 of] the Charter" (par. 136).

[93]This is similar to the concept of "newsworthiness" that, according to Barbas, "The Death of the Public Disclosure Tort: A Historical Perspective", caused the obsolescence of the tort of public disclosure in the US. See also footnote 10 *supra*.

[94]Par. 2 is related to any circumstance under which the DS is entitled to request erasure and not only to consent withdrawal.

[95]The protection of the DS has been strongly degraded from the original drafts of the GDPR. The DS does not have a definite right to have his or her content erased by all data controllers that may have acquired the data, but "the obligations are limited to taking 'all reasonable steps' to inform third parties" of the erasure request, which is seen as an obligation of endeavour and not of result (European Data Protection Supervisor. *Opinion of the European Data Protection Supervisor*. `https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf`. Mar. 2012, par. 146–148). Hoboken, *The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember*, p. 15 challenges this statement because it would be an obligation of result with respect to the information of third parties; however, it actually appears an obligation of endeavor, because technical difficulties might well put the controller in a situation where even informing third parties, or even knowing who they are, would not be feasible.

Still, there is still some room for significant changes. There is currently a proposal for a different formulation of Article 17 of the GDPR (European Commission, *Factsheet on the "Right to be Forgotten" ruling*).

5.2. Problems in the application

A lot of problems arise from Article 17:

- the controller might not know or be able to contact all third parties;
- third parties might have different grounds for the lawfulness of the data processing, so the erasure request might not be effective towards them even if it is for the original controller;
- in the case of Internet bounces, it is still unclear who the third party controller responsible for the bounce actually is, whether the manager of the service or its users. Modern Internet has blurred the distinction between controllers and DSs, and this is a weak spot in data protection laws.

The right to be forgotten is an instrument to protect the DS against undesired use of his or her personal data. Under the current legislation, DSs consenting to the processing of personal data are in an irreversible condition. Once the personal data have been lawfully processed by a data controller, the DS has no means of regaining complete control over them. The right to be forgotten aims at restoring this control, by granting the DS the power not only to decide who will be allowed to process his or her personal data (by giving consent), but also who will no longer be allowed to process them (by requesting erasure). This is in line with the right to the protection of personal data granted by the ECHR[96].

Clearly, the right to the protection of personal data must be balanced with freedom of expression, another fundamental right in the ECHR[97]. Requesting the erasure of one's personal data may be considered legitimate when the other party has merely a business interest, but it must not be used as a means to impose censorship, or in any case to prevent freedom of expression unconditionally. For this reason, Article 80 of the GDPR allows Member States to introduce further derogations and exemptions from the provisions protecting the DS, including the right to be forgotten, especially with respect to processing carried out solely for journalistic, artistic or literary expression.

To sum it up: the reform proposal allows the DS to withdraw consent, at will and without conditions (unless the derogation described earlier applies[98]). The controller must then erase all personal data pertaining to the DS, and forward the same request to data controllers that are known to be processing the data. Article 17 is explicitly contains "right to be forgotten" in the title. The question, at this point, is whether this is actually a right "to be forgotten", or it is not.

The DS would have the right "to obtain [...] the erasure of any links to, or copy or replication of that data"; and the controller "shall take all reasonable steps to have the data erased, including by third parties". Also, the title of Article 17, according to this proposal, would be "Right to erasure". In this formulation, the right granted to the DS appears much sharper and enforceable, and a heavier burden on the controller.

[96] Article 8.

[97] At Article 10.

[98] The derogation to Article 17, due to the generality of its formulation, is a potential weak spot against a legitimate exercise of the right to be forgotten. The right to be forgotten can be denied if there are other legal grounds to continue the processing; it would be easy for the controller to invoke such "legal grounds" such as the right to exercise a business without losing data which are significant assets. The exact breadth of the derogation will be depend on future decisions by the CJEU.

5.3. Scope of the right to be forgotten

Previous sections analyze what, in the authors' opinion, the right to be forgotten *is not*. It is not an application of the right to object[99], nor the equivalent of the withdrawal of consent[100], although both are potential grounds to enact it. The unique feature of the right to be forgotten, which makes it different from the rights granted by the existing legislation, is its retroactivity. The *Google Spain* decision does not address the right to be forgotten, either[101].

So, what *is* the right to be forgotten? Based on the above considerations, it is a novelty that will be introduced by the reform, which has a broader scope (and raises more problems) than any of the existing rights and has (rightfully) not been enforced by courts yet.

The concept of "right to be forgotten" does not have a unique definition. It originates in several European legislation, with different meanings. In France, the *droit à l'oubli* is related to the right that, after relevant news have been made public for the sake of the right of information, a person has to remain secluded, without further disclosure of his or her own private life[102]. In Italy, the *diritto all'oblio* is "the legitimate interest of individuals not to be forever exposed to further damages to his or her honor and reputation due to ongoing publication of a news that was legitimately spread in the past"[103]. The Spanish, on the basis of the *derecho al olvido*, has issued decisions that forced data controllers to delete personal data that were no longer useful for their purpose[104] (but without the obligation to propagate the erasure request). There is no definition of the right to be forgotten at an European level; at most, the draft Regulation describes it as "the right that their personal data are erased and no longer processed"[105] under certain circumstances, including withdrawing consent.

At a first glance, it would appear that the boundaries of such a right are quite sharp, but its enforcing would pose major problems. Under the Regulation, the DS can request erasure to *every* data controller who is processing the data, and not only to the one who processed the data in the first place. The fact that the DS gave consent only to the original controller does not appear to be relevant: the obligation to erase the data arises when the DS withdraws consent, without any specification on the controller who received it. Theoretically, knowing all controllers to whom his or her personal data have been bounced, the DS would be entitled to obtain erasure by all of them.

