Certain aspects of the CJEU's Google Spain judgment relative to lawfulness of data processing and liability of internet search engine operators

Kunda, Ivana

Regulating Smart Cities

Actas del 11º Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona, 2-3 de julio de 2015

Regulating Smart Cities

Proceedings of the 11th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya, Barcelona, 2-3 July, 2015

2015

UOC Universitat Oberta de Catalunya | 20 anys

HUYGENS EDITORIAL

REGULATING SMART CITIES

COORDINADORES

Balcells Padullés, J., Delgado García, A.M., Fiori, M., Marsan Raventós, C., Peña-López, I., Pifarré de Moner, M.J. & Vilasau Solana, M.

© 2015, Huygens Editorial
La Costa, 44-46, át. 1ª
08023 Barcelona
www.huygens.es

ISBN: 978-84-606-9621-6
Editado en España

CERTAIN ASPECTS OF THE CJEU'S *GOOGLE SPAIN* JUDGMENT RELATIVE TO LAWFULNESS OF DATA PROCESSING AND LIABILITY OF INTERNET SEARCH ENGINE OPERATORS

Ivana Kunda
Head of the International and European Private Law Department, University of Rijeka

Darja Lončar Dušanović[1]
Croatian Telecom Inc.

ABSTRACT: The judgment of the Court of Justice of the European Union in the case C-131/12 *Google v AEPD and Gonzalez* of May 2014 is important for several reasons. Not only because it prompts the right to be forgotten and liability of Internet search engine operators for content published by third parties, but also because it subjects Internet search engine operators to data protection legislation. These operators are characterised as data controllers, their activities as data processing activities, within the meaning of the Data Protection Directive 95/46/EC, while a number of issues related to applicability of Article 7(f) thereof remain unsettled. Besides departing from the Advocate General's opinion in this case, these aspects of the judgment provoked controversy in scientific and professional circles. In this paper, authors examine reasons offered by the CJEU, in particular related to the abovementioned features of the ruling. Besides, authors focus on some other issues which seem to be insufficiently addressed in the judgment, such as the liability of Internet search engine operators and the implications on the legal scheme for Internet service providers under the E-Commerce Directive 2000/31/EC. The proposition is put forward that the CJEU judgment errs in finding legal ground for Internet search engine operators' activities in Article 7(f), due to inherent lack of possibility of Internet search engine operators to conduct ex ante balancing test. As a result, the CJEU's finding about Internet search engine operators as data controllers is called into question. Inconsistencies may also be found in attempting to establish their liability, which is equally tied to the awareness of and control over the data. Therefore, more convergence is recommended with the scheme under the E-Commerce Directive.

KEYWORDS: Data controller, data processing, legitimate interest, balancing test, right to be forgotten, liability of Internet search engine operator, liability of Internet service provider.

1 The views expressed in this paper are the author's own and do not necessarily present the view of Croatian Telecom.

1. INTRODUCTION

In May 2014, the Court of Justice of the European Union passed a judgment in the case of *Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez* (further in the text: *Google Spain*)[2]. This judgment, which has already been named as landmark or historic, is important for several reasons, all of which can be summarized as subjecting Internet search engine operators to data protection regulation for the first time in EU law. Prior to the judgment, Internet search engine operators, in performing their core activities, were understood as mere intermediaries between web publishers and Internet users.

Newly established legal position of Internet search engine operators within the data protection framework resulted in many questions, posed by both professionals and academics. Pondering upon the effects of this judgment, one has to consider its direct and indirect implications on legal certainty in the context of personal data processing. The following chapters concentrate on several aspects of the judgment, attempting to provide a fresh look into the issues related to applicability of the balancing test to Internet search engine operators and their liability under the Data Protection Directive.

