The Shaky Ground of the Right to Be Delisted

Miquel Peguera*

ABSTRACT

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. Agencia Española de Protección de Datos, the Court of Justice of the European Union (CJEU) 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 both in favor and against the ruling, 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 that 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, this Article discusses how the “right to be delisted” was crafted by the CJEU. It then argues that the “right” 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

* Ph.D., mpeguera@uoc.edu. Associate Professor of Law, Universitat Oberta de Catalunya (Barcelona, Spain); Affiliate Scholar, Stanford Law School Center for Internet and Society; and Researcher, Internet Interdisciplinary Institute (IN3). Thanks to Agustí Cerrillo, Giancarlo Frosio, Eric Goldman, James Grimmelmann, Martin Husovec, Daphne Keller, Alessandro Mantelero, and Frank Pasquale. Thanks also to the Journal’s editors for their great editing job. All errors remain my own.
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. The Article further 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 protection, 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.

**TABLE OF CONTENTS**

I. INTRODUCTION .............................................................. 509

II. THE EU LEGAL FRAMEWORK ON PERSONAL DATA
    PROTECTION ........................................................................ 514
    A. Some Key Elements of the Data Protection Directive 516
    B. The Pivotal Notions of “Personal Data,” “Processing,”
       and “Controller” .......................................................... 518
    C. Conditions for Lawful Processing ............................... 520
    D. The Right to Have the Data Erased and to Object to its
       Lawful Processing ......................................................... 522

III. GOOGLE SPAIN ................................................................. 522
    A. How the Case Originated and Reached the CJEU ........ 522
    B. Finding a Right to Be Delisted Under the Data
       Protection Directive ...................................................... 527
    C. Follow-Up by the National Court .................................. 532

IV. A RIGHT ON SHAKY GROUND? .............................................. 534
    A. Search Engines as Data Controllers ............................ 534
    B. Protecting Search Engines’ Intermediary Role ................. 541
       1. Intermediary Liability Safe Harbors ......................... 541
       2. Intermediaries Under the Data Protection
          Legal Framework ..................................................... 544
    C. The Legal Basis for Having the Links Delisted ............... 545
       1. Overlapping Rights ................................................ 545
       2. Is it the Search Engine’s or the Publisher’s
          Processing? ................................................................ 547
       3. A Creative Surgical Approach Taken by the
          CJEU ........................................................................ 549
    D. The Balancing of Rights .............................................. 551
       1. The Balancing Under the Directive Provisions ... 552
       2. The (Missing) Balancing Under the Charter
          Provisions .................................................................. 554
I. INTRODUCTION

The United States should adopt the “right to be forgotten” online. This was the motion under discussion in an Intelligence Squared US debate held in New York on March 11, 2015.1 Two teams put forward their arguments for and against the motion before the audience,2 which would cast its vote at the end of the debate. The discussion focused on whether it would be advisable for the United States 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 European Union (CJEU), in Google Spain v. Agencia Española de Protección de Datos.3 There, the CJEU addressed the issue of whether an individual may obligate a search engine’s operator to remove search results linking to information that included personal data related to that individual.4 The CJEU found that under EU law on personal data protection, a search engine does have the obligation, under certain 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 executed.5

The extent of this right is broader than what people unfamiliar with the ruling might think. Indeed, 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 (i.e., a civil action on defamation). One may think, then, that the right is confined to cases where the information is false or inaccurate. But it is not—while the right may be exercised with

---

2. In favor of the motion were Eric Posner and Paul Nemitz. Against the motion were Jonathan Zittrain and Andrew McLaughlin. The debate was moderated by John Donvan.
4. Id. ¶ 62.
5. Id. ¶ 88.
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 information at issue 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 is 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, yet the search engine still would be obliged to not 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? Essentially, this is what the court held. Specifically, it found that the right may be exercised whenever the information is “inadequate, irrelevant, no longer relevant or excessive,” unless the public has a preponderant right to access 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 behind the whole idea of having some degree of control over one’s personal information online. True, the CJEU ruled out the need to prove prejudice, but it nevertheless decided the case on the assumption that an individual might suffer real harm as a consequence of people stumbling on that information after typing that individual’s name into Google.

These harms have been detailed in more general debates about the right to be forgotten. Proponents of the right have long argued that the-web-that-never-forgets stands 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, or 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, 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. It also addressed the fact that person-based queries may produce a more or less detailed profile of the individual.

As will be discussed later, seeking to reach a moderate, not too far-reaching result, the CJEU chose to creatively sidestep the question originally posed before it. Instead of discussing whether the individual may request the removal of said information from the search engine’s index altogether, the CJEU 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 a consequence, the information could still be found in searches using terms other than person’s name. In this vein, the right

---

6. 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; see also Pere S. Castellano, The Right to be Forgotten Under European Law: A Constitutional Debate, 16 LEX ELECTRONICA 1 (2012); Cécile de Terwangne, Internet Privacy and the Right to Be Forgotten/Right to Oblivion, 13 IDP REVISTA DE INTERNET, DERECHO Y POLÍTICA 109, 119 (2012), http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-terwangne_esp/n13-terwangne_eng [perma.cc/JKU3-2EJF].

envisioned by the CJEU can be best described as a “right to be delisted.”

From a US law perspective, both 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 seem difficult to accommodate; although it has been noted that US law also recognizes some limited forms of a right to be forgotten. Many US commentators oppose a right with such a broad reach, though they acknowledge that it attempts to address an important problem. In contrast, others have shown sympathy for this new development, and some observers have noted that, in fact, US privacy law might already be leaning towards a more European approach.

This Article seeks to shed light on 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

---

8. The term “right to be delisted” has already been used in the literature. See, e.g., Brendan van Alsenoy and Marieke Koekkoek, Internet and Jurisdiction After Google Spain: The Extraterritorial Reach of the “Right to be Delisted,” 5 INT’L DATA PRIVACY LAW 105 (2015).

9. 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. 1173, 1183 (2015); Robert Lee Bolton III, The Right To Be Forgotten: Forced Amnesia In A Technological Age, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 133, 144 (2014) (noting public policy objections to a right to be forgotten); 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, 633 (2015) (“If 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 K. Walker, The Right to be Forgotten, 64 HASTINGS L.J. 257, 261 (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 US constitutional law).


11. Regarding the right to be forgotten as drafted in the GDPR Proposal, supra note 7; 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”).


13. See Eric Posner, We All Have the Right to be Forgotten, SLATE, May 14, 2014; see also Koenig & Rustad, supra note 9, at 634 (“The EU’s ‘right to erase’ provision would be particularly useful to America’s poor and less educated who seek to remove evidence of their spoiled identity.”).

data protection, thus enabling a better understanding of the right, and its shortcomings. Part II offers an introduction to the current EU legal framework on data protection, covering the most relevant concepts to the crafting of this right. That discussion 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 CJEU’s recognition of this right. Part III presents the facts and main holdings of the landmark Google Spain case. Part IV moves on to discuss the legal ground of the right to be delisted. Section IV.A argues that the right is on shaky ground, as its main premise under the EU legal framework on data protection—the characterization of a search engine as a “data controller”—is problematic.15 Section IV.B puts forward the need to protect search engines’ intermediary role. It both discusses their legal status under the liability limitations set forth in EU law and also suggests that data protection law should take this role into account, thus crafting specific provisions to avoid imposing a bundle of obligations on search engines that are at odds with their actual functions and possibilities. Section IV.C further discusses the specific legal basis and conditions to request delisting. Section IV.D explores the shortcomings that can be identified in the balancing of rights envisioned by the CJEU. Next, Part V considers if the scenario may change under the 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 to overcome some of the problems detected. Finally, a brief conclusion summing up the arguments of the paper is provided in Part VI.

The audience in the Intelligence Squared debate was not ultimately persuaded to adopt a right to be forgotten in the United States—nonetheless, other polls suggest that American citizens would approve of the right’s adoption.16 Unsurprisingly, the assertion that individuals have a right to even limited control of what search engines may display in search results about themselves is rather controversial.17 There are many assumptions involved, including

---

17. See, e.g., Solove, supra note 10; Sophie Curtis & Alice Philipson, Wikipedia Founder: EU’s Right to be Forgotten is ‘Deeply Immoral,’ TELEGRAPH, Aug. 6, 2014; Washington Post’s
different visions of key ideological aspects of the right, which have sometimes made the academic and social discussion vehement. This Article will not take sides on that front. However, in exploring the nuances of this right within the legal context in which it emerged, this Article will underscore some of the right’s problems and call for an approach that better reflects the intermediary nature of search engines. All in all, this 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.

