The Shaky Ground of the Right to Be Delisted

Miquel Peguera, *Universitat Oberta de Catalunya*
THE SHAKY GROUND OF THE RIGHT TO BE DELISTED

Miquel Peguera*

It has long been discussed whether individuals should have a “right to be forgotten” online to suppress old information that could seriously interfere with their privacy and data protection rights. In the landmark case of Google Spain v AEPD, the Court of Justice of the European Union addressed the particular question of whether, under EU Data Protection Law, individuals have a right to have links delisted from the list of search results, in searches made on the basis of their name. It found that they do have this right – which can be best described as a “right to be delisted” – when some conditions are met.

The ruling, which imposes on search engines the duty to assess and accommodate delisting requests, has proven to be highly controversial. Strong feelings have been expressed either in favor or against it, in what may be seen as a clash between the values of personal data protection and freedom of expression.

This article does not delve into this underlying debate. Instead, it aims to explore the solidness of the ground on which the right is based. It begins by providing an overview of the relevant elements of EU data protection law so as to allow readers not familiar with its nuances to properly follow the discussion. After presenting the facts of Google Spain, both at national and EU level, the article discusses how the ‘right to be delisted’ was crafted by the CJEU. It argues that it is based on shaky ground, as it is premised on the characterization of search engines as “data controllers”, which is arguably at odds with their intermediary role and – in the absence of specific safeguards – makes their activity largely incompatible with the data protection legal framework. Moreover, the article discusses how the Court failed to devise a proper balance of the different rights at stake, particularly that of freedom of expression and information. It suggests that the intermediary role of generalist search engines should be adequately protected, both under the data protection legal framework as well as under the liability limitation scheme established by the E-Commerce Directive. This, however, is not likely to be achieved in the near future. A careful approach by national courts and data protection authorities is thus suggested as a way to fix some of the shortcomings identified in the ruling.

* Miquel Peguera, PhD, mpeguera@uoc.edu. Associate Professor of Law, Universitat Oberta de Catalunya (Barcelona, Spain). Affiliate Scholar, Stanford Law School Center for Internet and Society. Researcher, Internet Interdisciplinary Institute (IN3). Thanks to Agustí Cerrillo, Giancarlo Frosio, Eric Goldman, James Grimmelmann, Daphne Keller, Alessandro Mantelero and Frank Pasquale.
INTRODUCTION

The U.S. should adopt the “right to be forgotten” online. This was the motion under discussion in an Intelligence Squared U.S. debate held in New York on March 11, 2015.¹ Two teams were putting forward their arguments for and against the motion before the audience,² which would cast their vote at the end of the debate. The discussion focused on whether it would be advisable for the U.S. to establish a right similar to that recognized in the landmark ruling handed down in May 13, 2014 by the Court of Justice of the

¹ See intelligencesquaredus.org. Debate available at https://www.youtube.com/watch?v=yvDzW-2qIZQ.
² In favor of the motion, Eric Posner and Paul Nemitz. Against the motion, Jonathan Zittrain and Andrew McLaughlin. The debate was moderated by John Donvan.
European Union (CJEU), in the Google Spain case.\(^3\) There the CJEU addressed the issue of whether individuals may obligate a search engine to remove search results linking to information that included personal data related to them. The Court found that under EU law on personal data protection, a search engine operator does have the obligation, under the appropriate circumstances, to accommodate requests from individuals who do not want links to information containing their personal data displayed among search results when a search based on their name is carried out.

One might think that such a right is meant to block access to defamatory statements. However, this is not the case – defamation law has its own protection mechanisms. One may think, then, that it is confined to cases where the information is false or inaccurate. But it is not – while the right may be exercised with regard to inaccurate information, an individual may also request the delisting of *perfectly accurate information*. Then, perhaps the right relates to the unauthorized disclosure of private information? The ruling answered again in the negative – the concerned person may request the removal *even if the concerned information is not private*. Does it relate then to situations where the dissemination of that information, even if accurate and public, is prejudicial to that person? Once more, the Court said no – *there is no need for the dissemination of the information to be prejudicial* to the individual. However, surely the ruling stated that the information must be somehow unlawful and established that the original source to which the result linked also had to be removed, right? Again, this was not necessarily so. The original source of information, for instance, a digital newspaper, might be entitled to publish that information and to keep it online, and still the search engine would be obliged not to display links to it in searches made on the basis of that person’s name.

Then, did the ruling say that an individual has the right to request the removal of links to non-defamatory, truthful, public and harmless information about her, even if it is lawful for the original source to publish and keep that information online? Yes, that is what the Court essentially held. Actually, it found that the right may be exercised whenever the information is “inadequate, irrelevant, no longer relevant or excessive”, unless there is a preponderant right of the public in accessing that information by the means of a search using the person’s name – which could be the case when that person is in the public eye.

However broad this right may seem, the underlying situations the court was trying to address are by no means necessarily frivolous or unmeritorious. Very real and pressing  

problems for private persons lie on the whole idea of having some degree of control over one’s personal information online. True, the Court ruled out the need to prove prejudice, but it nevertheless decided the case on the assumption that the individual might potentially suffer real harm, as a consequence of people stumbling on that information when typing the individual’s name on Google.

It has been long argued in connection with this issue that the-web-that-never-forgets seems ever ready to produce piecemeal fragments of old information about individuals, often entirely out of context, that may result in serious personal setbacks – perhaps causing someone to be denied a job; to lose social standing; to be unable to escape a past and build a new life. Viktor Mayer-Schönberger has written extensively about the perils that may arise from the fact that digital technology prevents us from forgetting and establishes remembering as the new default. Some of those ideas were included in the 2012 proposal for a new EU General Data Protection Regulation, still under discussion, where a provision on “the right to be forgotten” deals more generally with the possibility of requiring the removal of personal information from the Internet.

Google Spain, however, did not tackle the issue of removing information from the Internet generally, but focused on a much more narrow aspect. It specifically considered the problem that arises when a piece of information, which would have passed otherwise unnoticed, buried in the archives of a newspaper or official bulletin, is brought to the public’s attention through Internet search engines; and the fact that person-based queries may produce a more or less detailed profile of the individual.

As will be discussed below, seeking to reach a somehow moderated, more acceptable result, the court chose to creatively sidestep the question of whether the

---

4 Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (2009). The author argues that digital remembering negates time, offering a “synthetic past reconstructed from the limited information digital memory has stored about it, an utterly skewed patchwork devoid of time and open to manipulation in both what it contains, and what it doesn’t.” (id. at 123). He puts forward that “[f]rom the perspective of the person remembering, digital memory impedes judgment. From the perspective of the person remembered, however, it denies development, and refuses to acknowledge that all humans change all the time.” (id. at 125).

individual may request the removal of said information from the search engine index altogether, and instead limited itself to acknowledging the right to request the removal of the link from the list of search results when a search is carried out based on the name of that person – as long as there is not a preponderant interest on the part of the public in having access to that information by means of such a search. This, along with the fact that, in general, the content will remain on the original source, means that the information could still be found in searches using terms other than the name of the person. In this vein, the right envisioned by the Court can be best described as a “right to be delisted.”

From a U.S. law perspective, either the more general “right to be forgotten” envisioned in the proposal for the EU General Data Protection Regulation or the more specific search engines’ duty to delist would seem difficult to accommodate, although it has been noted that U.S. law also recognizes some limited forms of a right to be forgotten. Many U.S. commentators oppose a right with such a broad reach, even though they acknowledge that it tries to address a real problem. In contrast, some others have shown sympathy for this new development, and some have noted that, in fact, U.S. privacy law might be leaning towards a more European approach.

6 See, e.g. Ravi Antani, The Resistance of Memory: Could the European Union’s Right to be Forgotten Exist in the United States? 30 BERKELEY TECH. L.J. (2015, forthcoming); Robert K. Walker, The Right to be Forgotten, 64 HASTINGS L.J. 257 (2012) (arguing that only a limited form of the “right to be forgotten”, namely, the right to delete voluntarily submitted data, would be compatible with U.S. constitutional law); Thomas H. Koenig and Michael L. Rustad, Digital Scarlet Letters: Social Media Stigmatization of the Poor and What Can Be Done, 93 NEB. L. REV. 592 (2015) (“[i]f the U.S. adopts a digital eraser, it will be more limited that the EU’s right to be forgotten because of the need to balance expression with the right to a reputational fresh start.”); Robert Lee Bolton III, The Right To Be Forgotten: Forced Amnesia In A Technological Age, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 133 (2015) (noting public policy objections to a right to be forgotten).

7 Daniel Solove, What Google Must Forget: The EU Ruling on the Right to Be Forgotten (May 13, 2014), https://www.linkedin.com/pulse/20140513230300-2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten (“the Children’s Online Privacy Protection Act provides for a right to delete personal data. The Fair Credit Reporting Act restricts the ability of consumer reporting agencies to report on bankruptcies and criminal proceedings that are beyond a certain number of years old.”).

8 Regarding the right to be forgotten as drafted in the GDPR Proposal, supra note 5, see e.g. Jeffrey Rosen, The Right to Be Forgotten, 64 STAN. L. REV. ONLINE 88 (2012) (arguing that it “represents the biggest threat to free speech on the Internet in the coming decade”).

9 See e.g. Jonathan Zittrain, Don’t Force Google to ‘Forget’, NEW YORK TIMES (May 14, 2014).

10 See Eric Posner, We All Have the Right to be Forgotten, SLATE (May 14, 2014), http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html. See also Koenig and Rustad, supra note 6 (“[t]he EU’s “right to erasure” provision would be particularly useful to America’s poor and less educated who seek to remove evidence of their spoiled identity.”).

This article seeks to shed light onto the “right to be delisted” by providing valuable insight into how this right ended up being acknowledged by the CJEU on the basis of the EU legal framework on data protection, thus enabling a better understanding of the right – and of its limitations and shortcomings. Part I offers an introduction to the current EU legal framework on data protection, covering the concepts that were the most relevant in the crafting of this right. It is meant to provide readers not familiar with its nuances enough information so as to easily follow the legal discussion. The peculiar notion of data protection as a fundamental right to control one’s personal data, which goes beyond the notion of privacy, is essential to understand the recognition of this right. Part II presents the facts and main holdings of the landmark Google Spain case. Part III moves on to discuss the legal ground of the right to be delisted. Subpart III (A) argues that the right is on shaky ground, as its main premise – the characterization of a search engine as a “data controller” – is problematic. Subpart III (B) puts forward the need to protect search engines’ intermediary role. It discusses their legal status under the liability limitations set forth in EU law, and suggests that data protection law should take this role into account, thus crafting specific provisions so as to avoid imposing on search engines a bundle of obligations which are at odds with their actual functions and possibilities. Subpart III (C) further discusses the specific legal basis and conditions to request delisting. Subpart III (D) explores the shortcomings that can be identified in the balancing of rights envisioned by the Court. Next, Part IV considers how the scenario may change under the future General Data Protection Regulation, and suggests that national courts and data protection authorities carry out a careful balancing in the particular cases brought before them so as to overcome some of the problems detected. Finally, part VI offers a brief conclusion.

The audience in the abovementioned debate was finally not persuaded by the idea of adopting such a right in the U.S. – though nonetheless, other polls suggest a more favorable point of view. Indeed, a right to have even a limited control of what search engines may display in search results about oneself is unsurprisingly controversial. There are many assumptions involved, including different visions of key ideological aspects, which have made the academic and social discussion sometimes vehement. This article will not take sides on that front. However, in exploring the nuances of this right within the forward that American privacy law is starting to move in the direction of the European framework).

12 See Daniel Humphries, U.S. Attitudes Toward the ‘Right to Be Forgotten’, SOFTWARE ADVICE, (Sep. 5, 2014), http://www.softwareadvice.com/security/industryview/right-to-be-forgotten-2014/ (finding that “61% of Americans believe some version of the right to be forgotten is necessary.”).
legal context in which it emerged, it will underscore some of its problems and call for an
approach that better reflects the intermediary nature of search engines. All in all, the article
seeks to contribute to a better understanding of a right which appears to have come to stay
in the EU, and may certainly influence legal developments in other jurisdictions.

I. THE EU LEGAL FRAMEWORK ON PERSONAL DATA PROTECTION

Unlike in other jurisdictions, EU Data Protection law is not essentially about
preventing privacy harms, but about granting individuals the right to control third-party
uses of their personal data. The right to the “protection of personal data” is recognized by
the EU Charter of Fundamental Rights (“the Charter”), where it is established in Art. 8, separately from the right to “respect for private and family life”, laid down in Art. 7. This autonomous characterization in the Charter represented a notable departure from the traditional understanding of data protection as a mere facet of the right to privacy. Being recognized as a fundamental right, data protection enjoys the highest status within EU law – along with the rest of fundamental rights equally recognized by the Charter. It is also recognized in Art. 16 of the Treaty on the Functioning of the EU (“TFEU”).