This appears to be an actual "right to be forgotten", an absolute right to have data removed by every controller. If the DS had the technical means to know all controllers who are processing the data, Article 17(1) would adequately guarantee such a right[106].

---

[99] Subsection 3.3 *supra*.

[100] Subsection 4.3 *supra*.

[101] As shown in Subsection 6.2 *infra*.

[102] Mantelero, A. "The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'". In: *Computer Law & Security Review* 29.3 (June 2013), pp. 229–235.

[103] Corte di Cassazione, III sezione civile. "Sentenza 9 aprile 1998, n. 3679". In: *Il Foro Italiano* 121.6 (June 1998), pp. 1833/1834–1839/1840.

[104] Rallo Lombarte, A. "El derecho al olvido y su protección". In: *Telos* 85 (2010), pp. 104–108.

[105] Recital 53.

[106] However, that there are some notable exceptions to this, mostly in Chapter IX of the draft Regulation

The problem then becomes purely practical: knowing who the controllers processing the data are.

For this reason, the draft Regulation goes beyond the obligation of erasure. Since controllers are more likely to have knowledge of third parties processing some data that they collected, it places upon them the additional obligation to inform those third parties about the erasure request[107]. Although the Regulation does not say it explicitly, this obligation would also weigh transitively on every subsequent controller (otherwise it could be easily eluded).

Controllers are required to implement technical solutions to allow the tracking of bounces. In several cases, this is already a reality. Major Internet services, for instance, tend not to replicate shared content from an external source, but rather to create a link to it and keep track of the link (this is also more sustainable in terms of storage and performance). In the case of erasure of the original resource, all links would be invalidated, thus actually achieving the erasure. Other services (less involved in content sharing) tend to implement fewer technical measures to achieve this solution. However the trend is moving already. Even services that traditionally are far away from the "user-generated content" paradigm, such as online newspapers, are actually starting to implement some "social" features. In general, two opposite models can be envisioned for sharing content: a distributed model and a centralized model. In the former, controllers keep track of all links that reference a given content (even if the data are replicated). In the latter, a given content exists in a single instance, and every dissemination of the data is simply a reference to the original data; invalidating the originally-published data makes every copy inaccessible. In general, a combination of these two solutions is a very efficient (and easy to implement) solution to guarantee the enforcement of Article 17(2).

6. The Google Spain decision

On May 13, 2014, the CJEU issued a decision in the case of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*[108] that received a lot of resonance. The mainstream media and the general public, on the basis of this decision, claim that the EU is enforcing the right to be forgotten[109]. However, this definitely appears to be an overstatement. This section explores the findings of the decision and compares them against the existing law and the upcoming GDPR, explaining why the Google Spain decision does not appear to actually relate with the right to be forgotten, but rather with the right to object.

("Provisions relating to specific data processing situations"). In these cases there must be a balance of interest between the DS and data controllers. For example, Article 80 contains exceptions for journalistic purposes, meaning that the right of the DS to erasure is mitigated where there are facts which have a relevance to the general public.

[107]The GDPR currently has several different formulations. The text to which this paper is referring to is the "official" released text, which however dates back to 2012. It is possible that the obligation will be different in the final text.

[108]European Court of Justice, *Decision C-131/12, ECLI:EU:C:2014:317.*

[109]Many commentators share this opinion. See footnote 123 *infra* for a list.

6.1. Facts and decision

In 2010, a Spanish citizen lodged with the Spanish Data Protection Authority (DPA), the *Agencia Española de Protección de Datos* (AEPD), a complaint against a web site and against the Google search engine (namely against the companies Google Spain and Google Inc.), because a Google search with his name would allow to retrieve some remote personal data that were stored on the aforementioned web site and indexed by Google. The DS was asking for the removal of such data. The AEPD rejected the complaint related to the removal of the data from the original web site, but upheld the one towards Google Spain and Google Inc. The defendants later moved to annul against the AEPD decision before the Spanish High Court, which referred to the CJEU for a preliminary ruling. The question was whether a search engine should be considered a data controller according to the DPD, and in case of an affirmative answer whether it was in the power of the AEPD to order the search engine to "de-index" some web pages upon the request of the DS, even if they were legitimately published on the original web site.

First, the CJEU analyzed the relationship between the US-based Google Inc. (owner of the search engine) and its Spain-based subsidiary Google Spain (managing the advertising on the Google website), finding that Google processed personal data "in the context of the activities" of Google Spain. Therefore, the Court decided that Google is subject to the national law transposing the DPD[110]. Even if Google Spain is not the data controller or the data processor (Google Inc. is), the applicability of the law descends from the related business of Google Spain, for which the data processing is fundamental.

Then, the CJEU found that a search engine must definitely be considered a data controller pursuant to Article 2 of the DPD, because the search engine "collects", "retrieves", "records", "organises", "stores", "discloses" and "makes available"[111], and the fact that it doesn't modify the data is not relevant[112]. The processing activity of search engines, which is distinct from that of the publishers of websites[113], makes available data that would not be found otherwise. The Court concluded that "the operator of a search engine is obliged to remove [...] links to web pages [...] even [...] when its publication in itself on those pages is lawful"[114].

Finally, with regards to the DS's rights, the CJEU states that the DS has the right to request that the search results are no longer made available to the general public even if they remain accessible to users of the web site where they reside, in case they are the source of a prejudice to him or her; this right[115] overrides the economic interest of the search engine, except in the case where there is a public interest to information (possibly due to the public nature of the DS)[116].