2. DATA PROCESSING BY SEARCH ENGINE OPERATORS

The main paradigm of personal data protection is that any personal data processing which is not explicitly permitted is prohibited and not *vice versa*. Therefore, it is crucial to clearly determine legal grounds which allow collecting and further processing of personal data, in particular in digital and on-line environment, due to increasing volume and potentials of data processing[3]. Even more, clear identification of legal grounds for collecting and further processing of personal data is the starting point for defining the manners and scope of data processing and eventually for effective data protection. Lack of clearly set legal grounds for personal data processing essentially undermines a grasp of personal data protection in general, even if other requirements, such as data processing principles, are fulfilled. Therefore, vagueness and inconsistency related to these issues, both on EU and national levels, would be highly undesirable. Unfortunately, it seems the proposal of the new data protection framework on the EU level, i.e. the Proposal on

2 Judgment in *Google Spain SL and Google Inc.*, 13.5.2014, ECLI: ECLI:EU:C:2014:317.

3 «The principles of data protection are the foundation on which the right to our personal data is built. If the principles are weak, than the entire structure will be weak and unreliable.» (2015). Data Protection Broken Badly. EDRi/Access/Panoptykon Foundation/Privacy International. Retrieved March 16th, 2015 from https://edri.org/files/DP_BrokenBadly.pdf, at 3.

General Data Protection Regulation[4] (further in the text: GDPR) which has entered the legislative procedure[5] and is expected to be adopted by the end of 2015, as well as the CJEU judgment in *Google Spain*, do not contribute to solving this problem.

2.1. Legal grounds for lawful data processing

Article 7 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (further in the text: the Data Protection Directive)[6] sets legal grounds for lawful personal data processing, i.e. criteria for making data processing legitimate, as the Directive terms them[7]. These grounds are «exhaustive and restrictive […] cases in which the processing of personal data can be regarded as being lawful.»[8] The *numerus clausus* principle, governing legal grounds and their restrictive scopes, aims at protecting fundamental rights and freedoms of data subjects against business and other interests of data controllers. For data processing to be lawful, at least one

4 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) /* COM/2012/011 final - 2012/0011 (COD) */, retrieved on March 12th, 2015 from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012PC0011.

5 See European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), retrieved on May 10th, 2015 from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN (further in the text: EP legislative resolution on the GDPR).

6 OJ L 281, 23.11.1995, 31-50.

7 These legal grounds are: a) the data subject has unambiguously given his consent; b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; c) processing is necessary for compliance with a legal obligation to which the controller is subject; d) processing is necessary in order to protect the vital interests of the data subject; e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; and f) 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).

8 Judgement in *ASNEF and FECEMD*, C-468/10 and C-469/10, ECLI:EU:C:2011:777, paragraph 30.

of the criteria referred to in Article 7 has to be fulfilled[9]. This is further reaffirmed by the additional rights vested in data subjects under Articles 12 and 14 of the Data Protection Directive, enabling them to control processing of their personal data[10].

2.2. Interpreting Article 7(f)

One of the legal grounds, set under Article 7(f), recognises the legitimate interest of the controller or third party. In *Google Spain*, the CJEU concluded that data processing by Internet search engine operators is capable of being covered by Article 7(f)[11]. Because questions, referred to by the Spanish court to the CJEU for a preliminary ruling, did not necessitate examining the lawfulness of the legal ground for data processing under Article 7(f), the CJEU did not elaborate further on this issue[12]. Therefore, following the judgment in *Google Spain*, question remains as to reasons which might support the CJEU's assertion that the activities of search engine operators performed on personal data, consisting of finding information published or placed on the Internet by third parties, indexing them automatically, storing them temporarily and making them available to Internet users (further in the text: personal data processing by search engine operators), are capable of being covered by the provision of Article 7(f). To find answer to this question the paper looks more closely into the functioning of this provision.

Based on Article 7(f), threshold for lawful data processing is that such «processing is necessary for the purposes of the legitimate interests pursued by the controller or by 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)». With the aim of determining if the processing is lawful under Article 7(f), it is necessary to fulfil a threefold requirement: 1) the data controller (or third party) has to have a legitimate interest; 2) the processing must be necessary to satisfy that interest, and 3) the interests of the data controller (or third party) has to prevail over the interests for protecting fundamental rights of the data subjects[13]. The last two requirements

9 In addition to the legal grounds under Article 7 of the Data Protection Directive, the principles relating to data quality stated in Article 6 of the same Directive must also be fulfilled in order for data processing to be legitimate. Judgment in *Österreichischer Rundfunk and Others* EU:C:2003:294, paragraph 65; Judgment in *ASNEF and FECEMD*, ECLI:EU:C:2011:777, paragraph 26; Judgment in *Worten*, EU:C:2013:355, C342/12, paragraph 33.