14 Art. 8 of the Charter reads as follows:
Article 8. Protection of personal data
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

15 On the character of data protection and privacy as independent rights, see Orla Lynskey, Deconstructing Data Protection: The ‘Addedvalue’ of a Right to Data Protection in the EU Legal Order, 63 Int’l & Comp. L.Q. 569 (2014) (arguing that even though the rights to privacy and data protection significantly overlap, they are distinct rights, as the latter offers additional benefits and enhanced protection in the context of personal data processing, in particular by promoting individual personality rights and reducing information and power asymmetries).


17 See Consolidated version of the Treaty on the Functioning of the European Union art. 16, Oct. 26,
Before the EU embarked on the adoption of a catalogue of fundamental rights, a legal framework for data protection was laid down in the 1995 Data Protection Directive ("the Directive"), which is still in force. A substantial overhaul of the EU data protection regime is being prepared in the form of a future General Data Protection Regulation (GDPR), which might be adopted by the end of 2015 or early in 2016. This paper will deal primarily with the Directive, as it constitutes the current main piece of EU secondary legislation in relation to data protection, and is the legal framework under which Google Spain was decided. Nonetheless, appropriate reference will also be made to the how the right to be delisted might be affected by the future Regulation, whose final wording is still uncertain.

The purpose of the following subsections is to provide a brief overview of the key elements in the Directive, particularly those which are most relevant to discussing Google Spain – readers already familiar with the main elements of the Directive may want to skip this Part and go directly to Part II.

A. Some key elements of the Data Protection Directive

In a nutshell, the Directive covers the “processing” of “personal data” and sets out the conditions for that processing to be lawful.

Lawful processing requires, in the first place, a legitimate base. It may be either the consent given by the person to whom the personal data relate – called the “data subject” – or any other of the legitimacy grounds specifically provided for in the Directive.

---


19 There are other instruments of secondary legislation that complete the EU legal framework for data protection, but we will not need to deal with them for the purposes of this article. Those instruments include 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), 2002 O.J. (L 201) 37; and Regulation 45/2001, of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals With Regard To the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, 2001 O.J. (L 8) 1.

20 See GDPR Proposal, supra note 5.
In addition, the processing must respect the “data quality” principle, which seeks to ensure, *inter alia*, that the processing is proportionate and not excessive, having account of its purposes. Some other obligations must also be observed, including those relating to the confidentiality and security of the processing, the notifications to the supervisory authority, or the transfer of personal data to third countries. More stringent requirements and safeguards are established for the processing of sensitive data, i.e. “data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership,” and “data concerning health or sex life.”

Two categories of subjects involved in the processing of data are identified, namely, the “controller” and other “processors”, and different sets of legal duties are imposed on them.

The Directive further determines the rights of the “data subject,” which include that of being informed about the collection of data and its processing, as well as the rights of *access* to data, *rectification*, *erasure* or *blocking* of data, and the right to *object* to the processing under the appropriate circumstances.

As to its territorial scope, the Directive applies not only to controllers established in the territory of the EU or the European Economic Area (“EEA”), but also to those established outside the EU/EEA in some circumstances, including the case where “the processing is carried out in the context of the activities of an establishment of the controller” located in the territory of an EU/EEA Member State.

An administrative and judicial system of enforcement is envisioned by the Directive. In each Member State, one or more independent authorities must supervise the application of the national law implementing the Directive. These Data Protection Authorities (“DPAs”) are vested with powers such as that of hearing claims, investigating and effectively intervening – for instance, ordering the blocking, erasure or destruction of data, imposing a temporary or definitive ban on processing, or warning or admonishing the controller. They may also have the power to impose economic sanctions provided for by the national law in cases of infringement of the provisions implementing the Directive. Decisions by DPAs can be appealed before the courts.

All EU Member States are obliged to implement the Directive into their national law. While they are free to choose the particular way or method of implementation or

---

21 Id., art. 8.
22 The European Economic Area (EEA) includes all EU member states and three non-EU members, namely Iceland, Liechtenstein and Norway.
23 See Data Protection Directive, supra note 18, art. 4(1)(a). Emphasis added. The same provision sets forth that “when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.”
“transposition”, they must achieve the results prescribed by the Directive.\(^{24}\) Moreover, according to the so-called principle of consistent interpretation – or *interprétation conforme* – when applying the measures implementing the Directive, national courts must interpret the domestic law in a way which is consistent with EU law.\(^{25}\)

When a Member State’s court harbors doubts on how to interpret EU law, it may stay the proceedings and request that the Court of Justice of the European Union give a preliminary ruling on the matter.\(^{26}\) These preliminary rulings do not decide on the particular facts but on the interpretation that should be given to EU law. They answer the specific legal questions raised by the national court, which should then proceed with the case and render a final ruling. In this way, CJEU judgments form a body of case law which guides national courts in construing EU law in accordance with which they must apply their own national law.

A crucial role in the interpretation of the Directive is played in practice by the so-called Article 29 Working Party (“WP29”) – an advisory body composed of a representative of each Member State’s DPA, a representative of the European Data Protection Supervisor,\(^{27}\) and a representative of the European Commission.\(^{28}\) The WP29 advises the European Commission and regularly delivers opinions, recommendations and reports on issues covered by the Directive, and generally on any question regarding data protection.\(^{29}\) While its opinions are not binding, they constitute in practice a powerful

---

\(^{24}\) See TFEU, *supra* note 17, art. 288 (“A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.”)

\(^{25}\) See Court of Justice of the European Union, Case 14/83 Von Colson and Kamann v. Land Nordrhein-Westfalen, Apr. 10, 1984, ECR 1891, 1909 (“... in applying the national law and in particular the provisions of a national law specifically introduced in order to implement [a] Directive ..., national courts are required to interpret their national law in the light of the wording and the purpose of the directive in order to achieve the result referred to in the third paragraph of Article [288 TUEF]”). See also Katrine Sawyer, *The Principle of “interprétation conforme”*: *How Far Can or Should National Courts Go when Interpreting National Legislation Consistently with European Community Law?*, 28 STATUTE LAW REVIEW 3 (2007).

\(^{26}\) See TFEU, *supra* note 17, art. 267. In some cases, namely “when the question is raised in a case pending before a court or tribunal of a Member State against whose decisions there is no judicial remedy under national law,” it is not an option but an obligation for the national court make the reference for a preliminary ruling. See *id*.

\(^{27}\) The European Data Protection Supervisor (EDPS) is the independent Authority responsible for overseeing the processing of data by the EU institutions and bodies. It is established in art. 41 of the Regulation 45/2001, of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals With Regard To the Processing Of Personal Data by the Community Institutions and Bodies and On the Free Movement of Such Data, 2001 O.J. (L 8) 1.


\(^{29}\) The opinions, recommendations and reports adopted by the Art. 29 WP are available at
guidance for the interpretation of the Directive and thus for the application of the national transposition measures, both by DPAs and national courts.

B. The Pivotal Notions of “Personal Data”, “Processing” and “Controller”

The legal concepts of “personal data”, “processing” and “controller” are key building blocks of the Directive, and are conceived in a very broad way.

Personal data is defined as “any information relating to an identified or identifiable natural person (‘data subject').”30 In its turn, an “identifiable person” is “one who can be identified, directly or indirectly” – either by the controller or by any other person – “in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.31 In its preamble, the Directive notes that “to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person”,32 and excludes “data rendered anonymous in such a way that the data subject is no longer identifiable.”33

Assessing what is personal data under the Directive has proven difficult in some cases, leading to uncertainty and to divergent interpretations in different EU Member States. The WP29 issued an Opinion on this matter in 2007, contributing some interpretation criteria for a uniform understanding of the concept.34 The Opinion makes it clear that the information considered as personal data is not limited to information related to the individuals’ private life; rather it may be any kind of information.35 According to the WP29, for someone to be “identifiable” there is no need to know his or her name; rather it may be enough that this person can be “singled out”, for instance with a unique identifier.36

The notion of processing is defined as “any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection,
recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction”.\(^{37}\) It is hard to think of any action that could fall outside this all-embracing definition. Indeed, the way chosen by the Directive to limit the reach of its rules is not by limiting the notion of what constitutes data processing, but rather by excluding some types of actual data processing from its scope. The following limitations should be noted in this respect. \(^{38}\) \(^{39}\) \(^{40}\) The extent of these eventual exceptions for freedom of expression depends thus on each member state’s national law.\(^ {41}\)

Another key notion in the Directive is that of controller, defined as “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data”.\(^ {42}\)

\(^{37}\) See Data Protection Directive, \textit{supra} note 18, art. 2(b).

\(^{38}\) \textit{Id.}, art. 3(1). Therefore, some residual operations are not governed by the Directive, namely those which do not use automatic means at all and where the data are not going to be included in a “filing system,” that is in a “structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis”. \textit{Id.}, art. 2(c).

\(^{39}\) \textit{Id.}, art. 3(2). The exception has been interpreted in a very narrow way. For instance, the WP29 notes that having a high number of contacts in a social networking site “could be an indication that the household exception does not apply and therefore that the user would be considered a data controller.” See Article 29 Working Party Opinion 5/2009 on online social networking (01189/09/EN) WP 163, Jun. 12, 2009, at 6.


\(^{41}\) See Case C-101/01, Bodil Lindqvist (Nov. 6, 2003) para. 90, \url{http://curia.europa.eu/juris/liste.jsf?num=C-101/01 [hereinafter Lindqvist]}.

\(^{42}\) See Data Protection Directive, \textit{supra} note 18, art. 2(d) (emphasis added).
the one responsible for most of the duties imposed by the Directive. In contrast, more limited obligations are imposed on a mere “processor”, the natural or legal person which processes personal data on behalf of the controller.\textsuperscript{43}

\textit{C. Conditions for Lawful Processing}

For the processing of personal data to be lawful – leaving aside some exceptions provided for in the Directive – it must comply with certain conditions, which, as noted above, include that of having a \textit{legitimate basis} and that of respecting the principle of \textit{data quality}.

Regarding the \textit{legitimacy} of the processing, the Directive provides for several possible grounds.\textsuperscript{44} The first one, already pointed out, is the data subject’s \textit{consent} for the processing. In the absence of consent, the processing may still be legitimate under another of the alternative grounds provided for in Art. 7. One of those grounds, set forth in Art. 7(f), covers the situation where the “processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed.”\textsuperscript{45} It is not absolute ground, as it expressly excludes the case where those interests “are overridden by the interests or fundamental rights and freedoms of the data subject”.\textsuperscript{46} A balance is thus required to determine if a particular case of processing may rely on these grounds for lawfulness.\textsuperscript{47}

Data processing must also respect the \textit{data quality} principle laid down in Art. 6. It requires, \textit{inter alia}, that personal data be collected for specific purposes, and not further processed in a way that is incompatible with those purposes. Data must be “adequate, relevant and not excessive” in relation to the purposes of the processing. Moreover, they must be “accurate and, where necessary, kept up to date”. The provision establishes that “every reasonable step must be taken to ensure that data which are inaccurate or

\textsuperscript{43} \textit{Id.}, art. 2(e).

\textsuperscript{44} The CJEU has declared that art. 7 Data Protection Directive “sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful.” See \textit{Joined Cases C-468/10 and C-469/10, ASNEF and FECEMD}, Nov. 24, 2011, para. 30 [hereinafter \textit{ASNEF and FECEMD}].

\textsuperscript{45} \textit{See Data Protection Directive, supra} note 18, art. 7(f).

\textsuperscript{46} \textit{Id.}

\textsuperscript{47} While under art. 5 of the Data Protection Directive, EU member states have some room for flexibility in determining more precisely how this balance should be achieved, they may not introduce additional requirements to benefit from this ground of lawful processing. \textit{See ASNEF and FECEMD, supra} note 44, para. 39. The WP29 released a detailed Opinion in 2014 providing criteria on how this balance should be carried out. \textit{See Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (844/14/EN) WP 217, Apr. 9, 2014.}
incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.” Thus, a processing that was lawful at a certain time may become unlawful if it no longer respects these principles. Data must be “kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed,”48 and Member States must “lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.”49

D. The Right to Have the Data Erased and to Object to its Lawful Processing

The Data Protection Directive grants a number of specific rights to the person whose personal data are being processed (the “data subject”). Two of them will be of particular relevance in our case. First, the data subject has the right to have the data erased or blocked. Art. 12(b) establishes that every data subject will have “the right to obtain from the controller … as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data”.50 This right is thus conditioned on the fact that the processing does not respect the requirements set out in the Directive and hence cannot be deemed lawful. The specific reference to the “incomplete or inaccurate nature of the data” is just an example of a situation where the processing would not comply with the data quality principles laid down in Art. 6.51

Even where the processing fully complies with the provisions of the Directive, including the data quality principles, a data subject may still “object” to that processing in some situations. This “right to object” is provided for in Art. 14, which obliges EU Member States to grant the data subject the right “to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to

48 See Alessandro Mantelero, The EU Proposal for a General Data Protection Regulation and the roots of the ‘right to be forgotten’ 29 COMPUTER LAW & SECURITY REVIEW, 229, 233 (2013) (putting forward that a dissemination of old facts with no relationship with the present lifestyle or activities of the concerned individual “has to be considered an unnecessarily long processing of data and therefore constitutes an incompatible way of managing the data in relation to the initial purposes.”).
49 See Data Protection Directive, supra note 18, art. 6.
50 Id., art. 12(b).
51 In this case, the data processing would fail to comply with art. 6(d) (“personal data must be … (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;”).
him, save where otherwise provided by national legislation.” The nature of those “compelling legitimate grounds” is not specified in the Directive. If the objection raised is justified, then “the processing instigated by the controller may no longer involve those data.”