[110]European Court of Justice, *Decision C-131/12, ECLI:EU:C:2014:317.* par. 60.
[111]Ibid., par. 28.
[112]Ibid., par. 29.
[113]Ibid., par. 35.
[114]Ibid., par. 88.
[115]Charter of Fundamental Rights of the European Union Article 7, "Respect for private and family life"; Article 8, "Protection of personal data".
[116]European Court of Justice, *Decision C-131/12, ECLI:EU:C:2014:317.* par. 99.

Summing up the content of the decision, the search engine is a data controller, and it must de-index personal data if an easy search exposes data in a way that might be prejudicial to the DS.

6.2. Analysis of the decision

Clearly, the Google Spain decision builds over many years of evolution in the processing of personal data. The Court acknowledges radical changes in the way personal data are stored and accessed. Whereas back in time archives were accessible only by actually visiting the archive location, the migration of archives to IT systems and the vital role of search engines in modern society makes personal data ubiquitously accessible and at the hand of any individual. The fact that the data exist and are stored somewhere is not prejudicial to the DS's reputation *per se*. The damage stems from the possibility of instantly retrieving the data by means of search engines; and this is where the decision places itself.

The decision in itself is extremely revolutionary, because it emphasizes the role of an intermediate data controller/processor (the search engine), one which is not the data controller that legally processed the data in the first place. The search engine doesn't do anything that a normal user would not be able to do, but it does so massively by means of web crawling software ("spiders") and with a huge storage capacity. The responsibility of data controllers is thus emphasized from a quantitative point of view (the amount of data that are made accessible) and not just a qualitative one (the ways in which data are processed).

However, the decision does not actually seem to cover the right to be forgotten, but rather it appears to be more related with the right to object. There are several hints to this:

- the literal argument of the Court. The decision[117] states that the links must be removed from the list of results by virtue of Articles 12 subparagraph b and 14(1) subparagraph a[118];
- the decision hinged on the prejudice suffered by the DS, in line with the right to object under most legislation, and in contrast with the right to be forgotten which does not require the DS to prove any damage;
- the Google Spain decision does not even require that the search engine erase the personal data of the DS, but only that it avoid presenting them to users upon a web search performed using the plaintiff's first and last name as keywords;
- since Google is not required to delete those data, when a search with the relevant keywords is performed, there must be a technical means that excludes the unwanted results from the listing. This is actually a form of data processing;

[117] European Court of Justice, *Decision C-131/12, ECLI:EU:C:2014:317.* par. 99.

[118] The Court is consistent: par. 88, "Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that [...] the operator of a search engine is obliged to remove from the list of results [...]"; par. 98, "the data subject may, by virtue of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, require those links to be removed".

the decision imposes Google to process the data (even only *ad excludendum*), whereas Article 17 of the draft Regulation prevents any further processing apart from the erasure itself;

- in any case, it would be incorrect to require that the search engine erase the information, because a search engine normally does not store the web sites it indexes, but rather stores links to the web sites itself, along with some metadata (exceptions occur with respect to *caching*, temporary storage of data). Therefore, the obligation to "erase" the data would have been useless. On the other hand, the obligation to avoid that, through a series of operation, the data were retrieved and made available even if stored on servers over which Google has no control, actually achieved the desired result[119];

- bluntly, there is no right to be forgotten to enforce in the current legislation (the DPD), even though it will be present in the GDPR once it is approved;

- even taking into account the right to be forgotten as it is defined in the GDPR, the decision does not seem to be applying it, because under Article 17 of the GDPR the data controller is obliged to "take all reasonable steps" to inform third parties of the deletion request, or to obtain the erasure from them[120]; whereas the *Google Spain* decision clearly stated that only the search engine, and not the original website, was obliged to de-index the data[121].

The case seems to cover a particular application of the right to object, because it targets a secondary processing of the data and not the data controller who originally processed the data. However, this is perfectly in line with the content of the right to object. In particular, while a controller (the original web site) is allowed to process the personal data pertaining to the DS, another one (the search engine) isn't[122].

---

[119] Correctly, European Court of Justice, *Decision C-131/12, ECLI:EU:C:2014:317.* par. 99 states that the DS has a right that "the information in question no longer be made available to the general public on account of its inclusion in such a list of results". This does not imply that the data controller must erase the data (*rectius*, the links to the location where the data are stored) completely.

[120] Depending on the exact formulation of Article 17, since there are several existing versions: one available to the public domain, one as an internal working document (recently leaked out), and a different proposal by the European Parliament which has been shown by European Commission, *Factsheet on the "Right to be Forgotten" ruling*. See also footnote 95 *supra*.

[121] Specifically, the Court, at European Court of Justice, *Decision C-131/12, ECLI:EU:C:2014:317.* par. 99 states that, under Article 12 subparagraph b and 14(1) subparagraph a of the DPD, the DS has a right that "the information in question no longer be made available to the general public on account of its inclusion in such a list of results". This does not imply that the data controller must erase the data (*rectius*, the links to the location where the data are stored) completely.

[122] The same conclusion has been reached by the Google Advisory Council (Floridi, L. et al. *The Advisory Council to Google on the Right to be Forgotten*. Tech. rep. Google Advisory Council, Feb. 2015, p. 5), according to which "the Ruling does not establish a general Right to be Forgotten", but rather "invokes a data subject's right to object to, and require cessation of, the processing of data about himself or herself".