10 See *infra* 2.2.2. *in fine*.

11 Judgment in *Google Spain SL and Google Inc.*, ECLI: ECLI:EU:C:2014:317, paragraph 73.

12 Rather, the CJEU focused on Article 12(b) and Article 14(a), as the questions to the CJEU for a preliminary ruling referred *inter alia* to applicability of these rights. See *infra* 2.2.2.b).

13 The CJEU has split this provision to two cumulative requirements in the Judgement in *ASNEF and FECEMD*, ECLI:EU:C:2011:777, paragraph 38, but essentially they are the same as the

are joined in a specific balancing test between the legitimate interests of the controller or third party to whom the data are disclosed on one hand, and the interests for fundamental rights and freedoms of the data subject (which enjoy protection under Article 1(1) of the Data Protection Directive[14]) on the other. This balancing test is essential and probably the most complex issue in determining whether the legal ground referred to in Article 7(f) is met or not. While all legal grounds listed in Article 7 of the Data Protection Directive require a less flexible necessity test,[15] the legal ground under paragraph (f) is the only one involving the balancing test. Thus, it is *a priori* more problematic than other legal grounds when it comes to its application *in casu*.

According to studies conducted by the European Commission, there is a lack of harmonized interpretation of the Article 7(f) in the Member States. Approaches vary, from seeing Article 7(f) as the last resort for data processing when no other legal ground can be applied (*laissez faire* approach), as in UK, to imposing unnecessary burdens and additional requirements to data controllers, as in Greece and Spain[16]. Inconsistencies in interpretation also led to litigation before the CJEU[17]. Therefore, the Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data (further in the text: Article 29 WP)[18], had included the issue in its Work Program 2012-2013[19] and rendered the Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (further in the text: Opinion WP 217)[20]. The Opinion WP 217 provides guidelines on application of Article 7(f) with

abovementioned three requirements.

14 These are fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

15 Consent might be the exception.

16 Annex 2 Evaluation of the Implementation of the Data Protection Directive, to the COMMISSION STAFF WORKING PAPER, Impact Assessment Accompanying several documents, Brussels, 25.1.2012, SEC(2012) 72 final, retrieved on March 12th, 2015 from http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf, at 17.

17 Judgement in *ASNEF and FECEMD*, ECLI:EU:C:2011:777.

18 The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. See more at the web page retrieved on March 12th, 2015 from http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

19 Adopted on 1 February 2012 (WP 190).

20 ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Adopted on 9 April 2014, 844/14/EN, WP 217, retrieved on March 12th, 2015 from http://www.cnpd.public.lu/fr/publications/groupe-art29/wp217_en.pdf.

emphasis and detailed instructions on controller's or third party's legitimate interest and the balancing test between opposing interests of data controller or third party and those of data subject.

2.2.1. Legitimate interest

Establishing the legitimacy of the data controller's or third party's interest is the first step in justifying data processing under Article 7(f). Absent the legitimate interest, there cannot be lawful data processing. Irrespective of its importance, the concept of «legitimate interest» is left undefined under the Data Protection Directive. The Article 29 WP states that in order to be considered legitimate, the interest has to be: 1) lawful, 2) sufficiently specific and 3) real and present.[21] The lawfulness requirement entails that the interest is not contrary to pertinent law, either EU or national law applicable at issue, where law is understood in the broadest sense.[22] Furthermore, the interest has to be sufficiently articulated to allow performance of the balancing test. It would be impossible to precisely counterbalance certain interest for fundamental right of a subject against unclearly defined interest of data controller or third party. Thirdly, the legitimate interest cannot be hypothetical or abstract, but has to be actual and existing. Because of the nature of these requirements, it is possible that legitimacy of the interest may change over time. Thus, an interest which was not deemed legitimate might become legitimate due to technological or social development.

In addition to three abovementioned «formal» requirements, the final assessment of the legitimacy of the interest will also depend on nature of the interest in data processing, environment in which the data processing takes place, and type of the data controller' or third party' operation[23]. In comparing the attributes of the data controller's or third party's interests against those of data subjects, it is interesting to note that the legitimate interest of former may be of different nature, whereas the interest of latter is limited to fundamental rights and freedoms of the data subject. On the other hand, the data controller's or third party's interest has to be a legitimate one, whereas there is no such additional requirement for the interest of data subject[24]. Returning to the question

21 Opinion WP 217, at 25.

22 See further Opinion WP 217, at 25, n. 48.

23 The CJEU recognised that operators of search engines might have different legitimate interest than web publishers in processing the same data. Judgment in *Google Spain SL and Google Inc*, ECLI: ECLI:EU:C:2014:317, paragraph 86.