II. Google Spain

A. How the Case Originated and Reached the CJEU

In 1998, La Vanguardia – a newspaper based in Barcelona – published an official announcement of auctions of real estate properties following attachment procedures for the recovery of Social Security debts. A person by the name of Mario Costeja González was named as co-owner of one of the properties. There was nothing untrue or inaccurate in the information provided. Newspapers routinely publish this type of official announcement. It appears that Mr. Costeja eventually fixed his problems regarding the debt and the property, and the matter was put behind him. Ten years later, La Vanguardia digitized its archives and put them online, including the digitized version of all its daily paper-based editions. The rest of the story is easy to imagine. One day Mr. Costeja typed his name into Google only to find that some of the first results were links to the pages in the newspaper’s archive with the notice of the real estate auction, which brought back to life an old and long-forgotten episode.

In November 2009, Mr. Costeja asked La Vanguardia to erase his data, noting that the problem had long been solved and the information was not relevant anymore. On the following day, La Vanguardia answered him in the negative, stating that erasure was not appropriate, as the notice was published following an official order. Mr. Costeja then turned to Google Spain SL, the Spanish subsidiary of Google Inc. In its answer, Google Spain told him that he should instead contact Google Inc. in the U.S., as the latter was the entity which actually ran the search engine. In March 2010, he filed a complaint before the Agencia Española de Protección de Datos (AEPD) – the Spanish data protection authority – against La Vanguardia, Google Spain SL and Google Inc.

The AEPD initiated a so-called “procedure for the protection of rights” – a procedure available to data subjects seeking to oblige controllers to respect their rights of

---

52 See Data Protection Directive, supra note 18, art. 14(a) (emphasis added).
53 Id.
access, rectification, erasure or objection – but leaving the news publisher out.\textsuperscript{55} The procedure ended with a decision handed down on July 30, 2010,\textsuperscript{56} which upheld the claimant’s petition against Google Spain and Google Inc., ordering the search engine “to adopt the necessary measures to \textit{remove the data from its index and prevent future access to them.”}\textsuperscript{57}

The Spanish authority held that an ordinary citizen – one who is not a public figure, nor is involved in some publicly relevant event – must not resign herself to having her personal data available on the Internet. On the one hand, it noted that requiring prior consent from individuals before data are put online, or imposing the obligation to establish preventive filtering mechanisms, might pose too high an obstacle for the exercise of the rights to freedom of expression and information, and thus be a sort of censorship, which would be constitutionally barred. On the other hand, it asserted that ordinary citizens must have the possibility to \textit{react}, for instance by means of the right to erasure, once the data appear online. Thus, Mr. Costeja’s petition to have his personal data erased should be upheld, so as to avoid permanent effects against his will.\textsuperscript{58}

The decision did not elaborate much on whether or not the claimant’s petition met the legal requirements. In particular, it was not expressly discussed whether the right to erasure was appropriate because the processing did not comply with the provisions of the Directive,\textsuperscript{59} nor was there a discussion as to whether the data subject had “compelling legitimate grounds relating to his particular situation” on which to object to the processing.\textsuperscript{60} Likewise, the decision contained no discussion as to whether Google fit in

\textsuperscript{55} The AEPD considered that the newspaper rightly rejected Mr. Costeja’s request, since the publication of the announcement had been decided by the official body in charge of carrying out the auction, with the aim of giving maximum publicity to it so that as many bidders as possible could participate – an argument that, in itself, however, hardly accounts for the need to keep that information available after so many years.


\textsuperscript{57} Id. (emphasis added). Apparently, the obligation was imposed on Google Inc., though the wording is not very clear. The decision rules that it upholds “the complaint brought by Mr. Costeja against Google Spain S.L. and against Google Inc.,” and orders “this entity” (which grammatically would indicate the latter, that is Google Inc.) to remove the data and prevent future access to them. However, upholding the complaint also against Google Spain seems to indicate that the Spanish company is also responsible for the removal. \textit{See AEPD Costeja, supra} note 56, at 23. The CJEU, nonetheless, depicts the AEPD decision as ordering only Google Inc. to remove the data from the index. \textit{See Google Spain, supra} note 3, para. 2.


\textsuperscript{59} \textit{See Data Protection Directive, supra} note 18, art. 12(b).

\textsuperscript{60} \textit{See id., art. 14(a). In fact, however surprising it may be, it is not clear at all from the text of the
the legal notion of a controller. It simply assumed that “Google” – without really distinguishing between the parent and the subsidiary – was in fact a controller. The decision did quote a passage of a WP29 Opinion which considers a search engine to be a controller. However, the quoted passage does not relate to the processing of the data included in the linked-to websites, but to the processing of Google’s users’ data, and thus hardly applies to the case at hand.61

Google Spain SL argued that it was neither a controller, nor a processor, of the personal data included on the websites listed in the search results, as it limited itself to promoting the selling of advertising space and did not intervene in the activity of the search engine – it was its parent company, Google Inc., who solely provided the search services and carried out all the functions relating to the indexing and provision of search results. Google Spain SL also contended that EU data protection law was not applicable to the U.S. company. Furthermore, it argued that, in any event, Google Inc. could not be deemed the controller, as the main entities responsible for the processing were the publishers of the websites where the personal data had been included.62 All these contentions were rejected by the AEPD, though some of them, as noted, only by implication. The greatest effort was placed on arguing that the Spanish law and the Data Protection Directive did apply to Google. The decision put forward several arguments to that effect, including that the processing was carried out “in the context of the activities of an establishment” of Google in Spain.63

Both Google Spain and Google Inc., in separate briefs, appealed the AEPD decision before the Audiencia Nacional (National High Court) – the competent court for the review of the administrative decisions issued by the AEPD. Though this particular case would end up being a landmark one, at this stage there was nothing special about it. Dozens of similar appeals, which posed important questions regarding the proper interpretation of the law, were being brought before the Audiencia Nacional (AN).

decision whether Mr. Costeja had exercised the right of erasure or the right to object – or both. Remarkably enough, throughout the AEPD decision, the words “right to erasure” and “right to object” are used interchangeably as if they were synonyms, whereas, as we have seen in the previous part, they are in fact independent rights, each one having its own conditions and requisites in the law. In its final part, the decision seemed to refer specifically to the right to object, but without any reference to the compelling legitimate grounds of the data subject.


62 That was the reason why, when the claimant asked Google Spain SL to erase the data, it did not answer the petition and instead conveyed it to Google Inc., which in turn responded to the claimant that he should direct himself to the publisher – La Vanguardia – as this was the only way to get the data erased or blocked.

63 See id., at 14-15. This would trigger the applicability of the DP Directive. See Data Protection Directive, supra note 18, art. 4(1)(a).
The AN decided to make a reference for a preliminary ruling to the CJEU, just picking the Costeja case out of the many cases appealed before it. The AN posed three groups of questions to the CJEU. First, regarding the territorial scope, the AN harbored doubts on the interpretation of the connecting factors, particularly that consisting of the fact that the processing was carried out in the context of the activities of an establishment of Google Inc. located in Spain – Art. 4(1)(a) of the Directive. The Court considered it proven that the operation of the search engine was exclusively carried out by the parent company based in California. Nonetheless, it noted that the activity of the subsidiary, the promotion and sale of advertising space, might be deemed closely linked to the operation of the search engine, as the ads were displayed along with the search results. The court asked the CJEU whether it must be considered that an “establishment”, within the meaning of the Directive, exists “when the undertaking providing the search engine sets up in a Member State an office or subsidiary for the purpose of promoting and selling advertising space on the search engine, which orientates its activity towards the inhabitants of that State”.

The second set of questions related to how Google’s activity as a search engine fit in the Directive. Particularly, whether the indexation and location of search results constituted a processing of the personal data included in the linked contents, and if so, whether Google could be deemed a controller with respect to that processing under the Directive. The court noted that the fact that the indexation of the information was carried out automatically and without any actual control over its accuracy or truthfulness warranted the doubt as to whether the search engine could be considered a controller. Even if it would fall within the notion of controller, the question would arise as to the extent of its obligations, particularly with regard to the right to erasure and the right to object. In this vein, the Court asked whether the data protection authority might directly order the search engine to remove from its index a piece of information published by a

---

65 At the time of the reference there were some 130 appeals pending before the Audiencia Nacional. See id., at 16.
66 The AN asked as well for the interpretation of the connecting factor consisting of the use of equipment in the territory of a Member State – art. 4(1)(c) – and even asked as well if other connecting factors, not provided for in the Directive, might also be taken into account, such as the location of the conflict’s center of gravity (in order to avoid the data subject to litigate in the provider’s jurisdiction). See id., at 8-9.
67 See id., at 6-7.
68 See id., at 10.
third party, without addressing itself in advance or simultaneously to the publisher. It asked as well if the search engine would be excluded from the removal obligation where the information at stake was lawfully published by third parties and maintained on the publisher’s web page.

The last group of questions regarded the scope of the right to erasure and the right to object. The AN wanted to know whether those rights would allow the data subject to request the removal of the information based simply on his or her wish that the information be consigned to oblivion, and thus not necessarily depending on whether it might be prejudicial to him or her.

B. Finding a Right to Be Delisted under the Data Protection Directive

The landmark ruling handed down by the CJEU was in line with its recent case law underscoring and strengthening the right to data protection, particularly in the light of its recognition as a fundamental right in the EU Charter. The ruling was preceded by the Advocate General’s Opinion (AG). As to the core issues – the search engine’s characterization as controller, and the scope of the data subject’s rights to erasure and to object, the judgment substantially departed from the answers proposed by the AG.

The CJEU found that a search engine’s activity amounts to a processing of the personal data contained on the Internet pages it indexes and makes available to the public through the search results. However, in contrast to the AG’s conclusions, it held that the search engine operator determines the purposes and the means of that processing, and thus

---

69 A remarkable example of this trend is the CJEU’s judgment in the Digital Rights Ireland case, which declared the Data Retention Directive 2006/24/EC to be invalid. See Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v Ireland (April 8, 2014), available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&doclang=EN

70 In a procedure for a preliminary ruling before the CJEU, the Advocate General (AG) assigned to the case must submit an Opinion proposing how to answer the questions posed by the referring court. See Rules of Procedure of the Court of Justice art. 82, Sep. 9, 2012, 2012 O.J. (L 265) 1, 22. Where the court considers that the case raises no new point of law, it may decide to proceed without a submission from the Advocate General. See Statute of the Court of Justice of the European Union art. 20 Oct. 26, 2012, 2012 O.J. (C 326) 210, 215. While the AG opinions are not binding, it is not uncommon for the CJEU to end up adopting the solutions proposed by the AG. See Cyril Ritter, A New Look At the Role and Impact of Advocates-General — Collectively and Individually, 12 Colum. J. Eur. L. 751 (2006) (examining the impact of Advocate General’s opinions and noting that they have been a driving force behind changes and evolutions in the Court’s jurisprudence).

must be regarded as controller.\footnote{72} According to the Court, this processing “can be distinguished from and is additional to that carried out by publishers of websites, consisting in loading those data on an internet page”.\footnote{73} That additional processing is liable to affect significantly data subjects’ rights, as users that carry out searches on the basis of an individual’s name are able to obtain a structured overview of the information relating to that person available on the Internet, and thus can “establish a more or less detailed profile of the data subject.”\footnote{74} As controller, the Court noted, a search engine operator “must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive”.\footnote{75}

As to the applicability of the Directive, the Court came to the conclusion that it does apply to Google, stating that “when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State”,\footnote{76} that processing “is carried out \textit{in the context of the activities of an establishment} of the controller on the territory of a Member State”,\footnote{77} which triggers the applicability of the Directive pursuant to its Art. 4(1)(a).

In analyzing whether the data subject could indeed require the erasure of the data or object to the processing – in the form of delisting the links – the Court pointed out that all processing of personal data must comply with the data quality conditions,\footnote{78} and must be based on one of the legitimacy grounds set out in the Directive.\footnote{79} Regarding legitimacy, it expressly acknowledged that the processing by a search engine “is capable of being covered by the ground in Article 7(f),”\footnote{80} which – as noted above – considers the case where the data processing “is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.”\footnote{81}

If the processing failed to meet of legitimacy and data quality, the data subject had the right to obtain from the controller, as appropriate, \textit{the erasure of the data}. In addition,
even where the processing both respected the data quality requirements and was based on
grounds of legitimacy, the data subject could still object to the processing on compelling
legal grounds relating to her particular situation, except where the national legislation
provided otherwise. The data subject could address directly her requests to the search
engine, “who must then duly examine their merits and, as the case may be, end processing
of the data in question”, and where it did not grant the request, the data subject could
resort to the DPA or the judicial authority, who would then assess the request and order the
controller to take the appropriate measures.