6.3. Aftermath

The decision was generally welcomed with favour by data protection advocates, who saw an application of the right to be forgotten in it[123]. Nonetheless, the preferable interpretation is that the decision is not anchored to the right to be forgotten, at least not as it is formulated in the reform proposal[124]. While it can be assumed that the CJEU, in the application of existing DPD provisions, has undergone an evolutive interpretation

[123]In particular early commentators, for example Voss, W. G. "The Right to Be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment to the Proposed General Data Protection Regulation". In: *Journal of Internet Law* 18.1 (July 2014), pp. 3–7; Kropf, J. W. "Google Spain SL v. Agencia Española de Protección de Datos (AEPD). Case C-131/12". In: *The American Journal of International Law* 108.3 (July 2014), pp. 502–509. However, the resonance of the decision as enforcing the right to be forgotten still appears to be predominant in doctrine: see for example Crowther, H. "Google v Spain: is there now a 'right to be forgotten'?" In: *Journal of Intellectual Property Law & Practice* 9.11 (Nov. 2014), pp. 892–893; Van Eecke, P. and Cornette, A. "What the CJEU has actually decided in Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, No. C-131/12". In: *Computer Law Review International* 15.4 (Aug. 2014), pp. 101–107; Peron, S. "Il diritto all'oblio nell'era dell'informazione *on-line*". In: *Responsabilità civile e previdenza* LXXIX.4 (2014), pp. 1177–1191; Boix Palop, A. "El equilibrio entre los derechos del artículo 18 de la Constitución, el "derecho al olvido" y las libertades informativas tras la sentencia Google". In: *Revista General de Derecho Administrativo* 38 (Jan. 2015); Krošlák, D. "Practical implementation of the right to be forgotten in the context of Google Spain decision". In: *Communication Today* 6.1 (2015), pp. 59–71; Salarelli, A. "Ancora sul diritto all'oblio: cosa cambia dopo la sentenza della Corte di Giustizia Europea contro Google". In: *Italian Journal of Library, Archives, and Information Science* 6.1 (2015), pp. 147–160; Burden, K. "EU update". In: *Computer Law & Security Review* 31.1 (Feb. 2015), pp. 139–145; Bolton, R. L. I. "The Right to Be Forgotten: Forced Amnesia in a Technological Age". In: *The John Marshall Journal of Information Technology and Privacy Law* 31.2 (2015), pp. 133–144; Popoli, A. R. "Il diritto all'oblio approda alla Corte Europea dei Diritti dell'Uomo: ma non viene menzionato". In: *Giustizia Civile.com* (Mar. 2015); Mantelero, A. "Il futuro regolamento EU sui dati personali e la valenza "politica" del caso Google: ricordare e dimenticare nella *digital economy*". In: *Il diritto dell'informazione e dell'informatica* XXX.4–5 (July 2014), pp. 681–701; Kranenborg, H. "Google and the Right to Be Forgotten". In: *European Data Protection Law Review* 1.1 (2015), pp. 70–79; Resta, G. and Zeno-Zencovich, V., eds. *Il Diritto All'Oblio Su Internet Dopo La Sentenza Google Spain*. Vol. 3. Consumatori e Mercato. Roma TrE-Press, Apr. 2015 and maybe Frantziou, E. "Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, *Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*". In: *Human Rights Law Review* 14.4 (Oct. 2014), pp. 761–777, although some properly highlight the difference between the traditional concept of a right to be forgotten and its definition in Article 17 of the proposed Regulation. Some authors (Carvalho, S. de. "The right to be forgotten: an analysis of the CJEU's Google Spain judgment". In: *Proceedings of the 3rd Electronic International Interdisciplinary Conference (EIIC)*. vol. 3. EDIS - Publishing Institution of the University of Zilina, Sept. 2014, pp. 202–210; Iglezakis, I. *The Right to Be Forgotten in the Google Spain Case (Case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet?* `http://ssrn.com/abstract=2472323`. July 2014) even state that the Court maintains that the right to be forgotten is rooted in the general principles of the Directive, but such claims do not appear to be supported in the ruling.

[124]In this sense, the Advocate General points out in Jääskinen, *Opinion of Advocate General Jääskinen* that the right to be forgotten cannot be inferred from the current legislation. Also Kelsey, E. "Google Spain SL and Google Inc v AEPD and Mario Costeja Gonzalez: protection of personal data, freedom of information and the "right to be forgotten"". In: *European Human Rights Law Review* 4 (2014), pp. 395–400; Kulk, S. and Zuiderveen Borgesius, F. J. "Google Spain v. González: Did the Court Forget About Freedom of Expression?" In: *European Journal of Risk Regulation* 5.3 (2014), pp. 389–398; Dubois, P.-A. "Search engines and data protection - a welcome practical approach by the Advocate General". In: *Computer and Telecommunications Law Review* 19.7 (2013), pp. 206–208; Cofone, I. N. "Google v. Spain: A Right to Be Forgotten?" In: *Chicago-Kent Journal of International and Comparative Law* 15.1 (Jan. 2015), pp. 1–11, and apparently Scannicchio, T. "Tutela della privacy: motori di ricerca e diritto all'oblio". In: *Giurisprudenza Italiana* (June 2014), pp. 1323–1325 who avoids relating the decision to Article 17.

that runs along the same line of a principle underlying the reform proposal[125], the assumption[126] that the judges have anticipated some of the provisions of the reform cannot be upheld.

The importance of the *Google Spain* decision was also felt when, on 10 July 2014, the Italian Authority for the protection of personal data (*Garante per la protezione dei dati personali*) issued itself a decision against Google Inc.[127]. The Garante found that the Google Spain decision enforces the *diritto all'oblio*[128]. As a follow-up to this decision, the Garante, on the basis of an undisclosed verification protocol[129], imposed specific measures[130] upon Google, including greater transparency in the privacy policy, consent to profiling, full right to object, anonymization, deletion of personal information, and delisting of results[131]. The decision of the *Garante* is quite different from that of the CJEU, since it requires Google "to adopt a data deletion policy" based on the sole request of authenticated users. This is definitely more in line with the European draft concept of the right to be forgotten. In short, and approximately, the CJEU applies the *diritto all'oblio*, whereas the *Garante* applies the right to be forgotten.