II. THE EU LEGAL FRAMEWORK ON PERSONAL DATA PROTECTION

The right to the “protection of personal data” is recognized by the EU Charter of Fundamental Rights (“Charter”), where it is separately established in Article 8 from the right to “respect for private and family life,” laid down in Article 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. Now recognized as a fundamental right, data

---


19. Art. 8 of the Charter, supra note 18, 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.

Art. 8 of the Charter, supra note 18.

20. On the character of data protection and privacy as independent rights, see Orla Lynskey, Deconstructing Data Protection: The ‘Added-Value’ 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).

protection enjoys the highest status within EU law—along with the rest of fundamental rights equally recognized by the Charter. The right is also recognized in Article 16 of the Treaty on the Functioning of the EU (TFEU), which refers particularly to the protection of individuals with regard to the processing of personal data by EU institutions.22

Before the EU embarked on the adoption of a catalogue of fundamental rights, the 1995 Data Protection Directive ("Directive")23 laid down a legal framework for data protection that is still in force.24 A substantial overhaul of the EU data protection regime is being prepared in the form of a General Data Protection Regulation (GDPR), which is expected to be formally adopted in the first months of 2016, and would enter into force in 2018, two years after its official publication.25 This Article deals primarily with the Directive because it both 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 how the right to be delisted might be affected by the GDPR.

The purpose of the following Sections 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 III.

22. See Consolidated version of the Treaty on the Functioning of the European Union, Oct. 26, 2012, 2012 O.J. (C 326) 47, 55, art. 16 [hereinafter TFEU]. This Treaty is the result of amending and renaming the Treaty establishing the European Community (the TEC Treaty) by the Treaty of Lisbon in 2007. Art. 16 TFEU replaced the old art. 286 TEC, which was introduced in 1997, two years after the passing of the Directive 95/46—to which we will immediately refer. Since Directives are addressed to Member States, this art. 286 TEC was introduced so that the legal framework on data protection would apply as well to the Community institutions and bodies.


24. 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.

25. See GDPR final draft, supra note 7.
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.\(^\text{26}\) This 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. In addition, the processing must respect the “data quality” principle,\(^\text{27}\) which seeks to ensure, \textit{inter alia}, that the data are adequate, relevant, and not excessive in relation to the purposes for which they are collected or further processed. 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”).\(^\text{28}\)

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 the right to be 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),\(^\text{29}\) but also to those established outside the EU or 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 or EEA Member State.\(^\text{30}\)

\(^{26}\) See Data Protection Directive, supra note 23, art. 7.

\(^{27}\) Id. art. 6.

\(^{28}\) Id. art. 8.

\(^{29}\) The European Economic Area (EEA) includes all EU Member States and three non-EU members, namely Iceland, Liechtenstein, and Norway.

\(^{30}\) See Data Protection Directive, supra note 23, art. 4(1)(a). 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.” Id.
The Directive also envisions both an administrative and judicial system of enforcement. It requires that, in each Member State, one or more independent authorities, called Data Protection Authorities (DPAs), supervise the application of the national law implementing the Directive. These DPAs are vested with powers including 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 “transposition,” they must achieve the results prescribed by the Directive. 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 that is consistent with EU law.

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. These preliminary rulings do not decide on the particular facts of the case, but rather 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 that interprets EU law and guides national courts’

31. See TFEU, supra note 22, 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.”).
33. See TFEU, supra note 22, 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 to make the reference for a preliminary ruling. See id.
34. See id.
application of their own national law in a manner consistent with EU 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, and a representative of the European Commission. The WP29 advises the European Commission and regularly delivers opinions, recommendations, and reports on not only issues covered by the Directive, but also generally on any question regarding data protection. While its opinions are not binding, they constitute in practice a powerful 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 that are conceived in a very broad way. “Personal data” is defined as “any information relating to an identified or identifiable natural person,” or “data subject.” In 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.” In its preamble, the Directive notes that “to determine whether a person is identifiable, account

35. 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.


38. See Data Protection Directive, supra note 23, art. 2(a).

39. See id. For a comparison between the European notion of personal data and the parallel concept of “personally identifiable information” in the United States, see Paul M. Schwartz and Daniel J. Solove, Reconciling Personal Information in the United States and European Union, 102 CAL. L. REV. 877 (2014) (proposing a tiered approach to the concept of “personally identifiable information” so as to bridge the differences between the EU and the US frameworks).
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”40 and
excludes “data rendered anonymous in such a way that the data
subject is no longer identifiable.”41

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 interpretation criteria for
a uniform understanding of the concept.42 The opinion makes it clear
that the information considered as personal data is not limited to
information related to the individuals’ private life; instead, it may be
any kind of information.43 According to the WP29, there is no need to
know someone’s name for that person to be “identifiable”; rather it
may be enough that this person can be “singled out,” for instance with
a unique identifier.44

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.”45 It is difficult to
think of any action that could fall outside this all-embracing
definition. Indeed, the method chosen by the Directive to limit the
reach of its rules is not to limit the notion of what constitutes data
processing, but rather to exclude some types of actual data processing
from its scope.

The following limitations should be noted in this respect. First,
the Directive only applies to “the processing of personal data wholly or
partly by automatic means, and to the processing otherwise than by
automatic means of personal data which form part of a filing system
or are intended to form part of a filing system.”46 Second, the
processing operations concerning public security, defense, state
security, activities of the state in areas of criminal law, and other

41. See *id.*
43. See *id.* at 6.
44. See *id.* at 14.
46. *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.” *Id.* art. 2(c).
similar instances are also excluded.\textsuperscript{47} Third, the Directive contains a so-called “household exception,” which leaves outside its scope the processing of personal data carried out “by a natural person in the course of a purely personal or household activity.”\textsuperscript{48} Finally, Article 9 of the Directive mandates that Member States provide exceptions for the processing of data carried out solely for journalistic purposes or for the purpose of artistic or literary expression, inasmuch as they are necessary to reconcile the right to privacy with the right to freedom of expression.\textsuperscript{49} The extent of these eventual exceptions for freedom of expression depends thus on each member state’s national law.\textsuperscript{50}

Another key notion in the Directive is the already mentioned concept 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.”\textsuperscript{51} The controller is 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 that processes personal data on behalf of the controller.\textsuperscript{52}

\textbf{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 include that of having a legitimate basis and that of respecting the principle of data quality.\textsuperscript{53}

Regarding the legitimacy of the processing, the Directive provides for several possible grounds.\textsuperscript{54} The first one, already pointed

\textsuperscript{47} Id. art. 3(2).
\textsuperscript{48} Id. 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 Art. 29 Working Party Opinion 5/2009 on online social networking (01189/09/EN) WP 163, Jun. 12, 2009, at 6.
\textsuperscript{49} See Data Protection Directive, supra note 23, art. 9. For more on the origins and interpretation of this provision, see David Erdos, \textit{From the Scylla of Restriction to the Charybdis of License? Exploring the Present and Future Scope of the ‘Special Purposes’ Freedom of Expression Shield in European Data Protection}, 52 COMMON Mkt L REv. 119 (2015).
\textsuperscript{50} See Case C-101/01, Bodil Lindqvist (Nov. 6, 2003) ¶ 90 [hereinafter Lindqvist].
\textsuperscript{51} See Data Protection Directive, supra note 23, art. 2(d).
\textsuperscript{52} Id. art. 2(e).
\textsuperscript{53} See Data Protection Directive, supra note 23, Articles 6 and 7; see also Article 8 of the Charter, supra note 19.
\textsuperscript{54} The CJEU has declared that Article 7 of the 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 Joined Cases C-468/10 and C-469/10, ASNEF and FECEMD, Nov. 24, 2011, ¶ 30 [hereinafter ASNEF and FECEMD].
out, is the data subject’s consent for the processing. In the absence of consent, the processing may still be legitimate under another of the alternative grounds provided for in Article 7. One of those grounds, set forth in Article 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.”\(^5\) However, Article 7(f) does not provide an absolute basis because it expressly excludes the case where those interests “are overridden by the interests or fundamental rights and freedoms of the data subject.”\(^6\) A balance is thus required to determine if a particular case of processing may rely on that ground for lawfulness.\(^7\)

Data processing must also respect the data quality requirements laid down in Article 6. Accordingly, personal data must be collected for specific purposes and not further processed in a way that is incompatible with those purposes. Likewise, data must be “adequate, relevant and not excessive” in relation to the purposes of the processing and be “accurate and, where necessary, kept up to date,” and the provision establishes that “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.”\(^8\) In addition, 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,”\(^9\) and Member States must “lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.”\(^10\)