In any of those situations, a balancing of the opposing rights and interests must be
carried out to appraise the data subject request. In this respect, the CJEU emphasized that
that balancing must duly take into account “the significance of the data subject’s rights
arising from Articles 7 and 8 of the Charter.” Noting that search engine processing “is
liable to affect significantly the fundamental rights to privacy and to the protection of
personal data when the search by means of that engine is carried out on the basis of an
individual’s name”, the CJEU held that that potentially serious interference “cannot be
justified by merely the economic interest which the operator of such an engine has in that
processing”. Therefore, the elements to weigh in the balancing should be the data
subject’s fundamental rights, against the “the legitimate interest of internet users
potentially interested in having access to that information”. However, the possibility of
actually balancing those elements was sharply reduced by the Court, as it stated that “data
subject’s rights protected by [Arts. 7 and 8 of the Charter] also override, as a general rule,
that interest of internet users”. Nonetheless, the Court noted, in specific cases, this could
depend “on the nature of the information in question and its sensitivity for the data
subject’s private life and on the interest of the public in having that information, an interest
which may vary, in particular, according to the role played by the data subject in public
life”.

Furthermore, the Court answered that the obligation of the controller to end the
processing is not conditioned on the fact that the publisher remove the information

---

82 See id., art. 14(b).
83 See Google Spain, supra note 3, para. 77
84 Id.
85 Id., para. 74. The importance of Arts. 7 and 8 of the Charter was already underscored by the Court in Digital Rights Ireland, see supra, note 69.
86 Id., para. 80.
87 Id., para. 81.
88 Id.
89 Id. (emphasis added).
90 Id.
previously or simultaneously from the web page. It is neither affected by the fact that the information was lawfully published on the web. The CJEU stressed that those are two different processing operations and thus each controller had to comply with its own obligations. It could well be that the processing by the web publisher was lawful and complied with the Directive, whereas the search engine’s did not. For instance, the Court noted, the web publisher might benefit from the exclusions granted by national law, pursuant to Art. 9 of the Directive, for processing carried out solely for journalistic purposes, whilst “that does not appear to be so” in the case of the processing by a search engine. Moreover, the legitimate interests of the different controllers – the publisher and the search engine operator – could lead to a different balance regarding the legitimacy basis for the processing.

Finally, the Court tackled the question of whether the right to erasure and the right to object could be exercised “on the ground that that information may be prejudicial to [the data subject] or that he wished it to be ‘forgotten’ after a certain time.” It held that in order determine whether a data subject “has a right that the information relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name … it is not necessary … that the inclusion of the information in question in the list of results causes prejudice to the data subject.” It went on to repeat the principles it had previously stated, in the sense that under the Charter the data subject does have that right, a right that will take priority over any other legitimate interest, the only exception being a possible prevailing interest of the general public in particular circumstances. Against that backdrop, the Court held that, in a situation such as the one at issue in the main proceedings:

having regard to the sensitivity for the data subject’s private life of the information contained in those announcements and to the fact that its initial publication had

---

91 *Id.*, para. 85.
92 *Id.* paras. 82-87.
93 *Id.* para. 89. Again, the CJEU rephrased the original referred question into a more surgical one. The referring court had in fact asked whether the right to erasure and the right to object extend to enabling the data subject to address himself to search engines in order to prevent indexing of the information relating to him personally, published on third parties’ web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though the information in question has been lawfully published by third parties. *Id.*, para. 20 (Question 3) (emphasis added). *See also* AN Reference Google Spain, *supra* note 64, at 17.
94 *See Google Spain, supra* note 3, para. 96.
95 *Id.*, para. 97.
taken place 16 years earlier, the data subject establishes a right that that information should no longer be linked to his name by means of such a list. Accordingly, since in the case in point there do not appear to be particular reasons substantiating a preponderant interest of the public in having, in the context of such a search, access to that information, a matter which is, however, for the referring court to establish, the data subject may, by virtue of Article 12(b) [the right to erasure] and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 [the right to object], require those links to be removed from the list of results.

Whereas the CJEU clearly stated that a prejudice to the data subject is not required, it did not directly respond to the question of whether the rights to erasure and to object enable a data subject to require a search engine to stop the processing merely because she wishes the information is consigned to oblivion. It may seem that, for the CJEU, unless there was a prevailing interest of the general public – for instance because of the public relevancy of the data subject – the question should be answered in the affirmative, owing to the fundamental rights recognized in the Charter. Nonetheless, the Court did require that the data subject’s requests meet some threshold, namely, the conditions set forth either in Art. 12(b) for the right to erase, or in Art. 14(a) for the right to object. Therefore, it must be either that (a) the processing failed to comply with some of the requisites laid down in the Directive, particularly those related to the quality of the data, which include that the data must be “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed”, or that (b) the data subject had some “compelling legitimate grounds relating to his particular situation” that allowed him or her to object to the processing.

C. Follow-up by the National Court

After receiving the judgment from the CJEU, the referring court – the Audiencia Nacional (AN) – resumed the proceedings and handed down its final ruling on the case on

96 Id., para. 98. (Emphasis added).
97 See the operative part of the ruling, #3 (“in so far as the conditions laid down by those provisions are in fact satisfied”). This might be seen as mere lip service, as in the court’s balance there was no assessment as to whether those requirements were actually fulfilled. See also id. para. 82.
98 See Data Protection Directive, supra note 18, art. 6(b).
99 See id., art. 14(a).
December 29, 2014. Under EU law, it is for the national referring court to apply the interpretation criteria provided by the CJEU to the facts of the particular case. Arguably, thus, the CJEU went too far when it appraised the facts of the case and directly held that Mr. Costeja had established a right that the information should no longer be linked to his name by means of the search results. In any event, the AN accepted the CJEU’s assessment, and further found that Mr. Costeja had no relevant role in public life that could make the interest of the general public prevail over his rights.

According to the AN, this was an initially lawful processing of accurate personal data by Google, but due to the lapse of time, the data became unnecessary with regard to the purposes of the processing. Remarkably, the AN expressly held that freedom of information was duly satisfied thanks to the fact that the information was kept on the source, and thus still findable through searches which were not made on the basis of the data subject’s name. The AN rejected Google’s contention that the DPA decision violated its right to freedom to conduct businesses, noting that it was not an absolute right and that, following the CJEU approach, this right was overridden by the data subject’s fundamental rights to privacy and data protection.

A noteworthy aspect of the AN ruling was the holding that Google Spain SL, the Spanish subsidiary, is also responsible for the processing, that is, a data controller itself, along with Google Inc. This responsibility stems from the fact both the subsidiary and its parent form a business unit, in which the subsidiary’s activity is essential to the business model of the search engine. According to the AN, once it is established that the Directive applies to Google Inc. precisely because the processing is carried out in the context of the activities of Google Spain, it would make no sense to exclude Google Spain from any liability in the processing carried out by Google Inc. and holding otherwise would prejudice the protection the Directive sought to ensure.

Finally, the AN did accept the appellants contention that the decision by the AEPD, which was the subject of the appeal, was too broad, as it ordered the search engine “to adopt the necessary measures to remove the data from its index and prevent future access to them.” According to the AN, the DPA could only “order the search engine operator to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages published by third parties containing information


101 The ruling has been appealed by Google Spain SL, particularly on account of the liability imposed on the subsidiary, and is currently pending before the Spanish Supreme Court.

102 See AEPD Costeja, supra note 56, at 23.
relating to that person.”103 Hence, the DPA decision was affirmed, but remarking that it should be interpreted in this more limited sense of delisting links in search results.104

III. A RIGHT ON SHAKY GROUND?

The outcome of Google Spain was premised on Data Protection Directive provisions, construed in light of the fundamental rights to privacy and personal data protection enshrined in the EU Charter. This Part will discuss the legal basis of the CJEU’s findings in Google Spain, focusing particularly on the conceptualization of a search engine as a controller; the search engine’s intermediary role; the legal grounds for the data subject’s request to have the links delisted; and the Court’s criteria to balance the rights at stake.

A. The Controller and the Proportionality Principle

Leaving aside the issue of territorial applicability, the key threshold question to trigger the data protection framework is whether or not a search engine should be considered a “controller” under the Directive, and thus liable for complying with the obligations it imposes on controllers. While the Directive offers an apparently clear definition of a controller – the one who “alone or jointly with others determines the purposes and means of the processing of personal data” – its application to specific cases is far from being straightforward.105 In particular, the participation of multiple actors in a processing operation or in a number of related processing operations makes it difficult to determine if all of them should be considered controllers, and, if so, how the responsibilities should be allocated among them.106

103 See AN follow-up judgment, supra note 100, at 27.
104 Nonetheless, the ruling said nothing on whether the surprising of the links must be done in all Google domains, including Google.com, or just in the European country-code top-level domains, such as Google.es, or Google.fr.
105 The complexities of the issue are well illustrated in the Article 29 Working Party Opinion 1/2010 on the concepts of “controller” and “processor” (264/10/EN) WP 169, Feb. 16, 2010 [hereinafter WP29 Opinion on the concepts of “controller” and “processor”].
106 As the WP29 noted, “in the context of joint control the participation of the parties to the joint determination may take different forms and does not need to be equally shared”. See id., at 19. These parties “may have a very close relationship (sharing, for example, all purposes and means of a processing) or a more loose relationship (for example, sharing only purposes or means, or a part thereof).” See id. In this regard, the WP29 Opinion put forward that “a broad variety of typologies for joint control should be considered and their legal consequences assessed, allowing some flexibility in order to cater for the increasing complexity of current data processing reality.” See id. In addition, the WP29 noted that “the mere fact that different subjects cooperate in processing personal data, for example in
In a typical right-to-be-delisted scenario, at least two different entities process the relevant personal data. First, there is the information content provider that publishes the information including the personal data on a webpage; second, there is the search engine that indexes that content and displays a link to it when a user types the data subject’s name into the search box. Both processing operations are obviously related, in that the second one constitutes a further processing of the data already processed by the publisher, and also in that the publisher would generally be aware that the information will be indexed and findable through search engines. In fact, in many cases, the publisher will be able to prevent search engines from indexing its content by using the robots.txt protocol or other technical means. Should those two activities be considered as a “set of operations” where both the publisher and the search engine pursue a jointly determined purpose, which would make them joint controllers?  

In an Opinion issued in 2008 dealing specifically with search engines, the WP29 noted that “[t]he principle of proportionality requires that to the extent that a search engine provider acts purely as an intermediary, it should not be considered to be the principal controller with regard to the content related processing of personal data that is taking place.” Rather – the Opinion held – the principal controllers of personal data in this case are the information providers. This seems to assume that both the publisher and the search engine are joint controllers, although the responsibilities are distributed asymmetrically among them. The WP29 chose to understand that a search engine will only be responsible for what falls under its control, pointing out that “[t]he formal, legal and practical control the search engine has over the personal data involved is usually limited to the possibility of removing data from its servers”. This led the WP29 to assert that, “[w]ith a chain, does not entail that they are joint controllers in all cases, since an exchange of data between two parties without sharing purposes or means in a common set of operations should be considered only as a transfer of data between separate controllers.”

107 See WP29 Opinion on the concepts of “controller” and “processor”, supra note 105, at 20.
108 See WP29 Opinion on Search Engines, supra note 61, at 14 (emphasis added). “Principal controller” is not a notion defined in the Directive.
109 In contrast, where a search engine actively searches for personal data as such and provides added value services based on those data, or where it sells advertisements triggered by the data, the search engine is not acting as a pure intermediary, according to the WP29. In those cases “the search engine provider is fully responsible under data protection laws for the resulting content related to the processing of personal data.” Id. Likewise, the WP29 considered that search engines go beyond their intermediary role when they cache contents for a longer period than the strictly necessary to address the problem of the temporary inaccessibility of the origin page. In this situation, the WP29 deemed the search engines “responsible for compliance with data protection laws, in their role as controllers of the personal data contained in the cached publications.” Id., at 15.
regard to the removal of personal data from their index and search results, search engines have sufficient control to consider them as controllers (either alone or jointly with others) in those cases.”\textsuperscript{110} Apparently, thus, their obligations as controllers would be limited to that removal. Remarkably, nonetheless, it further noted that “the extent to which an obligation to remove or block personal data exists, may depend on the general tort law and liability regulations of the particular Member State” – thus assuming that even though search engines are to be considered controllers with regard to those removals, their role as intermediaries might relieve them from such an obligation.\textsuperscript{111}

If the analysis by the WP29 was driven by the principle of proportionality, the same principle led the AG to reach a different conclusion, namely that – except in special circumstances – a search engine is not a controller. This was because, in the AG’s view, one can only be considered a controller where one “is aware of the existence of a certain defined category of information amounting to personal data and the controller processes this data with some intention which relates to their processing as personal data,”\textsuperscript{112} which would not be the case with a search engine.\textsuperscript{113}

Against the above-described backdrop, the conclusion by the CJEU that Google is indeed a controller is not that surprising. Although it has been criticized in the literature as a departure from a more careful approach taken by the WP29,\textsuperscript{114} as we have seen, the

\textsuperscript{110} See WP29 Opinion on Search Engines, supra note 61, at 14. This approach is arguably at odds with what the WP29 had determined in a previous Opinion, holding that especially in cases of joint control, not being able to directly fulfill all controller’s obligations (ensuring information, right of access, etc) does not exclude being a controller. It may be that in practice those obligations could easily be fulfilled by other parties, which are sometimes closer to the data subject, on the controller’s behalf. However, a controller will remain in any case ultimately responsible for its obligations and liable for any breach to them.