Google's reaction to the Google Spain decision has been twofold. On one side, it has complied with the ruling, by creating an online form[132] which allows DS to request deletion from the search engine results. The form explicitly mentions CJEU's decision C-131/12 as the basis for the deletion request. The form does not require the DS to enter a motivation for the deletion request; this is more in line with the right to be for-

---

Markou, C. "The '*Right to Be Forgotten*': Ten Reasons Why It Should Be Forgotten". In: *Reforming European Data Protection Law*. Ed. by Gutwirth, S. et al. Vol. 20. Law, Governance and Technology Series. Springer Netherlands, Oct. 2014. Chap. 8, pp. 203–226 observes that the absence of a reference to the expression "right to be forgotten" in the decision suggests that the right granted by Article 17 of the proposed Regulation can be achieved by means of erasure, without the need of a "forgotten" label; however, this position seems to underestimate the differences between the content of Article 17 and the CJEU ruling.

[125] Also in the light of the length of the approval procedure and the difficulties that the reform is encountering.

[126] Mantelero, "Il futuro regolamento EU sui dati personali e la valenza "politica" del caso Google: ricordare e dimenticare nella *digital economy*".

[127] Garante per la protezione dei dati personali. *Decision Setting forth Measures Google Inc. Is Required to Take to Bring the Processing of Personal Data under Google's New Privacy Policy into Line with the Italian Data Protection Code – 10 July 2014*. `http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3295641`. July 2014. The decision was issued as the outcome of an *ex officio* verification concerning the new Google privacy policy. Other EU DPAs have undergone similar procedures (Rauhofer, J. "Of Men and Mice: Should the EU Data Protection Authorities' Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle?" In: *European Data Protection Law Review* 1.1 (2015), pp. 5–15).

[128] The Italian *diritto all'oblio* is conceptually different (and less incisive) from the right to be forgotten as it is defined in the draft Regulation. See Subsection 5.3 *supra*.

[129] Garante per la protezione dei dati personali. *Approvazione del protocollo di verifica che disciplina le attività di controllo da parte del Garante sulle prescrizioni impartite a Google il 10 luglio 2014 – 22 gennaio 2015*. `http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3738244`. Jan. 2015.

[130] Garante per la protezione dei dati personali. *Google to comply with the privacy measures set forth by the Italian DPA*. `http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3740585`. Feb. 2015.

[131] Distinguishing deletion of personal data and delisting of results corroborates the opinion that the Google Spain decision does not enforce the right to be forgotten.

[132] `https://support.google.com/legal/contact/lr_eudpa?product=websearch`.

gotten than the right to object, which normally requires the DS to motivate or justify the objection. Sources report that a large number of users have been requesting deletion[133] On the other hand, it established an advisory council[134] to discuss the Google Spain decision. The advisory council published a report[135] which defines the criteria and procedures that should be adopted when assessing a delisting request by a DS. The report notes that an evaluation of the possible harm that might come to the DS is required when assessing a delisting request, to guarantee the correct balancing between the data protection rights of the DS and the "interest of the general public in having [...] access to the information"[136]. The actual presence of a harm was disregarded by the CJEU.

6.4. The decision by the European Court of Human Rights

On September 18, 2014, another significant decision was issued, this time by the European Court of Human Rights, that might add new fuel to the discussion on the right to be forgotten. The decision[137] states that the retention of personal data even in the specific case implied a violation of the claimant's rights, because the processing of those data was no longer justified by the original purpose they were collected for. According to the few commentators[138], the Court, without expressly mentioning it, based its decision upon the right to be forgotten.

The juridical basis is necessarily different. While the CJEU decided according to the DPD, the European Court based its decision on Article 8 of the ECHR.

By ruling in favor of the claimant on the basis of an obligation to *erase* personal data, the right invoked by the European Court of Human Rights is closer to the right to be forgotten[139] than the obligation imposed by the CJEU. The duty to erase the

[133] For one, Cutlack, G. *Google Swamped by 'Right to be Forgotten' Deletion Requests*. `http://www.gizmodo.co.uk/2014/07/google-swamped-by-right-to-be-forgotten-deletion-requests/`. July 2014 reports that, as of 11 July 2014, 70,000 requests concerning 250,000 web pages were received.

[134] `https://www.google.com/advisorycouncil/`.

[135] Floridi et al., *The Advisory Council to Google on the Right to be Forgotten*.

[136] Ibid., p. 6.

[137] European Court of Human Rights. *Affaire Brunet c. France*. `http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-146389`. Sept. 2014. The case concerns a man whose data were placed in a criminal archive, but after he reached a mediation his data were not erased, despite his judicial request for their erasure. The claimant complained that retaining the data for the prescribed duration of twenty years despite the mediation was illegitimate, and the European Court upheld his claim.

[138] Gaté, J. "STIC : la France doit respecter un certain droit à l'oubli dans ses fichiers policiers". In: *Dalloz Actualité* (Sept. 2014); Popoli, "Il diritto all'oblio approda alla Corte Europea dei Diritti dell'Uomo: ma non viene menzionato". The latter observes that there is a significant difference between the traditional concepts of the *droit à l'oubli* and the decision by the European Court. Normally, the *droit à l'oubli* is anchored to the lack of general interest in some information after a significant amount of time. In the case under examination, the Court applies the same right even in the absence of a lengthy time span. The factual basis, according to the author, appears to be the presumption of innocence of the claimant.

[139] According to Popoli, "Il diritto all'oblio approda alla Corte Europea dei Diritti dell'Uomo: ma non viene menzionato", the decision by the European Court is an application of the right to be forgotten, *which was previously applied* by the CJEU. The author seems to overlook the fundamental differences between the content of the two decisions.

personal data from the original source is what the CJEU did not (and probably could not) enforce.