---

55. See Data Protection Directive, supra note 23, art. 7(f).
56. Id.
57. While under Article 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. See ASNEF and FECMD, supra note 54, ¶¶ 36–39. The WP29 released a detailed opinion in 2014 providing criteria on how this balance should be carried out. See Art. 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.
58. See Data Protection Directive, supra note 23, art. 6(b)–(d).
59. Id. art. 6(e). See Alessandro Mantelero, The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten,' 29 COMPUTER L. & SECURITY REV. 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”).
60. See Data Protection Directive, supra note 23, art. 6(e).
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. Two of them will be of particular relevance for the CJEU’s recognition of what may be called a “right to be delisted.” First, the data subject has the right to have the data “erased.” Article 12(b) of the Directive 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.” 61 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 Article 6. 62

Even where the processing fully complies with the provisions of the Directive, including the data quality principle, a data subject may still “object” to that processing in some situations. This “right to object” is provided for in Article 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 him, save where otherwise provided by national legislation.” 63 However, 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.” 64

III. 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

---

61. Id. art. 12(b) (emphasis added).
62. In this case, the data processing would fail to comply with id. art. 6(d) (“[P]ersonal 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 . . . .”).
63. Id. art. 14(a) (emphasis added).
64. Id.
estate properties following attachment procedures for the recovery of Social Security debts. A person by the name of Mario Costeja González was named in the announcement as co-owner of one of the properties. There was nothing untrue or inaccurate in the information provided. 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 resolved 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 United States, as the latter was the entity that actually ran the search engine. In March 2010, he filed a complaint before the Agencia Española de Protección


66. See id. Article 117 of the General Regulation on the Collection of Social Security Contributions provides that the announcement of the auction of seized goods may be published in mass communication media with big circulation or in specialized publications if it is convenient to the end sought and proportionate to the value of the goods. The same article establishes that the announcement of the auction will include, inter alia, a description of the goods and its ownership. Spanish Royal Decree 1415/2004, Jun. 11 2004, http://www.boe.es/diario_boe/txt.php?id=BOE-A-2004-11836 [perma.cc/R8J2-KDW7].

67. See Audiencia Nacional, Reference for a preliminary ruling to the Court of Justice of the European Union of Feb. 27, 2012, Google Spain, Google Inc., v AEDP, Mario Costeja González, ECLI:ES:AN:2012:19A, at 1–2, http://www.poderjudicial.es/search/indexAN.jsp [https://perma.cc/3G7J-JABX] (searching for ECLI:ES:AN:2012:19A) [hereinafter AN Reference Google Spain]. It must be noted that in Spain the names of individuals are anonymized in the published version of court rulings, where fictitious names are used instead. In this case, the name of Mario Costeja González was changed into that of “Carlos José.”


69. See AN Reference Google Spain, supra note 67, at 1–2.

70. Id. at 2.

71. Id.

72. Id.
de Datos (AEPD)—the Spanish DPA—against La Vanguardia, Google Spain SL, and Google Inc.\textsuperscript{73}

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 access, rectification, erasure, or objection—but only against Google Spain and Google Inc., leaving the news publisher out.\textsuperscript{74} The procedure ended with a decision handed down by the AEPD on July 30, 2010,\textsuperscript{75} which upheld the claimant’s petition against Google Spain and Google Inc., ordering the search engine “to adopt the necessary measures to remove the data from its index and prevent future access to them.”\textsuperscript{76}

In its decision, the Spanish authority built on the premise that an ordinary citizen—one who is neither a public figure nor is involved in some publicly relevant event—need not resign herself to having her personal data available on the Internet.\textsuperscript{77} It noted, nonetheless, 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.\textsuperscript{78} Having said that, the AEPD asserted that, once the data appear online, ordinary citizens must have the possibility to react—for instance, by means of the right to erasure.\textsuperscript{79} Thus, the AEPD concluded that Mr. Costeja’s

\textsuperscript{73} Id.

\textsuperscript{74} 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. See Agencia Española de Protección de Datos, Decision n° R/01680/2010 of July 30, 2010, procedure TD-00650-2010 against Google Inc., Google Spain S.L. and La Vanguardia Ediciones S.L., at 22–23, http://www.agpd.es/ (searching for TD-00650-2010) [hereinafter AEPD Costeja].

\textsuperscript{75} Id.

\textsuperscript{76} Id. (emphasis added). Apparently, the obligation was imposed on Google Inc., though the wording of the decision is not very clear. The decision states 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 only the latter—that is, Google Inc.) to remove the data and prevent future access to them. However, saying that it upholds the complaint against Google Spain and Google Inc. seems to indicate that the Spanish company is also considered responsible for the removal. See AEPD Costeja, supra note 74, at 23. The CJEU, nonetheless, depicts the AEPD decision as ordering only Google Inc. to remove the data from the index. See Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014), http://curia.europa.eu/juris/liste.jsf?num=C-131/12, ¶ 2.


\textsuperscript{78} See AEPD Costeja, supra note 74, at 20.

\textsuperscript{79} Id.
petition to have his personal data erased should be upheld to avoid permanent effects against his will.\footnote{80}{Id.}

The AEPD decision did not elaborate much on whether or not the claimant’s petition met the legal requirements. In particular, the decision did not expressly discuss whether the right to erasure was appropriate because the processing did not comply with the provisions of the Directive,\footnote{81}{See Data Protection Directive, supra note 23, art. 12(b).} 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.\footnote{82}{See id. art. 14(a). In fact, however surprising it may be, it is not clear at all from the text of the AEPD 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 AEPD decision seemed to refer specifically to the right to object, without any reference to the compelling legitimate grounds of the data subject.}

Likewise, the decision contained no discussion as to whether Google fit the legal notion of a controller. The AEPD 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 that considers a search engine to be a controller.\footnote{83}{See AEPD Costeja, supra note 74, at 8.} However, the quoted passage does not relate to the processing of the data included in the linked-to websites, but instead to the processing of Google users’ data—thus hardly applying to the case at hand.\footnote{84}{See Art. 29 Working Party Opinion 1/2008 on Data Protection Issues Related to Search Engines (737/EN) WP 148, at 9, Apr. 4, 2008 [hereinafter WP29 Opinion on Search Engines].}

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, because it limited itself to promoting the selling of advertising space and did not intervene in the activity of the search engine.\footnote{85}{See AEPD Costeja, supra note 74, at 2–3.} Rather, its parent company, Google Inc., solely provided the search services and carried out all the functions relating to the indexing and provision of search results.\footnote{86}{Id.} Google Spain SL also contended that EU data protection law was not applicable to the US company. Finally, Google Spain SL argued that Google Inc. could not be deemed the controller in any event because the main entities responsible for the processing were the publishers of the websites where the personal data had been included.\footnote{87}{Id. at 3. 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
were rejected by the AEPD, though some of them were rejected only by implication.\textsuperscript{88} The AEPD placed its greatest effort on justifying that Spanish law and the Data Protection Directive did apply to Google, asserting 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.\textsuperscript{89}

Both Google Spain and Google Inc., in separate briefs, appealed the AEPD decision before the Audiencia Nacional (AN), 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 EU data protection law, were being brought before the AN.

The AN decided to make a reference for a preliminary ruling to the CJEU,\textsuperscript{90} simply picking the Costeja case out of the many cases appealed before it.\textsuperscript{91} The AN posed three groups of questions to the CJEU. Regarding the territorial scope, the AN harbored doubts about the AEPD’s interpretation of the connecting factors, particularly regarding the fact that the processing is carried out in the context of the activities of an establishment of Google Inc. located in Spain.\textsuperscript{92} The AN 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 advertisements were displayed along with the search results. The AN 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

\begin{itemize}
\item \textsuperscript{88} See id. at 2–3.
\item \textsuperscript{89} See id. at 14–15. This would trigger the applicability of the DP Directive. See Data Protection Directive, supra note 23, art. 4(1)(a).
\item \textsuperscript{90} See generally AN Reference Google Spain, supra note 67.
\item \textsuperscript{91} At the time of the reference, there were some 130 appeals pending before the Audiencia Nacional. See id. at 16.
\item \textsuperscript{92} See id. at 8–9. That connecting factor is set forth in Article 4(1)(a) of the Data Protection Directive. 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—Article 4(1)(c)—and even asked 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. Id.
\end{itemize}
promoting and selling advertising space on the search engine, which orientates its activity towards the inhabitants of that State.”

The second set of questions the AN posed to the CJEU related to how Google’s activity as a search engine fit in the Directive. Particularly, the AN asked 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 AN 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 doubts as to whether the search engine could be considered a controller. Even if it were to 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 AN asked the CJEU whether the data protection authority might directly order the search engine to remove from its index a piece of information published by a third party, without addressing itself in advance or simultaneously to the publisher. The AN 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 inquired 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, 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 Charter. The ruling was preceded by the
Advocate General’s (AG) opinion. The AG had concluded that, while the Directive does apply, a search engine cannot be considered a controller of the data processing except in limited situations. The AG had further found that even if a search engine were to be considered a controller, a data subject could not prevent a search engine from indexing personal information legally published on third parties’ web pages, invoking that it might be prejudicial to her or that she wishes it to be forgotten. As to the core issues—the search engine’s characterization as a controller and the scope of the data subject’s rights to erasure and to object—the CJEU 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, it held, in contrast to the AG’s conclusions, that the search engine determines the purposes and the means of that processing, and thus must be regarded as a controller. According to the CJEU, 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.” Such processing could significantly affect data subjects’ rights, because users who 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. Those users thus can “establish a more or less detailed profile of the data subject.” As a controller, the CJEU noted, a search engine “must

---

100. 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 of 25 September 2012, art. 82, 2012 O.J. (L 265) 1, 22. Where the court decides 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, 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, 763 (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).