\textsuperscript{111} See WP29 Opinion on Search Engines, supra note 61, at 14. Indeed, the Conclusions part of the Opinion does not include any such obligation to remove, and refers only the situation where the search engine is considered a principal controller with regards to its cache. See id., at 25.

\textsuperscript{112} See AG Opinion, supra note 70, para. 82 (emphasis in the original).

\textsuperscript{113} The AG concluded that a search engine could only be considered a controller when it had not complied with the instructions set out in the publisher’s page establishing that the search engine’s robots should not crawl or cache the page, or requiring specific conditions for the updating of the information cached by the search engine, a situation which was not the case in the proceedings that led to the reference for a preliminary ruling. AG Opinion, supra note 70, para. 99. Arguably, however, considering the search engine a controller in those cases is at odds with the AG’s own notion of controller requiring specific awareness by the controller that it is being processing personal data as such.

\textsuperscript{114} See for instance Giovanni Sartor, Search engines as controllers: inconvenient implications of a questionable classification, 21 MAASTRICHT JOURNAL OF EUROPEAN AND COMPARATIVE LAW 564 (2014) [hereinafter Sartor, Search engines].
WP29 had in fact also concluded that a search engine is a controller, albeit not the principal one, and with limited obligations, as even the removal of the data from its index and search results might depend on national tort law. Of course, there is a big difference, namely, that the CJEU treats the search engine operator as a separate controller, whose processing is different from, and additional to, that of the publishers, which, at least in theory, makes it fully responsible for that processing.

It must be stressed that, according to the CJEU, the data “processed” by the search engine are not only those displayed on the search results, i.e. the text of the link and the snippet below it, but also the content data, i.e. the data included in the linked-to webpages. Indeed, the court held that

first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as ‘processing of personal data’ within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the ‘controller’ in respect of that processing, within the meaning of Article 2(d).

Thus, the question is not only about the text displayed in on the results screen, but about the information the results link to. The court stated that “the supervisory authority or judicial authority may order the operator of the search engine to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages published by third parties containing information relating to that person.”

However, characterizing a search engine as controller of all personal data included in the indexed web pages is arguably a far-reaching result. As noted, there is a first problem, that of whether a search engine operator actually meets the definition of controller when it is not specifically aware that the data it is processing are personal data. But even if this is answered in the affirmative, the question arises as to whether this

---

115 See Google Spain, supra note 3, para. 35.
116 Id., para. 41. Emphasis added.
117 Id., para. 82. Emphasis added.
118 This objection, already raised by the AG, has been stressed by some commentators. See, in particular, Sartor, Search engines, supra note 114 (pointing out that the CJEU’s conclusion is based on the underlying assumption that “a search engine chooses to process personal data whenever it knows that among the data it processes there are personal data, even though it does not know and does not care which they are”, and that such an assumption “is premised on a questionable understanding of the role of services on the internet, such as those performed by a
characterization can be seen as a *proportionate* outcome in terms of the legal duties that stem from it. Considering search engines as controllers is not without consequences, as they are unable to comply with most of the obligations the Directive imposes on data controllers. In particular, indexing any information published on public websites that happen to include sensitive categories of data – i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concerning health or sex life – would be unlawful, as the controller’s legitimate interests are not a valid exception against the general prohibition of processing this type of data set forth in Art. 8 of the Directive. Ultimately thus, as the AG noted, search engines would simply be incompatible with EU law. Besides, they would be subject to civil, administrative and even criminal liability for unlawful processing. Maybe in an effort to mitigate the consequences of such a finding, the CJEU limited the obligations of a search engine operator as controller by holding that it “must ensure, *within the framework of its responsibilities, powers and capabilities*, that the activity meets the requirements of [the] Directive”. However, such a holding hardly comports with the language of the Directive. While the Directive does exempt controllers from fulfilling some obligations which would require disproportionate efforts, it does so only in particular areas, such as regarding the duty to inform data subjects, or the need to notify third parties.

The court apparently faced a difficult choice: either to consider the search engine a controller, thus enabling the data subject to exercise before the search engine the right to erasure or the right to object to the processing, or to conclude that it was not a controller, thereby leaving the data subject unprotected. For some authors, though, this dichotomy

search engine,” where in fact the users who upload the content are those who choose to have that content indexed by search engines).

119 See, for instance, controllers’ obligations established in art. 6 of the Directive, regarding the “data quality.”

120 AG Opinion, *supra* note 70, para. 90. See also Joris van Hoboken, Case note, CJEU 13 May 2014, C-131/12 (Google Spain) (2014), http://ssrn.com/abstract=2495580 [Hereinafter Hoboken, Case note] ¶9 (“[s]ince the conclusion that all sensitive data would have to be purged from search engines is as unworkable as undesirable, some exceptions derogations should clearly apply”).

121 See *Sartor*, *Search engines*, *supra* note 114.

122 See *Google Spain, supra* note 3, para. 38 (emphasis added).

123 See *Data Protection Directive*, *supra* note 18, art. 11(2) (exempting the controller from the obligation to provide some information to the data subject when “the provision of such information proves impossible or would involve a disproportionate effort”); see also id., art. 12(c) (providing that the controller must notify to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out after a request by the data subject, unless this proves impossible or involves a disproportionate effort).

124 The CJEU noted in fact that concluding that the search engine is not a controller “would be
could have been avoided by considering search engines as controllers but then applying to them the so-called media exception – a possibility ruled out by the CJEU.\textsuperscript{125} Others put forward that the Court should not have considered them controllers, and that the interests of both search engine operators and data subjects could be satisfactorily handled resorting to the specific legal regime for intermediaries set out in the E-Commerce Directive.\textsuperscript{126}

As the right recognized by the ruling is ultimately premised on the search engine characterization as a data controller, in spite of the fact that a search engine’s activity can hardly be reconciled with the obligations controllers face under the Directive, the “right to be delisted” is arguably a right on shaky ground. In fact, the Court failed to properly take into account the intermediary role played by generalist search engines’ in the digital information ecology – although the one to blame in this respect is more the legislator than the court, as the Directive itself does not appear to allow the recognition of such a role. If the characterization of search engines as controllers is mandated by the law, then there is arguably a problem with that law – which is not that uncommon in data protection law, with its extremely broad scope, which while aiming to afford data subjects the maximum level of protection may lead to some inconsistent outcomes.

It is submitted here that the law should specifically protect search engines’ intermediary role. This would not be incompatible with the establishment of some obligation to delist links in specific cases, but such an obligation should not be based on a categorization of a search engine as a controller, as that entails a set of duties which even if never enforced, are arguably at odds with their intermediary nature. Let us now briefly consider such role and its implications.

\subsection*{B. Protecting search engines’ intermediary role}

Generalist search engines carry out two different types of activities that must be distinguished. On the one hand, they provide search services; i.e. they crawl the Web to index publicly available information and respond to users’ search queries by displaying links to the most relevant contents – in other words, they perform the intermediary

\textsuperscript{125} See Hoboken, Case note, supra note 120, ¶7 (noting that “[t]he only way out of far-reaching obligations after this conclusion [that search engines are controllers] would have been an acknowledgement of the relevance of Article 9 Directive 95/46/EC, the so-called media exemption”).

\textsuperscript{126} See Sartor, Search engines, supra note 114.
function of locating information on the Internet. They allow their users to find content online, staying between the content providers and the users who seek information. The Internet would hardly work without information location tools such as those provided by search engines – the information would be up there, but impossible to find for most of the users. On the other hand, in a related but clearly different function, search engines establish a relationship with their users and collect personal information about them, which allows them to track users’ search queries’ history and even their surfing behavior by following them across different services and platforms. A search engine may process that information to profile users and show them targeted advertising as well as to provide them with more personalized search results. With regard to the processing of users’ data, search engine operators squarely fall within the notion of controller.

However, a completely different situation emerges with regard to third-party personal data that happen to be included in the content that search engines index and link to. As noted, the operator is generally not aware of the nature of the indexed content and does not treat it as personal data, and furthermore its activity simply does not comport

127 Of course, one may argue that, far from offering a purely neutral and objective view of the relevant information, search engines produce biased results. That is nonetheless a different debate. Some authors claim search engines should avoid bias and act as mere conduits of the information available online. See, e.g. Frank Pasquale, Rankings, Reductionism, and Responsibility, 54 CLEV. ST. L. REV. 115 (2006). Others put forward that search engines are in fact editors, and thus free to choose the results as they see fit, exercising their freedom of speech. See, e.g. Eric Goldman, Search Engine Bias and the Demise of Search Engine Utopianism, 8 YALE J.L. & TECH. 188 (2006); Eugene Volokh and Donald M. Falk, Google First Amendment Protection for Search Engine Search Results, 8 J.L. ECON. & POL’Y 883 (2012). Departing from both the conduit theory and the editor theory, a third view has been offered by James Grimmelmann, considering search engines as trusted users’ advisors. See James Grimmelmann, Speech Engines, 98 MINN. L. REV. 868 (2014).

128 In this regard, the WP29 has noted that «[s]earch engines play a crucial role as a first point of contact to access information freely on the internet. Such free access to information is essential to build one’s personal opinion in our democracy.» See WP29 Opinion on Search Engines, supra note 61, at 8.

129 Admittedly, in some cases, search engines do provide some added value that arguably entails knowingly treating personal data as such. For instance, for some entities and persons, Google displays a box where it highlights some relevant data which may include the day of birth, name of the spouse, name of the children, and so on. Of course this is only likely to occur with public figures or otherwise people frequently searched for by users. See Google Official Blog, Introducing the Knowledge Graph: things, not strings (May 16, 2012), http://googleblog.blogspot.com.es/2012/05/introducing-knowledge-graph-things-not.html. See also Christopher Null, Google, Why Won’t You Let Me Forget My Divorce? WIRED (May 7, 2015), http://www.wired.com/2015/05/google-wont-let-forget-divorce/. While it ultimately relies on gathering information publicly available on the internet, this type of processing appears indeed to be more problematic. See also WP29 Opinion on Search Engines, supra note 61, at 15.
with the role of a controller envisioned by the Data Protection Directive, as it is not able to comply with most of the obligations a controller is supposed to fulfill.

Search engines’ intermediary role as information locators raises the questions of how they should be treated in terms of liability, and how data protection law should acknowledge and adapt to such a role.

1. Intermediary liability safe harbors

Just like with other Internet intermediaries, such as conduit operators and hosting service providers, it would seem appropriate to establish a statutory limitation of liability for the third-party content that search engines index and make available through search results. EU law has in place a set of safe harbors exempting certain types of intermediary services from liability so that, as long as they meet some conditions, they cannot be held liable for the unlawful content provided by their users. This safe harbor scheme is laid down in Arts. 12 through 15 of the 2000 E-Commerce Directive, a set of rules that was inspired to a large extent by the 1998 U.S. Digital Millennium Copyright Act (DMCA). Both statutes present nonetheless significant differences, including the fact that, while the DMCA deals exclusively with infringements of copyright, the E-Commerce Directive’s safe harbors apply horizontally to any kind of unlawful content.

Another key difference is that, unlike the DMCA, the E-Commerce Directive does not provide for a specific safe harbor for information location tools; it only establishes exemptions for mere conduit, proxy caching and hosting of third-party contents. Some Member States, however, did introduce an information location tool safe harbor when implementing that Directive. In addition, some national courts have

---

wrangled with the absence of such a safe harbor, eventually concluding, that the hosting exemption may be enough to cover the operation of a search engine. In some cases, even in the absence of any applicable safe harbor, courts have decided there was no sufficient basis as to hold the search engine liable.

However, and even if the hosting safe harbor were to be considered enough to accommodate search, the applicability of the safe harbors to situations where the third-party content may violate data protection rights remains unclear. This is because, in spite of the horizontal approach of the E-Commerce Directive, Art. 1(5)(b) excludes from the Directive’s scope “questions relating to information society services covered by [Data Protection Directives].” Now, concluding that a service provider may rely on the safe harbors for any possible kind of unlawful third-party content except where the content happens to include personal data would run afoul of the rationale behind the horizontal approach, i.e. that an intermediary would carry out the same technical activity regardless of the kind of content involved. It would also go against the principle established in Art. 15(1) of the E-Commerce Directive that intermediaries cannot be subject to a general


136 See Metropolitan Int’l Schools Ltd. v. Designtechnica Corp., [2011] 1 WLR 1743, [2009] EWHC 1765 (Q.B.) (holding Google Inc. not liable for an allegedly defamatory snippet displayed in search results, as the defendant could not be characterized as a publisher under common law).