7. Conclusions

In an age of instant access to vast amount of material, policy makers must search for solutions which allow digital citizens the ability to maintain control over the image they present to the world. The DPD represented a step in this direction. Adopted in 1995, during the infancy of digital age, it represented a progressive protection regime which addressed technological developments of that age. Since then the Internet has exploded and changed the landscape of what it means to be a digital citizen. It has transformed the concepts of privacy, access and consent.

Yet with each action comes a reaction. One such action is currently being undertaken in the form of the GDPR, which seeks to shift the balance of power away from the data controllers in favour of the DSs, if only ever so slightly. Through its adoption of a right to be forgotten the EU will simplify and embolden citizens' right to control their image in the web. The existing provisions which allow limited editorial control based upon objection or consent will be replaced. Yet, in the mean time, the CJEU's decision against Google Spain has, to a certain extent, complicated the debate. Does the decision recognize a previously existing right to be forgotten? Or rather is the Court simply morphing the right to objection in order to fill a void in existing law in order to protect rights of users within the spirit of existing legislation?

The Court could not enforce a right that does not exist in the current legislation. And yet, what it could do was to plant the seeds, to affirm something that goes in the direction of the right to be forgotten, although it is a mere application of the right to object.

What did the Court achieve? Very much, and very little. The clear statement that the search engine *is* a data controller is a definite step forward in adapting the existing data protection principles to the new technological context. And yet, on a concrete ground, the effect on the case was the opposite than the upholding of the claim actually aimed at. The original content on the Spanish website is still available; it cannot be found on Google Spain using only the name of the claimant as the search string, but the search service from different countries still displays those results, as does the Spanish service by using a more detailed search string; and the claimant has earned a lot of visibility, which was probably the opposite of what he wanted.

Under the existing legal framework, the Court could not require the original data to be erased. At any rate, those data (actually a copy of an old issue of a newspaper from the archive repository) were unlikely to be looked for in the original website, thus not causing any harm to the claimant's reputation. The harm came from the fact that the search engine brought under present light something that had no real interest. The decision finds a balance between the rights granted by Articles 8 and 11 of the Charter: once the public interest in the information on the subject has ceased, the right to the DS's personal data must prevail.

The Court stopped here. The decision was based on the context "here and now", and several critical issues were left open. First off, many search strings, involving

or not the name of the DS, display those results. To what extent should the search engine be forced to disable those results? Of course, if Google is obliged to avoid the indexing of those results in response to more search strings, the limitation to the freedom of information is stronger, and at some point the balance shifts. Finding the perfect balance is extremely hard, but that topic was not discussed in the decision.

Second, the Court discussed the facts in a static perspective. If the DS runs for a political career or a position with significant public responsibilities, then maybe what has been considered an obsolete and irrelevant information about his past financial problems may become interesting again in the eyes of the public. The transparency of the information to the public might suddenly shift the balance back in favor of the ease in finding those results. A dynamic analysis of the possible scenarios is not available yet.

It seems that the Court planted a seed. Possibly, it used the case to put its endorsement upon an idea which has been struggling to gain full approval from the legislature of the European Union, even without recognizing its existence under the current legal framework: the right to be forgotten. Quite possibly, the Court is sending a signal that it will recognize the essence of a right until it is adopted into codified law.

References

Acquisti, A. "Nudging Privacy: The Behavioral Economics of Personal Information". In: *IEEE Security & Privacy* 7.6 (Dec. 2009), pp. 82–85.

Barbas, S. "The Death of the Public Disclosure Tort: A Historical Perspective". In: *Yale Journal of Law & The Humanities* 22.2 (2010), pp. 171–215.

Bartolini, C. *Privacy in the information society and the principle of necessity*. Saarbrücken, Germany: LAP Lambert Academic Publishing, Feb. 2013.

Beyleveld, D. and R. Brownsword. *Consent in the law*. Legal Theory Today. 16C Worcester Place, Oxford OX1 2JW, UK: Hart Publishing, Jan. 2007.

Bloustein, E. J. "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser". In: *N.Y.U. Law Review* 39.6 (Dec. 1964), pp. 962–1007.

Boix Palop, A. "El equilibrio entre los derechos del artículo 18 de la Constitución, el "derecho al olvido" y las libertades informativas tras la sentencia Google". In: *Revista General de Derecho Administrativo* 38 (Jan. 2015).

Bolton, R. L. I. "The Right to Be Forgotten: Forced Amnesia in a Technological Age". In: *The John Marshall Journal of Information Technology and Privacy Law* 31.2 (2015), pp. 133–144.

Brownsword, R. "Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality". In: *Reinventing Data Protection?* Ed. by Gutwirth, S., Poullet, Y., De Hert, P., Terwangne, C. de, and Nouwt, S. Springer Netherlands, 2009. Chap. 2, pp. 83–110.

Burden, K. "EU update". In: *Computer Law & Security Review* 31.1 (Feb. 2015), pp. 139–145.

Carvalho, S. de. "The right to be forgotten: an analysis of the CJEU's Google Spain judgment". In: *Proceedings of the 3rd Electronic International Interdisciplinary Conference (EIIC)*. Vol. 3. EDIS - Publishing Institution of the University of Zilina, Sept. 2014, pp. 202–210.

Cate, F. H. "The EU Data Protection Directive, Information Privacy, and the Public Interest". In: *Iowa Law Review* 80.3 (May 1995), pp. 431–443.

Cofone, I. N. "Google v. Spain: A Right to Be Forgotten?" In: *Chicago-Kent Journal of International and Comparative Law* 15.1 (Jan. 2015), pp. 1–11.

Corte di Cassazione, III sezione civile. "Sentenza 9 aprile 1998, n. 3679". In: *Il Foro Italiano* 121.6 (June 1998), pp. 1833/1834–1839/1840.