102. Id.


104. Id. ¶ 35.

105. Id. ¶ 37.
ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive.”

As to the applicability of the Directive, the CJEU concluded 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,” that processing “is carried out in the context of the activities of an establishment of the controller on the territory of a Member State,” which triggers the applicability of the Directive pursuant to Article 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 requesting the delisting of the links—the CJEU pointed out that all processing of personal data must both comply with the data quality conditions and be based on one of the legitimacy grounds set out in the Directive. Regarding legitimacy, the CJEU expressly acknowledged that the processing by a search engine “is capable of being covered by the ground in Article 7(f),” which—as noted earlier—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.”

If the processing lacks a legitimate ground or fails to meet any of the data quality requirements, the data subject would have the right to obtain from the controller, as appropriate, the erasure of the data. Furthermore, even if the processing both respects the data quality requirements and is based on a legitimate ground, the data subject could still object to the processing on compelling legitimate grounds relating to her particular situation, except where 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

106. Id. ¶ 38.
107. Id. ¶ 60.
108. Id. (emphasis added).
110. See id. art. 7.
112. See Data Protection Directive, supra note 23, art. 7(f).
113. See id. art. 14(b).
data in question."  

Where the search engine did not grant the request, the data subject could resort to the DPA or the judicial authority, who would then assess the request and potentially 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 evaluate 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 the 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 measured 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 CJEU, as it stated that “data subject’s rights protected by [Articles 7 and 8 of the Charter] also override, as a general rule, that interest of internet users.” Nonetheless, the court noted that 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.”  

In addition, the CJEU answered that the obligation of the controller to end the processing is not conditioned on the fact that the publisher removed the information previously or simultaneously from the web page, and the controller’s obligation is not affected by the fact that the information was lawfully published on the Internet. The CJEU stressed that those are two different processing operations and

114. See Google Spain, Case C-131/12, ¶ 77.  
115. Id.  
116. Id. ¶ 74. The importance of Articles 7 and 8 of the Charter was already underscored by the court in Digital Rights Ireland. See Dig. Rights Ir. Ltd., supra note 99, ¶ 37.  
117. See Google Spain, Case C-131/12, ¶ 80.  
118. Id. ¶ 81.  
119. Id.  
120. Id. (emphasis added).  
121. Id.  
122. Id. ¶ 88.
thus each controller has to comply with its own obligations.\textsuperscript{123} 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 CJEU noted that the web publisher might benefit from the exclusions granted by national law, pursuant to Article 9 of the Directive, for processing carried out solely for journalistic purposes, while “that does not appear to be so” in the case of the processing by a search engine.\textsuperscript{124} Moreover, the legitimate interests of the different controllers—the publisher and the search engine—could lead to a different balance regarding the legitimacy basis for the processing.\textsuperscript{125}

Finally, the CJEU 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.”\textsuperscript{126} 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.\textsuperscript{127}

The CJEU went on to repeat the principles it had previously stated—that under the Charter, the data subject does have a right that will take priority over any other legitimate interest; the only exception to this principle being a possible prevailing interest of the general public in particular circumstances.\textsuperscript{128} Against that backdrop, the CJEU held, in a situation such as the one at issue in the main proceedings:

[H]aving 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 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.\textsuperscript{129}

While 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

\textsuperscript{123} Id. ¶ 83.
\textsuperscript{124} Id. ¶ 85.
\textsuperscript{125} Id. ¶¶ 82–87.
\textsuperscript{126} Id. ¶ 89.
\textsuperscript{127} Id. ¶ 96.
\textsuperscript{128} Id. ¶ 97.
\textsuperscript{129} Id. ¶ 98 (emphasis added).
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 to be consigned to oblivion. It may seem that, for the
CJEU, unless there is 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
CJEU did require that the data subject’s requests meet some
threshold—namely, the conditions set forth either in Article 12(b) for
the right to erasure or in Article 14(a) for the right to object.130
Therefore, it must be either that: (1) the processing fails to comply
with some of the requisites laid down in the Directive, particularly
those related to the quality of the data requiring that the data be
“adequate, relevant and not excessive in relation to the purposes for
which they are collected and/or further processed,”131 or (2) the data
subject has some “compelling legitimate grounds relating to his
particular situation” that allows him or her to object to the
processing.132

C. Follow-Up by the National Court

After receiving the judgment from the CJEU, the referring
court, the AN, resumed the proceedings and handed down its final
ruling on the case on December 29, 2014.133 Under EU law, the
national referring court applies the interpretation criteria provided by
the CJEU to the facts of the particular case. Arguably, the CJEU thus
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.134

According to the AN, this was an initially lawful processing of
accurate personal data by Google; however, the lapse of time caused

130. See id. ¶ 88 (“[I]n so far as the conditions laid down by those provisions are in fact satisfied”). Admittedly, 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. ¶ 82.
131. See Data Protection Directive, supra note 23, art. 6(c).
132. See id. art. 14(a).
134. Id. at 27.
the data to become unnecessary with regard to the purposes of the processing. Remarkably, the AN expressly held that freedom of information was duly satisfied because the information was kept on the source and thus still findable through searches 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 this freedom is 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 “processing.” Indeed, the AN held that Google Spain SL was a data controller itself, along with Google Inc. This responsibility stems from the fact that both the subsidiary and its parent form a business unit, in which the subsidiary’s activity is essential to the business model of the parent company. 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. Additionally, holding otherwise would, according to the AN, prejudice the protection the Directive sought to ensure.

Finally, the AN accepted the appellants’ contention that the decision by the AEPD, the subject of the appeal, was too broad because 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 AEPD 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 relating to that person.” Hence, the AN affirmed the AEPD decision, but remarked that it

---

135. *Id.*
136. *Id.*
137. *Id.* at 21.
138. *Id.* at 17.
139. This ruling was appealed by Google Spain SL, particularly on account of the liability imposed on the subsidiary, and is currently pending before the Spanish Supreme Court.
140. *See* AEPD Costeja, *supra* note 74, at 23.
141. *See* AN follow-up judgment, *supra* note 133, at 27.
should be interpreted in this more limited sense of delisting links in search results.  

IV. A RIGHT ON SHAKY GROUND?

This Part discusses the legal basis of the CJEU’s holdings in Google Spain. As indicated in the previous Sections, the outcome of the ruling was premised on construing the Data Protection Directive provisions in light of the fundamental rights to privacy and personal data protection enshrined in the Charter. This Part argues that: (1) in the absence of specific safeguards, the conceptualization of search engines as controllers, even if mandated by the Directive, is problematic because search engines are unable to fulfill most of a controller’s legal obligations; (2) a search engine’s intermediary role should be recognized under the data protection legal framework; (3) the specific legal basis the CJEU uses to recognize the right to be delisted (i.e., the right to erasure and the right to object) presents some difficulties; (4) even though it is not expressly acknowledged by the Court, the ultimate driver of the ruling is the potential harm for the data subject; (5) the CJEU artificially built an apparently limited right through a creative rephrasing of the questions presented before it; and (6) the CJEU confined its balancing exercise to the criteria laid down in the Directive, disregarding the assessment of competing rights required by the Charter.

A. Search Engines as Data Controllers

Generalist search engines carry out two different types of activities that must be distinguished. On the one hand, they provide search services—they crawl the Internet to index publicly available information and respond to users’ search queries by displaying links to the most relevant content and perform the intermediary function of locating information on the Internet. Nonetheless, the ruling said nothing about whether the delisting 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.

143. This is not to say that search engines offer necessarily a purely neutral and objective view of the relevant information. 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 & Donald M. Falk, Google First Amendment Protection for Search Engine Search Results, 8 J.L. ECON. & POLY 883 (2012). Departing from both the conduit theory and the editor theory, a third view has been offered by James Grimmelmann considering search engines...
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 on the Internet but impossible for most users to find. On the other hand, search engines, in a related but clearly different function, establish a relationship with their users and collect personal information about them, which allows them to track both users’ search query histories and their surfing behaviors by following them across different services and platforms. A search engine may process that information to profile users to show them targeted advertising as well as to provide them with more personalized search results. With regard to the processing of users’ data, search engines 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 make available to users (content data). As the AG noted, the search engine is generally not aware of the nature of the indexed content and does not treat it as personal data. Furthermore, its activity simply does not comport with the role of a controller envisioned by the Data Protection Directive.