137 See E-Commerce Directive, supra note 130, art. 1(5)(b). In the same vein, Recital 14 to the E-Commerce Directive, notes that Directives on Data Protection “already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States.” It further states that “the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries.”

138 See Commission First Report on the application of Directive 2000/31/EC, at 12, COM (2003) 702 final (Nov. 21, 2003) (“The limitations on liability provided for by the Directive are established in a horizontal manner, meaning that they cover liability, both civil and criminal, for all types of illegal activities initiated by third parties.”).
obligation “to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.”\(^{139}\) Therefore, a reading of Art. 1(5)(b) more consistent with the rest of the Directive might conclude that it does not intend to limit the scope of the safe harbors.\(^ {140}\) Apparently recognizing the need to keep the safe harbors available, the proposed General Data Protection Regulation expressly declares that the Regulation will be “without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.”\(^{141}\)

In any event, the current framework does not provide search engines with enough legal certainty regarding (i) whether the search activity is covered by the E-Commerce safe harbors, and (ii) whether safe harbors apply to content including personal data.\(^ {142}\) Greater legal certainty would be desirable, which might be achieved through an amendment of the E-Commerce Directive to include a safe harbor for information location tools. Such a safe harbor should expressly exempt from liability not just the conduct consisting of locating potentially unlawful third-party content on the internet, but also – if they are to be considered controllers – the processing activity carried out by search engines.

2. Intermediaries under the data protection legal framework

\(^{139}\) See E-Commerce Directive, supra note 130, art. 15(1) – a provision parallel to that in section 512(m) of the DMCA.

\(^{140}\) In the Vividown case, the Italian Supreme Court held that art. 1(5)(b) E-Commerce Directive does not in itself render the safe harbors inoperative when it comes to data protection; rather it is merely meant to make it clear that the data protection framework remains applicable to online activities. See Corte di Cassazione, sez. III Penale, judgment n. 5107, Dec 17, 2013 – Feb. 3, 2014 (Vividown), available at http://www.dirittoegiustizia.it/allegati/15/0000063913/Corte_di_Cassazione_sez_III_Penale_sentenza_n_5107_14_depositata_il_3_febbraio.html. Along the same lines, see Sartor, Search engines, supra note 114, at 574 (“this provision can be understood as only meaning that the obligations concerning data protection remain only those established by the Data Protection Directive, a statement that is fully compatible with the immunity of intermediaries for third parties’ violations of such obligations.”).

\(^{141}\) This statement was included in art. 2(3) of the Commission’s proposal. In the version agreed by the Council on June 26, 2015, art. 2(3) is deleted, but the same statement is kept in Recital 17. See supra note 5.

\(^{142}\) By way of comparison, search engines’ protection from liability for third-party content is much stronger under US law. First, when it comes to copyright infringing content a search engine would find a shelter under the DMCA. Second, and more generally, a search engine operator will be protected from most liability claims under Section 230 of the Communications Decency Act (“CDA”). See 47 U.S.C. § 230. See, e.g. Nieman v. Versuslaw, Inc., 2012 WL 3201931, (C.D. Ill. Aug. 3, 2012), aff’d No. 12-2810 (7th Cir. 2013) (holding that the claims of invasion of privacy and defamation against defendant search engines were barred by 47 U.S.C. § 230).
The Data Protection Directive does identify a particular kind of Internet intermediary, namely ISPs that provide transmission services, and makes it clear that when they transmit messages containing personal data, “the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services.”¹⁴³ This exclusion of transmission service providers from normally being characterized as controllers appears to rest on their purely intermediary role as passive conduits. In spite of all the differences, a similar rationale could have arguably been used for search engines, acknowledging their intermediary function of finding information available online without any intervention as to the creation of the content they allow users to locate. The Directive, nonetheless, remains silent about search engines, and the Google Spain court found them to be controllers of the data included in the searched-for content.¹⁴⁴

Data protection legal framework should evolve so as to appropriately accommodate general search engines. This might be done by crafting specific provisions for search engines so that, while being subject to specific reasonable obligations, they are otherwise allowed to provide search services without violating the law. Those obligations might include specific duties with regard to the harm data subject’s may experience as a consequence of the widespread dissemination of search results that point to information that includes an individual’s personal data, in particular after a search made on the basis of his or her name. However, such a redress should be addressed in a way that avoids the problems detected in Google Spain, especially with regard to the appropriate balance of competing rights and interests so as to overcome its shortcomings and a wide range of potentially unintended consequences.

¹⁴³ See Data Protection Directive, supra note 18, Recital 47 ("where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services."). See also AG Opinion, supra note 70, para. 87.

¹⁴⁴ See Joris van Hoboken, The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember. Freedom of Expression Safeguards in a Converging Information Environment (2013), http://www.law.nyu.edu/sites/default/files/upload_documents/VanHoboken_RightTo%20Be%20Forgotten_Manuscript_2013.pdf (suggesting that data protection law distinguish “between the processing of personal data in the relation between users and the service (user data) and the processing of data on or through the service (content data),” and noting that “the first type of relation seems more suitable to be structured through the application of data protection rules and principles.”).
C. The Legal Basis for Having the Links Delisted

1. Overlapping rights

While the CJEU found that Mr. Costeja established a right that that information should no longer be linked to his name by means of the search results list, it did not determine the precise legal basis for the data subject to require such delisting under the Directive in the case brought before it. Rather, it held that in such a case the data subject may “require those links to be removed from the list of results” by virtue of both the right to erasure (Art. 12(b)), and the right to object (Art. 14(a)).

In principle, though, those rights are mutually exclusive, as the former covers data processing which does not fulfill, or no longer fulfills, the Directive provisions and is thus unlawful, whereas the latter concerns situations of lawful processing, to which the data subject is nonetheless allowed to object on account of “compelling legitimate grounds relating to his particular situation”. Therefore, in a specific case, it should be either one right or the other – or none. The CJEU nonetheless conflated both rights in its judgment, maybe so as to cover other cases with slightly different circumstances, although in theory – since it held that in this case the data subject (Mr. Costeja) “establishes” a right to have the links delisted – it should have been able to discern which was the specific right applicable in that particular case.

Arguably, however, the matter is not that obvious. Actually, both rights highly overlap and, in a way, they are caught in a somehow circular rationale. Indeed, when a data subject has compelling grounds to object under Art. 14(a) to an otherwise lawful

---

145 See Google Spain, supra note 3, para. 98.
146 Id.
147 See Data Protection Directive, supra note 18, art. 6.
148 Id., art. 14. The proposed Regulation intends to shift the burden of proof, by stating that “[t]he data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data … unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.” See GDPR Proposal, supra note 5, art. 14.
149 See Anna Bunn, The curious case of the right to be forgotten, 31 COMPUTER LAW & SECURITY REVIEW, 336. 342-43 (2015) (correctly observing that “the Court made no findings that the personal data relating to Mr [Costeja] in the search results were unnecessary or inadequate or were irrelevant, excessive or inaccurate in light of the purposes for which that data was collected or processed by Google.”).
processing, the conclusion should probably be reached that under Art. 7(f) “the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed,” are in fact “overridden by the interests for fundamental rights and freedoms of the data subject,” and thus that the controller lacks the legitimate grounds for the processing under Art. 7(f). In its turn, the lack of a such grounds – the consent of the individual being absent – would make the processing non-compliant with the Directive provisions, which would allow the data subject to exercise the right to erasure under Art. 12(b). In a similar vein, the “compelling legitimate grounds” relating to the data subject’s particular situation, in which he or she may base the objection to the processing under Art. 14(a), may well determine that the data are inadequate, irrelevant, or excessive in relation to the purposes of the processing, which would entail lack of compliance with Art. 6(1)(c) and, again, would allow the data subject to exercise the right to erasure under Art. 12(b).

2. Whose processing?

The Court’s widely reported finding that the individual has the right to have the links delisted when the data are “inadequate, irrelevant or no longer relevant, or excessive” deserves some further comment. Those adjectives have prompted harsh criticism against what has been considered too vague a standard, unable to meet any reasonable threshold for suppressing speech on the Internet. Whatever the merits of these critiques, it must be noted that those words are taken from Art. 6(1)(c) of the Directive, and they do not refer to the fact that the data subject may simply consider the data to be inadequate, irrelevant or excessive in general or according to his or her preferences; but rather to the fact that they are so, as the Court notes, “in relation to the purposes of the processing at issue carried out by the operator of the search engine.”

It is thus meant to be an objective, rather than a subjective standard. The question is then which are the “purposes” of the processing carried out by the search engine

150 See Data Protection Directive, supra note 18, art. 7(f). See Herke Kranenborg, Case note: Google and the right to be forgotten, 1 EUROPEAN DATA PROTECTION LAW (2015) (noting that the CJEU apparently absorbed the criterion of having “compelling grounds” to object in the balance of interests required in Art. 7(f), and that “[i]t thereby relinquishe[d] the opportunity to use the criterion provided in Article 14 to give a bit more weight to the right of freedom of expression and avoid criticism on the lack of a proper balance between the conflicting rights at stake.”).

151 See Google Spain, supra note 3, para. 94.

152 See Data Protection Directive, supra note 18, art. 6(1)(c) (“... personal data must be ... (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed”).

153 See Google Spain, supra note 3, para. 94. Emphasis added.
operator. While they were not made explicit in the judgment, it may be safe to assume that they consist in making easily findable the information publicly available on the Internet by displaying results relevant to users’ search queries.\textsuperscript{154} If this is so, an argument could be made that displaying links to information that is publicly available on the Web and relates to the name which has been used as a search term is consistent with the purposes of the processing carried out by the search engine – i.e. it is not inadequate, irrelevant or excessive with regard to those purposes.

In particular, the mere fact that the information was originally published many years ago doesn’t seem to contradict the search engine’s purpose of making the information which is currently existing on the Net available through search results.\textsuperscript{155}

Instead, it could be argued that in such a case the data may be inadequate, irrelevant or excessive with regard to the purposes of processing carried out by the publisher, rather than regarding the purposes of the search engine’s processing.\textsuperscript{156}

But then, the one who would be failing to comply with the data quality principle would be the publisher, not the search engine, and thus, the condition for requesting the delisting under the right to erasure would not be fulfilled. Indeed, the CJEU conditioned the delisting requests under the right to erasure to the fact that the “information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine”.\textsuperscript{157}

\textsuperscript{154} See Grimmelmann, \textit{Speech Engines, supra} note 127 (proposing a normative framework to deal with the provision of search engines’ results premised on the idea that search engines should not be treated neither as passive conduits nor as active editors but as trusted users’ advisors).

\textsuperscript{155} In the same vein, see Bunn, \textit{The curious case of the right to be forgotten, supra} note 149, at 343. See also the AG Opinion, \textit{supra} note 70, para. 98:

Inasmuch as the link is adequate in the sense that the data corresponding to the search term really appears or has appeared on the linked web pages, the index in my opinion complies with the criteria of adequacy, relevancy, proportionality, accuracy and completeness, set out in Articles 6(c) and 6(d) of the Directive.

\textsuperscript{156} The Guidelines published by the WP29 on the application of \textit{Google Spain} reflect this paradox. When considering whether the data are up to date or being made available for longer than is necessary for the purpose of the processing, the document states that “[a]s a general rule, DPAs will approach this factor with the objective of ensuring that information that is not reasonably current and that has become inaccurate because it is out-of-date is forgotten. \textit{Such an assessment will be dependent on the purpose of the original processing.” See Article 29 Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on “Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131/12 (14/EN) WP 225, Nov. 26, 2014 [hereinafter WP29 Guidelines], at 19 (emphasis added).

\textsuperscript{157} See \textit{Google Spain, supra} note 3, para. 94.
It is submitted that what is ultimately determinant for the Court’s position is not the fact that the data are inadequate, irrelevant or excessive for the purposes of the processing, as required by the Directive – in this case the search engine’s processing – but the fact that such processing may have a potentially excessive or disproportionate impact on the individual because of the wide availability and diffusion of search engines and the possibility to obtain a detailed profile of the data subject.\textsuperscript{158} If this is so, it would again show that the Directive constitutes a shaky ground for this right.

Likewise, the Court’s decision to focus only on the scenario where the search is made on the basis of the data subject’s name and requiring only the delisting of the results – a move that will be examined in the next subpart – appears to respond to the same idea. Arguably, should the real concern be that the data are inadequate, irrelevant or excessive for the purposes of the processing, the Court could have also required the complete deletion of the data from the search engine’s index, which it did not. The element of potential serious interference – that would only accrue where the search is made on the individual’s name, and would only need delisting to be avoided – appears thus to be the underlying driver for the Court’s holding,\textsuperscript{159} even though the Court held that a prejudice to the data subject is not required.\textsuperscript{160} That is, however, a different criterion, which could perhaps be better related to the general requirement in Art. 6(1)(a) that the data must be processed “fairly”. Admittedly, though, it might also count as an element to override the “legitimate interest” as a basis for the processing, or as “compelling grounds” on which to object to the processing.