Crowther, H. "Google v Spain: is there now a 'right to be forgotten'?" In: *Journal of Intellectual Property Law & Practice* 9.11 (Nov. 2014), pp. 892–893.

Curren, L. and J. Kaye. "Revoking consent: A 'blind spot' in data protection law?" In: *Computer Law & Security Review* 26.3 (May 2010), pp. 273–283.

Cutlack, G. *Google Swamped by 'Right to be Forgotten' Deletion Requests*. http://www.gizmodo.co.uk/2014/07/google-swamped-by-right-to-be-forgotten-deletion-requests/. July 2014.

Dubois, P.-A. "Search engines and data protection - a welcome practical approach by the Advocate General". In: *Computer and Telecommunications Law Review* 19.7 (2013), pp. 206–208.

Elgesem, D. "The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data". In: *Ethics and Information Technology* 1.4 (Dec. 1999), pp. 283–293.

European Commission. *Why do we need an EU data protection reform?* http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf. 2012.

— *Factsheet on the "Right to be Forgotten" ruling*. http://ec.europa.eu/justice/newsroom/data-protection/news/140602_en.htm. June 2014.

European Court of Human Rights. *Affaire Brunet c. France*. http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-146389. Sept. 2014.

European Court of Justice. *Decision C-131/12, ECLI:EU:C:2014:317*. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131. May 2014.

European Data Protection Supervisor. *Opinion of the European Data Protection Supervisor*. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf. Mar. 2012.

— *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*. http://europa.eu/rapid/press-release_EDPS-14-6_en.htm. Mar. 2014.

European Union Agency for Fundamental Rights. *Handbook on European data protection law*. Apr. 2014.

Faden, R. R. and T. L. Beauchamp. *A History and Theory of Informed Consent*. 200 Madison Avenue, New York, New York 10016, USA: Oxford University Press, 1986.

Fauvarque-Cosson, B. and D. Mazeaud. *European Contract Law: Materials for a Common Frame of Reference: Terminology, Guiding Principles, Model Rules*. European Private Law. München: Sellier, 2008.

Floridi, L., S. Kauffman, L. Kolucka-Zuk, F. La Rue, S. Leutheusser-Schnarrenberger, J.-L. Piñar, P. Valcke, and J. Wales. *The Advisory Council to Google on the Right to be Forgotten*. Tech. rep. Google Advisory Council, Feb. 2015.

Frantziou, E. "Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, *Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*". In: *Human Rights Law Review* 14.4 (Oct. 2014), pp. 761–777.

Garante per la protezione dei dati personali. *Decision Setting forth Measures Google Inc. Is Required to Take to Bring the Processing of Personal Data under Google's New Privacy Policy into Line with the Italian Data Protection Code – 10 July 2014*. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3295641. July 2014.

— *Approvazione del protocollo di verifica che disciplina le attività di controllo da parte del Garante sulle prescrizioni impartite a Google il 10 luglio 2014 – 22 gennaio 2015*. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3738244. Jan. 2015.

— *Google to comply with the privacy measures set forth by the Italian DPA*. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3740585. Feb. 2015.

Gaté, J. "STIC : la France doit respecter un certain droit à l'oubli dans ses fichiers policiers". In: *Dalloz Actualité* (Sept. 2014).

Geiger, A. "Die Einwilligung in die Verarbeitung von persönlichen Daten als Ausübung des Rechts auf informationelle Selbstbestimmung". In: *Neue Zeitschrift für Verwaltungsrecht* 8.1 (Jan. 1989). https://beck-online-beck-de.proxy.bnl.lu/?typ=reference&y=300&z=NVWZ&b=1989&s=35&n=1, pp. 35–37.

Gisclard, T. "Consent in Licenses of Personality Rights". In: *European Review of Private Law* 22.3 (2014), pp. 345–370.

Giurgiu, A. and G. Lommel. "A New Approach To EU Data Protection". In: *Die Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (KritV)* 97.1 (2014), pp. 10–27.

Goldstein, J. "For Harold Lasswell: Some Reflections on Human Dignity, Entrapment, Informed Consent, and the Plea Bargain". In: *The Yale Law Journal* 84.4 (Mar. 1975), pp. 683–703.

Gutwirth, S., Y. Poullet, P. De Hert, C. de Terwangne, and S. Nouwt, eds. *Reinventing Data Protection?* Springer Netherlands, 2009.

Hoboken, J. van. *The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember*. Tech. rep. European Commission, May 2013.

Hoofnagle, C. J., A. Soltani, N. Good, D. J. Wambach, and M. J. Ayenson. "Behavioral Advertising: The Offer You Can't Refuse". In: *Harvard Law & Policy Review* 6.2 (Aug. 2012), pp. 273–296.

Hurd, H. M. "The moral magic of consent". In: *Legal Theory* 2.02 (June 1996), pp. 121–146.

Iglezakis, I. *The Right to Be Forgotten in the Google Spain Case (Case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet?* http://ssrn.com/abstract=2472323. July 2014.

Jääskinen, N. *Opinion of Advocate General Jääskinen*. http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=416370. June 2013.

Kelsey, E. "Google Spain SL and Google Inc v AEPD and Mario Costeja Gonzalez: protection of personal data, freedom of information and the "right to be forgotten"". In: *European Human Rights Law Review* 4 (2014), pp. 395–400.

Kosta, E. *Consent in European Data Protection Law*. Vol. 3. Nijhoff Studies in European Union Law. Plantijnstraat 2, 2321 JC Leiden, The Netherlands: Brill, Mar. 2013.

Kranenborg, H. "Google and the Right to Be Forgotten". In: *European Data Protection Law Review* 1.1 (2015), pp. 70–79.