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 straightforward.\textsuperscript{149} 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.\textsuperscript{150}

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, that of the publisher and that of the search engine, are obviously related not only because the latter constitutes a further processing of the data already processed by the publisher, but also because the publisher will generally be aware that the information will be indexed and findable through search engines. In fact, the publisher will be able in many cases to prevent search engines from indexing its content by using the “robots.txt” protocol or other technical means.\textsuperscript{151} Should those two activities be considered a “set of operations” where both the publisher and the search engine pursue a jointly determined purpose, which would make them joint controllers?\textsuperscript{152}

In a 2008 opinion dealing specifically with search engines, the advisory body 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

\begin{footnotes}
\textsuperscript{149}. 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”].

\textsuperscript{150}. As the WP29 noted, “[i]n 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:

[T]he mere fact that different subjects cooperate in processing personal data, for example in 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.

\textit{Id.}

\textsuperscript{151}. For more information on the “robots.txt” exclusion protocol and html tags, see http://www.robotstxt.org/ [perma.cc/Y6NN-MKQC].

\textsuperscript{152}. See WP29 Opinion on the concepts of “controller” and “processor,” \textit{supra} note 149, at 20.
\end{footnotes}
controller with regard to the content related processing of personal data that is taking place.”

Rather, the WP29 held that the principal controllers of personal data in this case are the information providers. This conclusion 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 reasoning led the WP29 to assert that “[w]ith 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.” Apparently, the search engine’s obligations as controllers thus would be limited to that removal. Remarkably, nonetheless, the WP29 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.” Hence, the WP29 apparently assumed that even though search engines are to be considered controllers with

---

153. See WP29 Opinion on Search Engines, supra note 84, at 14 (emphasis added). “Principal controller” is not a notion defined in the Directive. Id.

154. 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 is 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.

155. See WP29 Opinion on Search Engines, supra note 84, at 14.

156. Id. This approach is arguably at odds with what the WP29 had determined in a previous opinion, holding:

[Es]pecially 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.

See WP29 Opinion on the concepts of “controller” and “processor”, supra note 149, at 22.

157. See WP29 Opinion on Search Engines, supra note 84, 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.
regard to those removals, their role as intermediaries might relieve them from such an obligation.

If the analysis by the WP29 was driven by the principle of proportionality, the same principle led the AG to reach a different conclusion: that, except in special circumstances, a search engine is not a controller. In the AG’s view, one can only be considered a controller if 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,”¹⁵⁸ which would not be the case with a search engine.¹⁵⁹

Against this backdrop, the conclusion by the CJEU that Google is indeed a controller is not that surprising. Although this interpretation has been criticized in the literature as a departure from the more careful approach taken by the WP29,¹⁶⁰ this advisory body had, in fact, also concluded that a search engine is a controller, albeit not the principal one and with only limited obligations, because even the removal of the data from its index and search results might depend on national tort law. However, there is a considerable difference—the CJEU treats the search engine as a separate controller whose processing is different from, and additional to, that of the publishers,¹⁶¹ which makes the search engine fully responsible for that processing, at least in theory.

It must be stressed that, according to the CJEU, the search engine is a data controller not only of the data displayed on the search results—the text of the link and the snippet below it—but also of the content data—the data included in the linked-to webpages. Indeed, the court held:

[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

---

¹⁵⁸. See AG Opinion, supra note 101, ¶ 82 (emphasis in the original).
¹⁵⁹. 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 in Google Spain. See AG Opinion, supra note 101, ¶ 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 processing personal data as such.
¹⁶¹. See Google Spain, Case C-131/12, ¶ 35.
the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d).\textsuperscript{162}

Thus, the question is not only about the text displayed on the results screen, but also about the information to which the search results link. Indeed, 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.”\textsuperscript{163}

However, characterizing a search engine as a controller of all personal data included in indexed web pages is arguably a far-reaching result. As noted, there is an initial problem—whether a search engine actually meets the definition of a controller when it is not specifically aware that the data it is processing are personal data.\textsuperscript{164} But even if this question is answered in the affirmative, another question arises as to whether this characterization can be seen as a proportionate outcome in view of the legal duties the Directive attaches to controllers. As already noted earlier, they are unable to comply with most of the obligations the Directive imposes on data controllers.\textsuperscript{165} 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 Article 8 of the Directive. Search engines would thus be subject to civil, administrative, and even criminal liability for unlawful processing.\textsuperscript{166} Ultimately, search engines’ activity would simply be incompatible with EU law.\textsuperscript{167}

\textsuperscript{162} Id. ¶ 41 (emphasis added).

\textsuperscript{163} Id. ¶ 82 (emphasis added).

\textsuperscript{164} This objection, already raised by the AG, has been stressed by some commentators. See, Sartor, supra note 160 (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 search engine,” where in fact the users who upload the content are those who choose to have that content indexed by search engines).

\textsuperscript{165} See, e.g., controllers’ obligations established in Article 6 of the Directive, regarding the “data quality” principles.

\textsuperscript{166} See Sartor, supra note 160.

\textsuperscript{167} AG Opinion, supra note 101, ¶ 90. This incompatibility had already been noted by the AN. See AN Reference Google Spain, supra note 67, at 11; see also Joris van Hoboken, Case note, CJEU 13 May 2014, C-131/12 (Google Spain) (2014), http://ssrn.com/abstract=2495580 [perma.cc/DG5K-CZPF], ¶ 9 (“Since the conclusion that all sensitive data would have to be
Maybe in an effort to mitigate the consequences of categorizing search engine as controllers, the CJEU appears to limit the obligations of a search engine as a 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 that would require disproportionate efforts, it does so only in particular areas, such as regarding the duty to inform data subjects and the need to notify third parties.

The CJEU apparently faced a difficult choice: either to consider the search engine a controller, which would enable the data subject to exercise her rights before the search engine, or to conclude that the search engine was not a controller, thereby leaving the data subject unprotected. For some authors, though, this dichotomy 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. Other commentators asserted that the court should not have considered them controllers; instead, the interests of both search engines and data subjects could be satisfactorily handled by resorting to the specific legal regime for intermediaries set out in another statute, the E-Commerce Directive, which will be considered below in subsection IV.B.1.


169. See Data Protection Directive, supra note 23, 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 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).

170. The CJEU noted, in fact, that concluding that the search engine is not a controller “would be contrary not only to the clear wording of [the definition of controller] but also to its objective—which is to ensure, through a broad definition of the concept of ‘controller,’ effective and complete protection of data subjects.” See Google Spain, Case C-131/12, ¶ 34.

171. See Hoboken, supra note 167, ¶ 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”).

In sum, the right to be delisted recognized by the CJEU ruling is arguably based on shaky ground, as it is ultimately premised on the search engine characterization as a data controller of content data in spite of the fact that a search engine’s activity regarding such data can hardly be reconciled with the obligations controllers face under the Directive. Thus, the CJEU failed to properly take into account the intermediary role played by generalist search engines in the digital information environment. However, 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.173 If the characterization of search engines as controllers is mandated by the EU data protection law, then there is arguably a problem with the law. Such a result is not uncommon in the sweeping data protection legal regime, whose broad approach that aims to afford data subjects the maximum level of protection may actually lead to inconsistent outcomes.

Data protection 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 search engines as controllers, because that classification entails a set of duties that, even if never enforced, are at odds with their intermediary nature.

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. Those questions will be briefly considered in the following Section.

B. Protecting Search Engines’ Intermediary Role

1. Intermediary Liability Safe Harbors

EU law has established 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 was set forth in Articles 12 through 15 of the 2000 E-Commerce Directive,174 a set of rules that was inspired, to a large extent, by the 1998 US Digital Millennium Copyright Act (DMCA).175 Both statutes present,

nonetheless, significant differences, such as how the DMCA deals exclusively with infringements of copyright, and the E-Commerce Directive’s safe harbors apply horizontally to any kind of unlawful content.176

Another key difference is that, unlike the DMCA,177 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 into national law.178 In addition, some national courts have wrangled with the absence of such a safe harbor, eventually concluding that the hosting exemption might be enough to cover the operation of a search engine.179

But even if the hosting safe harbor is to be considered broad enough to accommodate search engines’ activity, the applicability of the safe harbors to situations where the third-party content may violate data protection rights remains unclear. This situation arises because, in spite of the horizontal approach of the E-Commerce Directive, Article 1(5)(b) of this Directive excludes from the Directive’s scope “questions relating to information society services covered by


179. See e.g., Saif v. Google, Cour d’Appel de Paris, Pôle 5, Chambre 1, Judgment of Jan. 26 2011, http://juriscom.net/wp-content/documents/caparis20110126.pdf [perma.cc/68BE-QXAF] (holding that Google’s image search engine is a neutral intermediary that may benefit from the liability exemptions). See also the German Supreme Court’s Vorschaubilder case, BGH, I ZR 69/08, Apr. 29, 2010, ¶ 39, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2010&Sort=3&nr=51777&pos=1&anz=94 [perma.cc/XZ3D-NRUZ] (stating, though only in dicta, that Google Images would benefit from the hosting safe harbor). 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 for the content it linked to. 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).
[Data Protection Directives].” The interpretation of this provision is not straightforward, though. 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 Directive’s horizontal approach—that an intermediary would carry out the same technical activity regardless of the kind of content involved—and thus the rules should also be the same. Excluding personal data from the safe harbors’ protection would also go against the principle established in Article 15(1) of the E-Commerce Directive that Member States cannot impose a general obligation on intermediaries “to monitor the information which they transmit or store” or “a general obligation actively to seek facts or circumstances indicating illegal activity.” Therefore, a reading of Article 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 when it comes to content including personal data.