3. A creative surgical approach

\textsuperscript{158} According to the WP29 Guidelines, “[e]ven when (continued) publication by the original publishers is lawful, the universal diffusion and accessibility of that information by a search engine, together with other data related to the same individual, can be unlawful due to the disproportionate impact on privacy.”). See WP29 Guidelines, supra note 156 para. 7 (emphasis added). In the same vein, the WP29 notes that internal search engines on websites do not provide a complete profile of the data subject, and “the results will not have a serious impact on him”, which leads the WP29 to conclude that “as a rule the right to delisting should not apply to search engines with a restricted field of action, particularly in the case of search tools of websites of newspapers”. See id., para. 19.

\textsuperscript{159} See Google Spain, supra note 3, para. 81. See David Lindsay, The ‘Right to be Forgotten’ by Search Engines under Data Privacy Law: A Legal Analysis of the Costeja Ruling, 6 JOURNAL OF MEDIA LAW 159, 178 (2014) (“the CJEU’s analysis was particularly influenced by the extent to which it considered the enhanced accessibility of personal data enabled by search engines to be privacy-intrusive”).

\textsuperscript{160} See Google Spain, supra note 3, para. 96.
As noted, the Court was able to confine the discussion to searches made by the name of individuals, and to assert only a right to delist the link – as opposed to remove the information from the index altogether. This surgical approach was a creative move by the Court. Indeed, when discussing the extent of the obligations of a search engine operator with regard to the right of erasure and the right to object, the CJEU quietly rephrased the wording of the questions referred by the national court. This would allow it to sidestep the question of whether a data subject has a right to have the data removed from the search engine’s index, and affirm instead a more narrowly-tailored right – the right that some links are not displayed on the list of results when a search is carried out on the basis of the data subject’s name.

In fact, the referring court had posed the question of whether, to protect the data subject’s rights to erasure (Art. 12(b)) and to object (Art. 14(a)), the data protection authority could “directly impose on [Google] a requirement that it withdraw from its indexes an item of information published by third parties, without addressing itself in advance or simultaneously to the owner of the web page on which that information is located”.161 And, in the event that the answer to that question was affirmative, whether “the obligation of search engines to protect those rights [would] be excluded when the information that contains the personal data has been lawfully published by third parties and is kept on the web page from which it originates”.162 Purporting to report those questions, the CJEU actually rephrased them by stating that:

the referring court asks, in essence, whether [to comply with the right to erasure and the right to object] the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.163

By rephrasing the questions in this way, the Court was in fact determining beforehand and without a proper discussion that, to comply with the data subject’s rights, a search engine should remove the links from the list of results stemming from a search based on the data subject’s name – something notably different than removing the

---

161 Id., para. 20, Question 2(c) (emphasis added). See also AN Reference Google Spain, supra note 64, at 17.
162 See Google Spain, supra note 3, para. 20, Question 2(c).
163 Id., para. 62. (emphasis added).
information from its index altogether. The discussion in the judgment did not account for this surgical approach to the problem.

When the court addressed the question of whether the information must be prejudicial to the data subject, it again reformulated the original referred question into a more surgical one, considering whether prejudice is necessary for the data subject to have “a right that the information relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name.”

\[D. \text{The Balancing of Rights}\]

The right to data protection does not live in a vacuum; rather it coexists with other rights that must be adequately considered in a careful balancing. This balancing of rights must be done both “inside” and “outside” the data protection legal framework. On the one hand, the Data Protection Directive already contains some provisions that require a balancing of rights to be carried out, and provides for some exceptions and derogations aimed at reconciling data protection with other rights. Nonetheless, those are not the only provisions that must be taken into account before asserting a data subject’s right that may interfere with other fundamental rights recognized in the EU Charter, such as the freedom of expression and information (Art. 11), and freedom to conduct business (Art. 16). Specific criteria for determining whether a limitation to the rights provided by the Charter is acceptable are established in its Art. 52(1). In addition, account must be taken of the European Convention on Human Rights (ECHR) – and thus of the European Court of Human Rights (ECtHR) case law – as the Charter expressly provides that in so far as it contains rights which correspond to rights guaranteed by the ECHR, they will have the same meaning and scope than those in the ECHR.

---

164 See id. para. 89. The referring court had in fact asked whether the rights to erasure and to object extend to enabling the data subject to address himself to search engines in order to prevent indexing of the information relating to him personally, published on third parties’ web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though the information in question has been lawfully published by third parties. See id. para. 20 (Question 3) (emphasis added). See also AN Reference Google Spain, supra note 64, at 17.

165 See Charter, supra note 13, Art. 52(1), which will be transcribed below.

166 See id., Art. 52(3).
The way the CJEU approached the balancing of rights has been the focus of much of the criticism against the judgment. Indeed, a number of shortcomings may be identified in how the court tackled the question. On the one hand, the CJEU limited itself to consider the rules contained in the Data Protection Directive, particularly that of Art. 7(f), in order to balance the fundamental rights to privacy and data protection established in Arts. 7 and 8 of the Charter with other “interests”. It thus failed to engage in a proper balancing in the light of what is established in Art. 52(1) of the Charter. On the other hand, even the analysis carried out under the Directive’s provisions is far from satisfactory.

1. The balancing under the Directive provisions

Let’s recall that the court assumed that the data processing carried out by the search engine operator may find a legitimate basis under Art. 7(f). As noted, under this provision personal data may be processed without the data subject’s consent where “processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).” Thus, Art. 7(f) considers on the one hand the “legitimate interest” of the controller – in this case, according to the court, the search engine operator – and those of the third party or parties to whom the data are disclosed, which in this case would be the users who search for information on the basis of the data subject’s name. Those interests constitute a legitimate ground for the processing only if they are not overridden by the data subject’s fundamental rights to privacy and data


168 See Google Spain, supra note 3, para. 73.

169 See Data Protection Directive, supra note 18, art. 7(f). Art. 1(1) refers to the protection of “the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.”
protection, and hence a balancing is needed.\textsuperscript{170} Actually, all the balancing in which the Google Spain court engaged came down to this particular provision.

The court started by considering the data subject’s rights, and how the processing carried out by the search engine operator is liable to interfere seriously with them when a search is made on the basis of an individual’s name.\textsuperscript{171} Then it stated that “in the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing”.\textsuperscript{172} As a result, the first element of the balancing envisioned in Art. 7(f) was already decided against the controller. That is, the legitimate interests pursued by the controller could not be a ground for legitimate data processing. The remaining factor under Art. 7(f) was then whether the processing could be grounded on the legitimate interest pursued by those to whom the data are disclosed, that is, by users – or whether such an interest is also overridden by the data subject rights. The court stated that “a fair balance should be sought in particular between that interest and the data subject’s fundamental rights under Articles 7 and 8 of the Charter,”\textsuperscript{173} only to immediately declare that “the data subject’s rights protected by those articles also override, as a general rule, that interest of internet users.”\textsuperscript{174} This “general rule” notwithstanding, the court held that

that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject’s private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.\textsuperscript{175}

The above described analysis is all the balancing exercise advanced by the court. It did mention that a balancing is also needed under Art. 14(a) to determine whether the data subject may object “on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation.” According to the court, that balancing “enables account to be taken in a more specific manner of all the circumstances surrounding the data subject’s particular situation.”\textsuperscript{176} However, the court never elaborated on that, nor gave any clue as to how that balancing should be carried out. In fact, regardless of the specific right the data subject

\textsuperscript{170} See Google Spain, supra note 3, para. 74.
\textsuperscript{171} Id., para. 81 (emphasis added).
\textsuperscript{172} Id. (emphasis added).
\textsuperscript{173} Id. (emphasis added).
\textsuperscript{174} Id. (emphasis added).
\textsuperscript{175} Id.
\textsuperscript{176} Id., para. 76.
may invoke – either the right to erasure or the right to object – the Court essentially held that a balancing must be carried out by the search engine operator – or by the supervisor authority or the judicial authority – and that balancing was the one the court carried out under Art. 7(f).

Confining the balancing to the elements set forth in Art 7(f) could hardly result in a satisfactory outcome. For one thing, that provision does not consider the interests of the publisher.\textsuperscript{177} Moreover – following the language of Art. 7(f) – the balance was depicted as one between the data subject’s \textit{fundamental rights} and the “legitimate \textit{interests} of internet users potentially interested in having access to that information.”\textsuperscript{178} In addition, the controller’s interest was considered to be of a mere economic nature.\textsuperscript{179} Such a starting point allowed the CJEU to perceive the “interests” of either the controller or the users, as something of a less value than the data subject’s fundamental rights.\textsuperscript{180} This shows that such a balancing, if it can be understood as such,\textsuperscript{181} is not enough to achieve a result consistent with the Charter. In fact, if the outcome of Art. 7(f) analysis would favor the data subject, she would have a right to stop the data processing as a non legitimate one. However, \textit{that right} should still be confronted with other fundamental rights at stake – not merely interests.

Still under the Directive provisions, the court noted that the balancing under Art. 7(f) could lead to a different outcome in the case of the data processing carried out by the publisher, and notably stated that while the publisher’s processing might be covered by national law exceptions under Art. 9 (for processing carried out solely for journalistic purposes), this “does not appear to be so” in the case of a search engine operator.\textsuperscript{182} The Court’s understanding of Art. 9 in \textit{Google Spain} thus departed from the broader interpretation it had held in a previous judgment – the \textit{Satamedia} case.\textsuperscript{183} In \textit{Satamedia}, the CJEU understood “journalistic activities” as those whose sole objective is “the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to

\begin{footnotes}
\item\textsuperscript{177} See Kranenborg, supra note 150, (noting that the Court was able to leave the interests of the publisher out of the analysis because they are not considered under Article 7(f)).
\item\textsuperscript{178} See \textit{Google Spain}, supra note 3, para. 81 (emphasis added).
\item\textsuperscript{179} \textit{Id.}, paras. 81, 97. See Lindsay, supra note 159, at 178 (noting that “in the required balancing exercise the Court placed little weight on the interests of operators, which it identified as purely economic.”).
\item\textsuperscript{180} See Frantziou \textit{supra} note 167 (“The judgment mislabels a widely protected fundamental right as an ‘interest’, subjects it to a presumption of non-applicability and hence fails to take account of its equal weight in the ‘fair balance’ discussion.”). See also Kuner, supra note 167, at 29-30.
\item\textsuperscript{181} See Frantziou \textit{supra} note 167, at (noting that “seeking to balance rights against interests is questionable as a matter of principle”).
\item\textsuperscript{182} See \textit{Google Spain}, supra note 3, para. 85.
\end{footnotes}
transmit them,” and that “[t]hey are not limited to media undertakings and may be undertaken for profit-making purposes.” The exclusion of search engines in Google Spain from the scope of that provision therefore entails an arguably narrower view than in Satamedia.\footnote{See id, paras. 61-62.}

2. The (missing) balancing under the Charter provisions

The fundamental rights which may be limited as a consequence of asserting a data subject’s right to be delisted – as an expression of their fundamental rights to privacy and to data protection recognized in arts. 7 and 8 of the Charter – are those of freedom of expression and information and freedom to conduct business (enshrined in arts. 11 and 16 of the Charter, respectively). Art. 52(1) of the Charter prescribes that

Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.\footnote{See Charter, supra note 13, Art. 52(1).}

As noted, the CJEU did not engage in weighing whether those rights might in fact be limited by the right to be delisted, and whether such a limitation would meet the criteria set forth in Art. 52(1). The search engine operator’s fundamental right to freedom to conduct business was not even mentioned in the judgment,\footnote{In contrast, the AG reminded that “[a]n internet search engine service provider lawfully exercises both his freedom to conduct business and freedom of expression when he makes available internet information location tools relying on a search engine”. See AG Opinion, supra note 70, para. 132.} which only considered the economic “interests” of the search engine under the balancing required by Art. 7(f). There the CJEU established what it appears to be an absolute presumption that such interests will always be overridden by the data subject’s rights. This stands in contrast with the CJEU’s

\footnote{See Erdos, From the Scylla of Restriction to the Charybdis of License? supra note 40 (noting that since search engines “clearly do disseminate on request information to an indeterminate number of people (albeit on the basis of an individualised request), the Court’s explicit understanding even of ‘journalistic purposes’ [in Google Spain] is clearly inconsistent with an expansive reading of the holding in Satamedia.”). See also Steve Peers, The CJEU’s Google Spain judgment: failing to balance privacy and freedom of expression, EU Law Analysis (2014) http://eulawanalysis.blogspot.co.uk/2014/05/the-cjeus-google-spain-judgment-failing.html.}
own approach in ASNEF and FECEMD.\textsuperscript{188} There, in a case involving the interests of direct marketing companies as controllers, the Court rejected that Spanish law could establish an additional requirement within Art. 7(f) for certain categories of personal data “definitively prescribing, for those categories, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case,”\textsuperscript{189} and stressed the need to leave the outcome of the balancing open.