Kropf, J. W. "Google Spain SL v. Agencia Española de Protección de Datos (AEPD). Case C-131/12". In: *The American Journal of International Law* 108.3 (July 2014), pp. 502–509.

Krošlák, D. "Practical implementation of the right to be forgotten in the context of Google Spain decision". In: *Communication Today* 6.1 (2015), pp. 59–71.

Kulk, S. and F. J. Zuiderveen Borgesius. "Google Spain v. González: Did the Court Forget About Freedom of Expression?" In: *European Journal of Risk Regulation* 5.3 (2014), pp. 389–398.

Lando, O. and H. Beale, eds. *The Principles Of European Contract Law, Parts I And II*. Kluwer Law International, Nov. 1999.

Manson, N. C. and O. O'Neill. *Rethinking Informed Consent in Bioethics*. University Printing House, Shaftesbury Road, Cambridge, CB2 8BS, United Kingdom: Cambridge University Press, Apr. 2007.

Mantelero, A. "The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'". In: *Computer Law & Security Review* 29.3 (June 2013), pp. 229–235.

— "Il futuro regolamento EU sui dati personali e la valenza "politica" del caso Google: ricordare e dimenticare nella *digital economy*". In: *Il diritto dell'informazione e dell'informatica* XXX.4–5 (July 2014), pp. 681–701.

Markou, C. "The '*Right to Be Forgotten*': Ten Reasons Why It Should Be Forgotten". In: *Reforming European Data Protection Law*. Ed. by Gutwirth, S., Leenes, R., and Hert, P. de. Vol. 20. Law, Governance and Technology Series. Springer Netherlands, Oct. 2014. Chap. 8, pp. 203–226.

McClurg, A. J. "A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling". In: *Northwestern University Law Review* 98.1 (2003), pp. 63–143.

Messinetti, D. "Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali". In: *Rivista critica del diritto privato* 16.3 (1998), pp. 339–407.

O'Shea, T. *Consent in History, Theory and Practice*. Tech. rep. http://autonomy.essex.ac.uk/consent-in-history-theory-and-practice. University of Essex: Essex Autonomy Project, Mar. 2011.

Peron, S. "Il diritto all'oblio nell'era dell'informazione *on-line*". In: *Responsabilità civile e previdenza* LXXIX.4 (2014), pp. 1177–1191.

Popoli, A. R. "Il diritto all'oblio approda alla Corte Europea dei Diritti dell'Uomo: ma non viene menzionato". In: *Giustizia Civile.com* (Mar. 2015).

Popovici, A. "Personality Rights - A Civil Law Concept". In: *Loyola Law Review* 50.2 (2004), pp. 349–358.

Prosser, W. L. "Privacy". In: *California Law Review* 48.3 (Aug. 1960), pp. 383–423.

Rallo Lombarte, A. "El derecho al olvido y su protección". In: *Telos* 85 (2010), pp. 104–108.

Rauhofer, J. "Of Men and Mice: Should the EU Data Protection Authorities' Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle?" In: *European Data Protection Law Review* 1.1 (2015), pp. 5–15.

Reimer, S. "Die datenschutzrechtliche Zustimmung". MA thesis. Universitätsring 1, 1010 Wien, Austria: Universität Wien, 2010.

Resta, G. "Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali". In: *Rivista critica del diritto privato* 18.2 (2000), pp. 299–333.

Resta, G. and V. Zeno-Zencovich, eds. *Il Diritto All'Oblio Su Internet Dopo La Sentenza Google Spain*. Vol. 3. Consumatori e Mercato. Roma TrE-Press, Apr. 2015.

Robbers, G. "Der Grundrechtsverzicht. Zum Grundsatz 'volenti non fit iniuria' im Verfassungsrecht". In: *Juristische Schulung* 25.12 (Dec. 1985), pp. 925–931.

Rodotà, S. *Elaboratori elettronici e controllo sociale*. Vol. 2. Quaderni dell'Irsta. Strada Maggiore 37, 40125 Bologna, Italy: Il Mulino, 1973.

Rouvroy, A. and Y. Poullet. "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy". In: *Reinventing Data Protection?* Ed. by Gutwirth, S., Poullet, Y., De Hert, P., Terwangne, C. de, and Nouwt, S. Springer Netherlands, 2009. Chap. 2, pp. 45–76.

Rubinstein, I. S., R. D. Lee, and P. M. Schwartz. "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches". In: *The University of Chicago Law Review* 75.1 (2008), pp. 261–285.

Salarelli, A. "Ancora sul diritto all'oblio: cosa cambia dopo la sentenza della Corte di Giustizia Europea contro Google". In: *Italian Journal of Library, Archives, and Information Science* 6.1 (2015), pp. 147–160.

Santoro-Passarelli, F. *Dottrine generali del diritto civile*. 9th ed. Eugenio Jovene, 1997.

Scannicchio, T. "Tutela della privacy: motori di ricerca e diritto all'oblio". In: *Giurisprudenza Italiana* (June 2014), pp. 1323–1325.

Schermer, B. W., B. Custers, and S. van der Hof. "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection". In: *Ethics and Information Technology* 16.2 (Mar. 2014), pp. 171–182.

Van Eecke, P. and A. Cornette. "What the CJEU has actually decided in Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, No. C-131/12". In: *Computer Law Review International* 15.4 (Aug. 2014), pp. 101–107.

Voss, W. G. "The Right to Be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment to the Proposed General Data Protection Regulation". In: *Journal of Internet Law* 18.1 (July 2014), pp. 3–7.

Warren, S. D. and L. D. Brandeis. "The right to privacy". In: *Harvard Law Review* IV.5 (Dec. 1890), pp. 193–220.