Apparently recognizing the need to keep the safe harbors available in data protection issues, the General Data Protection Regulation expressly declares that the GDPR 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...”

180. See E-Commerce Directive, supra note 172, 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.”

181. 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.”).

182. See E-Commerce Directive, supra note 172, art. 15(1). For a provision parallel to that, see § 512(m) of the DMCA. 17 U.S.C. § 512(m) (2012).

183. In the Vividown case, the Italian Supreme Court held that Article 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), http://www.dirittoegiustizia.it/allegati/15/0000063913/Corte_di_Cassazione_sez_III_Penale_sentenza_n_5107_14_depositata_il_3_febbraio.html [perma.cc/3V2R-MD42]. Along the same lines, see Sartor, supra note 160, at 574 (“[T]his 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.”).
of that Directive." However, this may not be enough to protect search engines from liability. First, it is not clear whether the search activity is covered by the E-Commerce safe harbors in the first place. Second, even if linking is covered by the safe harbors, characterizing search engines as controllers might imply that they are not neutral and passive enough to be eligible for the safe harbors’ protection.

Greater legal certainty would be desirable in this regard, which could perhaps 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

The Data Protection Directive does not specifically leave out search engines from the notion of what a controller is. However, it does so with another kind of Internet intermediaries—Internet service providers (ISPs) that provide transmission services. The Directive makes it clear that when ISPs 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.” This exclusion of transmission service providers from the “controller” categorization appears to rest on the ISP’s purely intermediary role as a passive conduit. In spite of all the differences

---

184. See GDPR final draft, supra note 7, Art. 2(3) and Recital 17.
185. 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 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).
186. See CJEU, Joined Cases C-236/08 to C-238/08, Google France SARL, Google Inc. v. Louis Vuitton Malletier SA et al. (March 23, 2010), ¶ 114 (holding that to be eligible for the hosting safe harbor, the role played by the intermediary must be “neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores”).
187. See Data Protection Directive, supra note 23, Recital 47 (“[W]here 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 101, ¶ 87.
between the relevant Internet intermediaries, a similar rationale could arguably be used for search engines; they serve the 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.  

The legal framework surrounding data protection should evolve 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 subjects may experience as a consequence of the widespread dissemination of search results that point to information that includes an individual’s personal data, particularly 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, to overcome that decision’s shortcomings and wide range of potentially unintended consequences.

C. The Legal Basis for Having the Links Delisted

1. Overlapping Rights

The CJEU found that Mr. Costeja established a right that the information he complained of should no longer be linked to his name by means of the search results list, but it did not determine which precise legal basis under the Data Protection Directive would allow him to require such delisting—i.e., the right to erasure in Article 12(b) or the right to object in Article 14(a). Indeed, the CJEU held that in a case such as the one brought before it, the data subject could “require those links to be removed from the list of results” by virtue of both the right to erasure and the right to object.

---

188. 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 [perma.cc/545V-ZNMA] (suggesting that data protection law distinguishes “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”).

189. See Google Spain, Case C-131/12, ¶ 98.

190. Id.
In principle though, those rights are mutually exclusive. The former right covers data processing that does not fulfill, or no longer fulfills, the Directive provisions and is thus unlawful.\textsuperscript{191} The latter right 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.”\textsuperscript{192} Therefore, either one right or the other—or none—should apply in a specific case. The CJEU, however, conflated both rights in its judgment, maybe to cover other cases with slightly different circumstances. But since the CJEU held that Mr. Costeja “establishe[d]” 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. The right of erasure and the right to object actually overlap significantly, and they are, in a way, caught in a circular rationale. Indeed, when a data subject has compelling grounds to object under Article 14(a) of the Data Protection Directive to an otherwise lawful processing, the conclusion should probably be reached that under Article 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 legitimate grounds for the processing under Article 7(f).\textsuperscript{193} In turn, the lack of a such grounds—the consent of the individual being absent—would make the processing non-compliant with the Directive provisions, allowing the data subject to exercise the right to erasure under Article 12(b). In a similar vein, if the data subject has “compelling legitimate grounds” relating to her particular situation to object to the processing under Article 14(a), this might indicate that the data are in fact inadequate, irrelevant, or excessive in relation to the purposes of the processing. This situation would then entail lack of compliance with Article 6(1)(c) and, again, would allow the data subject to exercise the right to erasure under Article 12(b).

\textsuperscript{191} See Data Protection Directive, supra note 23, art. 12(b).
\textsuperscript{192} Id. art. 14(a).
\textsuperscript{193} See Data Protection Directive, supra note 23, art. 7(f); see also Herke Kranenborg, Case Note: Google and the Right to be Forgotten, 1 EUR. DATA PROTECTION L. (2015) (noting that the CJEU apparently absorbed the criterion of having “compelling grounds” to object in the balance of interests required in Article 7(f), and that “[i]t thereby relinquished 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”).
2. Is it the Search Engine’s or the Publisher’s Processing?

The CJEU found that the individual has the right to have the links delisted when the data are “inadequate, irrelevant or no longer relevant, or excessive.”\textsuperscript{194} Those adjectives have prompted criticism against what has been considered too vague a standard, unable to meet any reasonable threshold for suppressing speech on the Internet.\textsuperscript{195} Whatever the merits of these critiques, it must be noted that those words are actually taken from Article 6(1)(c) of the Directive.\textsuperscript{196} Those words do not refer to the fact that the individual may simply consider the data to be inadequate, irrelevant, or excessive \textit{in general} or \textit{according to his or her preferences}. Rather, the inadequateness, irrelevancy, or excessiveness is to be assessed, as the CJEU notes, “in relation to the purposes of the processing at issue carried out by the operator of the search engine.”\textsuperscript{197}

This legal standard, set forth in the Directive, is thus meant to be an objective one, rather than subjective. The question is then what are the “purposes” of the processing carried out by the search engine. While these purposes were not made explicit in the judgment, it may be safe to assume that they consist of making easily findable information publicly available on the Internet by displaying results relevant to users’ search queries.\textsuperscript{198} If this is so, an argument could be made that displaying links to information that is publicly available on the Internet 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—it is not inadequate, irrelevant, or excessive \textit{with regard to those purposes}.\textsuperscript{199}

In particular, the mere fact that the information was originally published many years ago does not seem to contradict the search engine’s purpose of making the information that \textit{currently} exists on

\textsuperscript{194}. See Google Spain, Case C-131/12, ¶ 94.

\textsuperscript{195}. See, e.g., Andrew McLaughlin’s opening statement at the Intelligence Squared US debate, supra, note 1; see also Washington Post’s Editorial Board, UnGoogled: The Disastrous Results of the ‘Right to be Forgotten’ Ruling, WASH. POST (July 12, 2014).

\textsuperscript{196}. See Data Protection Directive, supra note 23, art. 6(1)(c) (“[P]ersonal data must be . . . (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.”).

\textsuperscript{197}. See Google Spain, Case C-131/12, ¶ 94 (emphasis added).

\textsuperscript{198}. See Grimmelmann, supra note 143 (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{199}. See Anna Bunn, The Curious Case of the Right to be Forgotten, 31 COMPUTER L. & SECURITY REV., 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”).
the Internet available through search results. 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. But then the one failing to comply with the data quality principle would be the publisher, not the search engine, and 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.”

In any event, this Article submits that what is ultimately determinative for the CJEU’s recognition of a right to be delisted is not the fact that the data may be inadequate, irrelevant, or excessive for the purposes of the processing, as required by the Directive—in this case the search engine’s processing—but 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. Likewise, the CJEU’s decision to focus only on the scenario where the search is made on the basis of the data subject’s name and

---

200. *Id.* at 343; see also the AG Opinion, supra note 101, ¶ 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.”).