The fundamental right to freedom of expression was not considered in the balancing, either – beyond the brief mention regarding the Directive’s media exception. Arguably, a fair analysis should consider whether the publisher may rely on the right to freedom of expression in order to have its content disseminated through search engines, and whether the search engine operator may also be exercising this right when displaying the search results.\textsuperscript{190} It is commonly argued that Google Spain does not really affect freedom of expression, because, after delisting, the content is still available on the original source.\textsuperscript{191} Arguably, however, the obscurity that results from delisting search engine’s links to the information affects freedom of expression, at least to some extent. In any event, though, permanence in the origin website is not a result which is mandated by the ruling as a condition to ensure a balanced outcome. In fact, a data subject might also request the deletion in the original source, and the web publisher may be obliged to accommodate such a request if the publisher’s processing happens to go against the Directive provisions, or the data subject has compelling grounds to object to it, and unless the web publisher is covered by the media exception.

Moreover, no reference was made to the fact that the right to receive information is also a fundamental right under the Charter. Under Art. 11 of the Charter, the right to

\textsuperscript{188} ASNEF and FECEMD, supra note 44.

\textsuperscript{189} See id, para. 47. See Peers, The CJEU’s Google Spain judgment, supra note 185 (noting that while in ASNEF and FECEMD the CJEU “criticised the Spanish law for its automaticity, because it failed to weigh up the interests of companies and data subjects in individual cases,” here “it is the Court which sets out an automatic test.”).

\textsuperscript{190} See Erdos, From the Scylla of Restriction to the Charybdis of License? supra note 40 (“the CJEU studiously refused to acknowledge that regulation of the index of a search engine engaged freedom of expression, rather arguing only that this implicated ‘the economic interest of the operator of the search engine’ and ‘the interest of the general public in finding that information’”). See also See Hoboken, Case note, supra note 120, at 1; Orla Lysnkey, Rising like a Phoenix: The ‘Right to be Forgotten’ before the ECJ, European Law Blog (May 13, 2014), http://europeanlawblog.eu/?p=2351; Peers, The CJEU’s Google Spain judgment, supra note 185. On search engines’ legal claims under the right to freedom of expression, see JORIS VAN HOBOKEN, SEARCH ENGINE FREEDOM: ON THE IMPLICATIONS OF THE RIGHT TO FREEDOM OF EXPRESSION FOR THE LEGAL GOVERNANCE OF WEB SEARCH ENGINES (2012).

freedom of expression and information “shall include freedom ... to receive ... information and ideas without interference by public authority and regardless of frontiers.” As noted, this fundamental right was dealt with as a mere “interest”, which as a rule would be overridden by the data subject’s rights.

Finally, no mention was made in the ruling to the need to take into account ECtHR case law as to the meaning and scope of the rights contained in the Charter which correspond to rights included in the ECHR, as required under Art. 52(3) of the Charter. This is particularly relevant, as the ECtHR has already repeatedly dealt with the interplay between the rights to freedom of expression and to privacy (Arts 10 and 8 of the ECHR), and holds that as a matter of principle both deserve equal respect.

IV. LOOKING AHEAD

A. The Right to Be Delisted under the New General Data Protection Regulation

The Data Protection Directive will soon be replaced by a new statute, the General Data Protection Regulation, which was proposed by the EU Commission in January 2012 and is expected to be finally adopted by the end of 2015 or early 2016. The Regulation

---

192 See Charter, supra note 13, art. 11, which uses the same language than Art. 10 of ECHR. The ECtHR has stressed the fact that the right to receive information is part of this right. See ECtHR (2nd Section), December 10, 2012, Yildirim v. Turkey (App. No. 3111/10), paras. 50-55.

193 See Bunn, The curious case of the right to be forgotten, supra note 149, at 343 (noting that this fails to consider the extent to which the interference on the users’ rights is proportionate in protecting the data subject’s rights). See also Rees and Debbie Heywood, supra note 167, at 578 (“[t]he CJEU’s failure to give any serious weight to the public interest in having access to information (other than in limited circumstances) is likely to be the focus of future cases”).

194 See Kulk and Borgesius, supra note 167, see also Frantziou supra note 167.

195 While in a different set of circumstances, the ECtHR has underscored that “it is not the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publications which have in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations.” See ECtHR (4th Section), July 16, 2013, Węgrzynowski and Smolczewski v. Poland (App. No. 33846/07), para. 65, available at http://hudoc.echr.coe.int/eng?i=001-122365. See Frantziou supra note 167, (noting that while Google Spain “is not necessarily incompatible with the ECHR, the Strasbourg Court’s judgment in Węgrzynowski and Smolczewski suggests that such incompatibility cannot be ruled out either.”).

does not change substantially the basic concepts that allowed the CJEU to find a right to be delisted from search engines results under the Directive. The notions of “processing” and of “controller” remain essentially unchanged to that effect. In addition, Art. 7(f) of the Directive, under which the balancing was carried out in *Google Spain*, will be replaced by an almost identical provision – Art. 6(f) of the GDPR.\(^{197}\)

However, the GDPR does include a specific provision which in the last version of the text is titled “Right to erasure and to be forgotten”,\(^ {198}\) and which has been the subject of much academic commentary since it was originally proposed. Nonetheless, the provision does not deal specifically with search engines – it does not establish particularly a data subject’s right to request the delisting of links displayed in search engines’ results after queries in their name. Rather, it sets forth a general right to erasure, imposing on the controller the obligation to erase the data in a number of cases which to a large extent were, at least implicitly, already considered under the Directive – such as where the data have been unlawfully processed; they are no longer necessary in relation to the purposes of the processing; the data subject appropriately objects to the processing or withdraws consent and there is no other legal ground for the processing.\(^ {199}\) The main novelty – which apparently is the one that justifies the language “right to be forgotten” in the title of the Article – consists in imposing on controllers which have made the data public the obligation to inform other controllers which are processing the data that the data subject has requested that they erase any links, copy or replication of that data.\(^ {200}\)

On the one hand, thus, the new Regulation does not codify *Google Spain*.\(^ {201}\) On the other hand, it is not likely that a provision dealing with the intermediary role of search engines is included in the final version of the GDPR.

While it does not address the ruling’s shortcomings identified above, the GDPR might offer a better opportunity to include freedom of expression and information into the equation. First, in view of the amendments suggested by the Parliament and the Council, the language of the provision equivalent to the Directive’s media exception – art. 80 GDPR – might end up substantially broadening its scope, no longer being limited to data

\(^{197}\) The proposed Art 6(f) GDPR introduces a specific consideration to the case where the data subject is a child. On the other hand, it refers generally to the legitimate interests pursued “by a third party”, instead of “by the third party or parties to whom the data are disclosed.” *See id.*, art. 6(f) (emphasis added).

\(^{198}\) *See id.*, art. 17.

\(^{199}\) *Id.*

\(^{200}\) *See* Christiana Markou, *The ‘Right to Be Forgotten’: Ten Reasons Why It Should Be Forgotten*, *in Reforming European Data Protection Law* 203 (Serge Gutwirth, Ronald Leenes & Paul de Hert eds., 2015) (criticizing the choosing of this title for the proposed article).

\(^{201}\) Neither the amendments introduced by the European Parliament in March 2014, nor the Council’s version of June 2015, imported the *Google Spain* holdings.
processing carried out solely for journalistic purposes.\textsuperscript{202} Second, and remarkably, the provision on right to be forgotten – art 17 GDPR – explicitly states that the controller’s obligation shall not apply to the extent the data processing is necessary for exercising the right of freedom of expression.\textsuperscript{203}

\textit{B. Practical Fixes}

The extent to which the future GDPR will provide a basis for a more nuanced balancing of rights is still uncertain. In the absence of a more general solution, probably the only practical way to bypass some of the shortcomings indentified in the judgment seems to be a careful application by national courts and DPAs that takes into account all the rights at stake. The characterization of search engines operators as controllers with regards to content data, even if inconsistent with the role of an intermediary, cannot be avoided unless the CJEU changes its approach, which looks unlikely. Nonetheless, national courts and DPAs, are able to use their discretion in applying the CJEU’s interpretation criteria to the particular cases, using the little room it actually conceded – for instance, “as a rule” does not mean “always” – and particularly resorting to the Charter’s provisions.

As the CJEU noted in \textit{Lindqvist}, it is “at the stage of the application at national level of the legislation implementing Directive 95/46 in individual cases that a balance must be found between the rights and interests involved.”\textsuperscript{204} It also stated that “[i]n that context, fundamental rights have a particular importance,” noting that, in the specific case before it, freedom of expression had to weighed against the protection of private life. Consequently, the court noted,

it is for the authorities and courts of the Member States not only to interpret their national law in a manner consistent with Directive 95/46 but also to make sure they do not rely on an interpretation of it which would be in conflict with the fundamental

\textsuperscript{202} See GDPR comparative table, \textit{supra} note 5, art. 80. The text agreed by the Council mandates member states to “reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, \textit{including} the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression.” (Emphasis added).

\textsuperscript{203} While in the Commission’s and Parliament’s versions the exception was “for exercising the right of freedom of expression in accordance with Article 80;” the Council version reads “for exercising the right of freedom of expression and information,” without an express link to the derogations provided under Art. 80. \textit{See} GDPR comparative table, \textit{supra} note 5, art. 17.

\textsuperscript{204} \textit{Lindqvist}, \textit{supra} note 41, para. 85.
rights protected by the Community legal order or with the other general principles of Community law, such as inter alia the principle of proportionality.205

In applying the right to be delisted to particular cases, national courts and DPA should carry out a careful balancing, both within the Directive – or the GDPR when it is finally adopted – and under the criteria established in the Charter of Fundamental Rights. Both a full consideration of the particular circumstances of the case under the Directive, and the unavoidable balancing with other rights under the Chapter may lead to outcomes that while protecting the data subject’s rights are also respectful with the other rights at issue.

Ultimately, though, this is just a partial solution, as the vast majority of cases will be dealt with only by search engine operators – only a fraction of the operators’ decisions against delisting are likely to be appealed before courts or DPAs. This underscores again the problematic outcome of Google Spain, which vests private companies with the power to determine how the balancing will be carried out in practice.206 Such a question, though, can only be properly addressed with legislative intervention.207

V. CONCLUSION

In its landmark Google Spain judgment, the Court of Justice of the European Union devised what may be labeled a “right to be delisted” as a solution to the problems posed to individuals by search engines’ results pointing to personal information about them. The CJEU tackled this issue resorting to data protection law, and found that under the current Data Protection Directive – construed in the light of the EU Charter of Fundamental Rights, which explicitly includes the right to the protection of personal data – an individual may request that some results no longer be displayed in a search carried out on the basis of her name.

The court tried to reach a balanced outcome by crafting a somewhat narrow right – it only referred to the possibility of requesting the delisting of search results in searches made on the basis of the individual’s name, leaving the content to still be found using

205 Id., para. 87
206 See Lindsay, supra note 159 p. 178.
207 See Alessandro Mantelero, Finding a Solution to the Google’s Dilemma on the ‘Right to Be Forgotten’, after the ‘Political’ ECJ Decision (2014), http://ssrn.com/abstract=2528565 (proposing that the GDPR includes a provision excluding the direct enforcement by search engines and requiring a complaint before a court or a DPA, with an initial temporary delisting of the challenged links conditioned to the filing of the complaint).
different search terms. At the same time, however, the conditions to exercise this right – for instance, that content is inadequate, irrelevant or no longer relevant – are overly vague, and the right is not limited to the cases where private information is involved, nor does it require the content to be inaccurate, unlawful or even to cause harm. The reason for this extremely broad scope is to be found in the legal field to which the Court resorted – data protection law. EU data protection law is a very powerful instrument which needs some counterbalances so as to avoid certain far-reaching results that its all-embracing scope may lead to. Nonetheless, the Court arguably failed to devise appropriate criteria to balance it with competing rights, particularly that of freedom of expression and information, also recognized by the Charter.

The potentially harmful interference a person may face when some compromising content pops up after querying his or her name online can hardly be overstated. The solution provided, however, has proven to be highly controversial – particularly when seen from other legal traditions, but within Europe as well. This article has chosen not to delve into the more ideological debate prompted by the ruling, but has instead chosen to explore the solidness and weaknesses of the grounds on which the right to be delisted is built, and to expound on the nuances of EU law to contribute to a better understanding of some of the less obvious features of the newly recognized right.

In addition to the drawbacks deriving from the arguably flawed balance envisioned by the CJEU, and the unintended consequences that may follow from the lack of incentives for search engines to challenge the delisting requests, a more fundamental problem resides in the constrains imposed by the legal framework on which the right to be delisted is grounded, as it does not allow for the recognition of the intermediary role played by generalist search engines. In order to impose on search engine operators the duty to assess the individuals’ requests and to accommodate them when justified, the Court needed to consider search engines as data controllers of the personal data included in the indexed websites, a characterization which is arguably at odds with their intermediary role and which actually makes their activity – in the absence of specific safeguards – largely incompatible with the data protection legal framework. The intermediary role of generalist search engines should be adequately protected under EU law, both within the general scheme of liability limitation set forth in the E-Commerce Directive, and under data protection law. Only then a right to be delisted, with all the necessary limitations and due account of the competing rights, might be established on solid ground.