201. The Guidelines published by the WP29 on the application of *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. Such an assessment will be dependent on the purpose of the original processing.” See Art. 29 Working Party, Guidelines on the implementation of the Court of Justice of the European Union judgment on “Google Spain and Inco 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).

202. See *Google Spain*, Case C-131/12, ¶ 94 (emphasis added).

203. The WP29 Guidelines note that “[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 201, ¶ 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.*, ¶ 19.
requiring only the delisting of the results—a move that will be examined in the next subsection—appears to respond to the same idea. Should the real concern be that the data are inadequate, irrelevant, or excessive for the purposes of the search engine’s processing, the CJEU arguably could have also required the complete deletion of the data from the search engine’s index; however, 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 CJEU’s holding, even though the CJEU held that prejudice to the data subject is not required.

3. A Creative Surgical Approach Taken by the CJEU

As noted earlier, the CJEU confined the discussion to searches made by the name of individuals and asserted only a right to delist the link—as opposed to a right to remove the information from the search engine’s index altogether. This surgical approach was a creative move by the CJEU. When discussing the extent of the obligations of a search engine 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, the AN. Such rephrasing allowed the CJEU to sidestep the question of whether a data subject has a right to have the data removed from the search engine’s index and to 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 AN had posed to the CJEU the question of whether, to protect the data subject’s rights to erasure and to objection, 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.”

204. See Google Spain, Case C-131/12, ¶ 91; see also David Lindsay, The ‘Right to be Forgotten’ by Search Engines under Data Privacy Law: A Legal Analysis of the Costeja Ruling, 6 J. of Media L. 159, 178 (2014) (“[T]he 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.”).

205. See Google Spain, Case C-131/12, ¶ 96. The “potential serious interference” could perhaps be better related to the general requirement in Article 6(1)(a) that the data must be processed “fairly.” It might also count as an element to override the “legitimate interest” as a basis for the processing under Article 7(f), or as “compelling grounds” on which to object to the processing under Article 14(a).

206. Id. ¶ 20, Question 2(c) (emphasis added); see also AN Reference Google Spain, supra note 67, at 17.
In the event that the answer to that question was affirmative, the AN asked 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.”

Purporting to report those questions, the CJEU actually rephrased them by stating:

[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.]

By rephrasing the questions actually posed by the AN in this way, the CJEU was, in fact, determining beforehand—without a proper discussion—the boundaries of the right it was prepared to recognize. The CJEU answered that self-posed question in the affirmative, thus asserting that in order to comply with the data subject’s rights, a search engine must remove the relevant links from a list of results produced by a search for the data subject’s name—something notably different than removing the information from its index altogether, which was what the AN had asked the CJEU to determine. Whether or not a data subject might also ask for a complete removal from the search engine’s index remained unanswered by the CJEU. The discussion in the judgment did not provide any justification 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. The AN had posed the question of whether the data subject may request search engines “to prevent indexing of the information relating to him personally, published on third parties’ web pages.”

The CJEU changed that wording, as if the AN had asked whether the 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.” This alteration again allowed the court to acknowledge a narrowly tailored right.

207. See Google Spain, Case C-131/12, ¶ 20, Question 2(c).
208. Id. ¶ 62.
209. Id. ¶ 20 (Question 3) (emphasis added); see also AN Reference Google Spain, supra note 67, at 17.
210. See Google Spain, Case C-131/12, ¶ 89.
D. The Balancing of Rights

The right to data protection does not exist 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 mentioned in the Directive. 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 Charter, such as the freedom of expression and information (Article 11) and the freedom to conduct business (Article 16). Specific criteria for determining whether a limitation to the rights provided by the Charter is acceptable are established in Article 52. In addition, this provision expressly provides that insofar as the Charter contains rights that correspond to rights guaranteed by the European Convention on Human Rights (ECHR), they will have the same meaning and scope as those in the ECHR.

The way the CJEU approached the balancing of rights has been the focus of much of the criticism against the Google Spain judgment. Indeed, a number of shortcomings may be identified in how the court tackled the question. On the one hand, the CJEU only considered the rules contained in the Data Protection Directive, particularly that of Article 7(f), and failed to carry out the balancing required by Article 52(1) of the Charter. On the other hand, even the analysis carried out under the Directive’s provisions is far from satisfactory—as will be discussed later.

211. See Charter, supra note 18, art. 52(1).
212. See id. art. 52(3).

The court explicitly assumed that the data processing carried out by the search engine may find a legitimate basis under Article 7(f).\textsuperscript{214} 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).\textsuperscript{215}

Thus, Article 7(f) considers on the one hand the “legitimate interest” of the controller—according to the court in this case, the search engine—and those of the third party or parties to whom the data are disclosed—which in this case are 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 protection. Therefore, a balancing analysis is needed under this provision.\textsuperscript{216} Actually, all of the balancing the Google Spain court engaged in came down to this particular provision.

The court started this analysis by considering how the processing carried out by the search engine is liable to interfere seriously with a data subject’s rights when a search is made on the basis of an individual’s name.\textsuperscript{217} Then the court stated, “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{218} As a result, the first element of the balancing envisioned in Article 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 Article 7(f) was whether the processing could be grounded on the legitimate interest pursued by those to whom the data are disclosed—that is, by the 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...

\begin{footnotesize}
\begin{enumerate}
\item See Google Spain, Case C-131/12, ¶ 73.\textsuperscript{214}
\item See Data Protection Directive, supra note 23, art. 7(f). Article 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.”\textsuperscript{215}
\item See Google Spain, Case C-131/12, ¶ 74.\textsuperscript{216}
\item Id. ¶ 80.\textsuperscript{217}
\item Id. ¶ 81 (emphasis added).\textsuperscript{218}
\end{enumerate}
\end{footnotesize}
Charter,” 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.” This “general rule” notwithstanding, the court held:

This analysis is the entirety of the balancing exercise advanced by the CJEU. The ruling did mention that a balancing is also needed under Article 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.” However, the CJEU never elaborated on that point, nor gave any clue as to how that balancing should be carried out.

Confining the balancing analysis to the elements set forth in Article 7(f) could hardly result in a satisfactory outcome. For one thing, that provision does not consider the interests of the publisher. Moreover, the language of Article 7(f) led the CJEU to depict the balance as one between the data subject’s fundamental rights and the “legitimate interests of internet users potentially interested in having access to that information.” In addition, the controller’s interest was considered to be of a mere economic nature. Such a starting point allowed the CJEU to perceive the “interests” of either the controller or the users as something less valuable than the data subject’s fundamental rights. This outcome shows that such a

219. Id. (emphasis added).
220. Id. (emphasis added).
221. Id.
222. Id. ¶ 76.
223. Id.
224. See Kranenborg, supra note 193, at 78 (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)).
225. See Google Spain, Case C-131/12, ¶ 81 (emphasis added).
226. Id. ¶¶ 81, 97; see Lindsay, supra note 204, 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”).
227. See Frantziou, supra note 213, at 769 ("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 213, at 13.
balancing, if it can be understood as such,\textsuperscript{228} is not enough to achieve a result consistent with the Charter. In fact, if the result of Article 7(f) analysis would favor the data subject, she would have a right to stop the data processing under the Directive. However, that right should still be confronted with other fundamental rights at stake—not merely interests.

Still, under the Directive provisions, the CJEU noted that the balancing under Article 7(f) could lead to a different outcome in the case of data processing carried out by the publisher and notably stated that, while the publisher’s processing might be covered by national law exceptions under Article 9 (for processing carried out solely for journalistic purposes), this “does not appear to be so” in the case of a search engine.\textsuperscript{229} The court’s understanding of Article 9 in \textit{Google Spain} thus departed from the broader interpretation it had held in a previous judgment—the \textit{Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy} case.\textsuperscript{230} 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 transmit them” and that “[t]hey are not limited to media undertakings and may be undertaken for profit-making purposes.”\textsuperscript{231}


The fundamental rights which may be affected 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 Articles 7 and 8 of the Charter—are those of freedom of expression and information as well as freedom to conduct business (enshrined in Articles 11 and 16 of the Charter, respectively). Article 52(1) of the Charter prescribes:

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.\textsuperscript{232}

\begin{flushleft}
\textsuperscript{228} See Frantziou, \textit{supra} note 213, at 769 (noting that “seeking to balance rights against interests is questionable as a matter of principle”).
\textsuperscript{229} See \textit{Google Spain}, Case C-131/12, ¶ 85.
\textsuperscript{231} See id., ¶ 61.
\textsuperscript{232} See Charter, \textit{supra} note 18, art. 52(1).
\end{flushleft}
As noted, the CJEU neither engaged in weighing whether those rights might in fact be limited by the right to be delisted nor whether such a limitation would meet the criteria set forth in Article 52(1). The search engine's fundamental right of freedom to conduct business was not even mentioned in the judgment, which only considered the economic “interests” of the search engine under the balancing required by Article 7(f). There, the CJEU established what 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 own approach in ASNEF and FECEMD. 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 Article 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” 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. A fair analysis, however, 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 may also be exercising that right when displaying the search results. It is commonly argued that Google Spain does not really affect freedom of expression.

233. 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 101, ¶ 132.
234. See Google Spain, Case C-131/12, ¶ 81.
235. Id.
236. ASNEF and FECEMD, supra note 54, ¶ 47.
237. See id., ¶ 47; Steve Peers, The CJEU’s Google Spain Judgment, EU LAW ANALYSIS (May 13, 2014), [perma.cc/A6PK-JYUT] (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”).
238. See Erdos, supra note 49 (“[T]he CJEU also 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 van Hoboken, supra note 167, at 1; Orla Lynskey, Rising Like a Phoenix: The ‘Right to be Forgotten’ Before the ECJ, EUR. L. BLOG (May 13, 2014), http://europeanlawblog.eu/?p=2351 [perma.cc/N3CC-AP65]; Peers, supra note 237. For more 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).
expression, because, after delisting, the content is still available on the original source.\textsuperscript{239} However, the obscurity that stems from delisting search engine’s links to the information does affect freedom of expression, at least to some extent. And, in any event, permanence in the origin website is not 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 might 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—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 Article 11 of the Charter, the right to freedom of expression and information “shall include freedom . . . to receive . . . information and ideas without interference by public authority and regardless of frontiers.”\textsuperscript{240} As noted earlier, this fundamental right was dealt with as a mere “interest,” which the CJEU held would be overridden, as a rule, by the data subject’s rights.\textsuperscript{241}

Finally, no mention was made in the ruling regarding the need to take into account European Court of Human Rights (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 Article 52(3) of the Charter.\textsuperscript{242} This is particularly relevant, as the ECtHR has already repeatedly dealt with the interplay between the rights to freedom of expression and to privacy (Articles 10 and 8 of the ECHR, respectively) and held that both deserve equal respect as a matter of principle.\textsuperscript{243}


\textsuperscript{240} See Charter, supra note 18, art. 11, which uses the same language as Article 10 of the ECHR. The European Court of Human Rights (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), ¶¶ 50–55.

\textsuperscript{241} See Google Spain, Case C-131/12, ¶ 97; see also Bunn, supra note 199, 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 & Heywood, supra note 213, at 578 (“The 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.”).

\textsuperscript{242} See Kulk & Borgesius, supra note 213; see also Frantzio, supra note 213, at 773.

\textsuperscript{243} 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), ¶ 65,
V. 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, is expected to be finally adopted in 2016, and would enter into force in 2018.244 The GDPR does not substantially change the basic concepts that allowed the CJEU to find a right to be delisted from search engine results under the Directive. The notions of “processing” and of “controller” remain essentially unchanged to that effect.245 In addition, Article 7(f) of the Directive, under which the balancing was carried out in Google Spain, will be replaced by an almost identical provision—Article 6(1)(f) of the GDPR.246

However, the GDPR does include a specific provision that in the final draft is titled “Right to erasure (‘right to be forgotten’)”247 and that has been the subject of much academic commentary since it was originally proposed.248 Nonetheless, the provision does not deal specifically with search engines. It also does not establish with particularity a data subject’s right to request the delisting of links displayed in search engines’ results for name-specific queries—in short, it does not codify Google Spain. Rather, the GDPR sets forth a general right to erasure, imposing on the controller the obligation to

http://hudoc.echr.coe.int/eng?i=001-122365 [perma.cc/HPU8-QD6D]; see Frantziou, supra note 213, at 774 (noting that while Google Spain “is not necessarily incompatible with the ECHR, the Strasbourg Court’s judgment in Węgrzymowski and Smolczewski suggests that such incompatibility cannot be ruled out either”).

244. See GDPR final draft, supra note 7.

245. Id. arts. 4(3), 4(5).

246. The proposed Article 6(1)(f) GDPR introduces a specific consideration to the case where the data subject is a child. On the other hand, that provision 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(1)(f) (emphasis added).

247. Id. art. 17; 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 choice of this title for the proposed article).

erase the data in a number of cases, which—to a large extent—were, at least implicitly, already considered under the Directive. For example, the right to erasure will apply to cases where the data are no longer necessary in relation to the purposes of the processing; where the data subject appropriately objects to the processing or withdraws consent and there is no other legal ground for the processing; or where the data have been unlawfully processed.249 The main novelty—which supposedly would warrant the language “right to be forgotten” in the title of the Article—is a further obligation of the controller. According to Article 17(2a):

Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the data, that the data subject has requested the erasure by such controllers of any links to, or copy or replication of that personal data.250

The GDPR does not contain a provision dealing with the intermediary role of search engines; nor does it address the Google Spain ruling’s shortcomings identified above. Nonetheless, the GDPR might offer a better opportunity to include freedom of expression and information into the analysis. First, remarkably, the provision on the right to be forgotten, Article 17, states explicitly that the controller’s obligation shall not apply to the extent that data processing is necessary “for exercising the right of freedom of expression and information.”251 Second, the language of the provision equivalent to the Directive’s “media exception,” Article 80, appears to broaden its scope. The exception, which must be established by EU Member States, aims more generally to reconcile data protection rights with “the right to freedom of expression and information, including the processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression.”252

B. Practical Fixes

In the absence of a more general solution, the only practical way to bypass some of the shortcomings identified in the Google Spain judgment seems to be a careful application by national courts and DPAs that takes into account all of the rights at stake. The characterization of search engines as controllers with regards to content data, even if inconsistent with the role of an intermediary,

249. See GDPR final draft, supra note 7, art. 17.
250. Id. art. 17(2a).
251. Id. art. 17(3)(a).
252. Id. art. 80(1) (emphasis added).
cannot be avoided unless the CJEU changes its approach. Nonetheless, national courts and DPAs can use their discretion in applying the CJEU’s interpretation criteria to particular cases, thus using the little room the CJEU actually conceded (for instance: “as a rule” does not mean “always”) and can resort to the Charter’s provisions.

As the CJEU noted in *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.”253 It also stated, “In that context, fundamental rights have a particular importance,” noting that freedom of expression had to be weighed against the protection of private life in the specific case before it. 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 rights protected by the Community legal order or with the other general principles of Community law, such as inter alia the principle of proportionality.254

In applying the right to be delisted to particular cases, national courts and DPAs should carry out a careful balancing, both within the Directive—or the GDPR when it enters into force—and under the criteria established in the EU 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 Charter 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 engines—only a fraction of the search engines’ decisions against delisting are likely to be appealed before courts or DPAs. This trend 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.255 Such a question, though, can only be properly addressed with legislative intervention.256

---

254. *Id.* ¶ 87.
255. *See* Lindsay, *supra* note 204, at 178.
256. *See* Alessandro Mantelero, *Finding a Solution to the Google’s Dilemma on the 'Right to Be Forgotten', After the 'Political’ ECJ Decision*, ICT LAW AND DATA PROTECTION (Nov. 19, 2014), http://ssrn.com/abstract=2525565 [perma.cc/EB87-RQEY] (proposing that the GDPR include a provision excluding the direct enforcement by search engines and requiring filing a complaint before a court or a DPA, with an initial temporary delisting of the challenged links conditioned to the filing of the complaint).
VI. 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 implicating personal information about them. The CJEU tackled this issue resorting to data protection law and held 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 from a search carried out on the basis of her name.

The CJEU 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 available through the use of different search terms. However, the conditions to exercise this right—for instance, that the content is inadequate, irrelevant, or no longer relevant—are overly vague. Moreover, the right is neither limited to 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 CJEU resorted—data protection law. EU data protection law is a very powerful instrument that needs some counterbalances to avoid certain far-reaching results that its all-embracing scope may enable. The court arguably failed to devise appropriate criteria to balance data protection with competing rights recognized by the Charter, particularly that of freedom of expression and information.

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 soundness 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 to be delisted.

In addition to the drawbacks deriving from both 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 constraints imposed by the legal framework on which the right to be delisted is grounded. Indeed, such framework does not allow for the recognition of the intermediary role played by generalist search engines. In order to impose on search engines the duty to assess individuals’ requests and to accommodate them when justified, the CJEU needs to consider search engines as data controllers of the personal data included in the indexed websites. Nonetheless, such a characterization is arguably at odds with search engines’ intermediary role and 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 under data protection law and under the general scheme of liability limitation set forth in the E-Commerce Directive. Only then might a “right to be delisted,” with all the necessary limitations and due account of the competing rights, be established on solid ground.