24 «This implies a wider scope to the protection of individuals' interests and rights. Even individuals engaged in illegal activities should not be subject to disproportionate interference with their rights and interests. For example, an individual who may have perpetrated theft in a supermarket could still see his interests prevailing against the publication of his picture and private ad-

of nature of the interest, it is apparent that the interest might be private or public. The experience shows that such interest would often be private and economic, but it might be also social or political. This is reflected in the list of potentially legitimate interests provided by the Article 29 WP.[25] Thus, it is irrelevant that the Directive Preamble mentions only «the legitimate ordinary business activities of companies and other bodies».[26]

Without doubting that the existence of economic interest in data processing would not be an obstacle to its legitimacy, the question may arise as to whether a purely economic interest might be qualified as legitimate. In its judgment in *Google Spain*, the CJEU stated that there is «the economic interest of the operator of the search engine, but also the interest of the general public in finding that information upon a search relating to the data subject's name»[27]. In this case, as in many other cases, the legitimate interest is a mixed interest of the data controller or third party, and that of the specific user or public. A case in point is marketing or advertising, where data processing is economically-driven, but also has favourable effects on the interest of information addressee since the latter will have possibility to be informed in the personalised manner of the products or services marketed or advertised, not to mention direct interest of information addressee in finding desired information upon a search. Nevertheless, it would be erroneous to conclude that the interest could not be deemed legitimate just because it is exclusively economic. For example, a company which (internally) processes information about the type of company's products and services their customer use, with the purpose of selling a new service or product to this customer, does so exclusively with the economic interest to sell additional products and services. However, this interest alone should be sufficient to be qualified as legitimate. This conclusion seems to be further confirmed by the non-exhaustive list of the most common potentially legitimate interests where one may find marketing and advertising, employee monitoring for management purposes and debt collection[28].

Personal data processing by Internet search engine operators is specific because of intermediary role the Internet search engine operators play between third party web pages, on which personal data are published, and Internet search engine users. Acting as intermediaries, they are finding information published or placed on the Internet by third parties,

---

dress on the walls of the supermarket and/or on the Internet by the owner of the shop.» Opinion WP 217, at 30.

25 See the full list in Opinion WP 217, p. 25 (see also p. 26 for the public interests).

26 Recital 30 of the Data Protection Directive. For pointing to this type of interest, see Bergkam, L. (2003). *European Community Law for the New Economy*. Antwerp: Intersentia, at 83.

27 Judgment in *Google Spain SL and Google Inc.*, ECLI: ECLI:EU:C:2014:317, paragraph 97.

28 Opinion WP 217, p. 25. See also Recital 2 of the Data Protection Directive stating that «data-processing systems [...] must [...] respect [natural persons'] fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals».

indexing them automatically, storing them temporarily and making them available to Internet search engine users. In providing services to Internet search engine users, Internet search engine operators are not altering original information containing personal data, but are simply producing hyperlinks to pages selected based on keywords entered by users. Based on given activity description, one may conclude that there is a legitimate interest on the part of the Internet search engine operator to process personal data and produce search results in reply to the user's request. To be precise, such service is certainly lawful (at least in EU), sufficiently specific, real and present. Moreover, the Internet search engine operator's interest in processing the data is apparently one of economic nature as this is the means to make the provision of its services profitable[29]. In addition to the economic interest of the Internet search engine operator, there is also interest of the public to find information via the Internet search engine based on the keyword corresponding to a person's name.[30]

Irrespective of the economic interest in the basis of Internet search engine service, this service is very important for the Internet search engine users. Given the abundance of information on the Internet it is presently the unparalleled means for finding desired information, which otherwise would probably not be known to and/or accessed by many, becomes available to Internet search engine users on a large scale. As the CJEU points out in Google Spain, collection of data eventually allows anyone to make a relatively detailed profile of a natural person simply by searching the Internet[31]. Thus, the CJEU confirms that there is potentially a myriad of data on a single person which might be posted on different Internet sites. Nevertheless, these personal data have not been posted by the Internet search engine operators. Moreover, in performance of their activities, Internet search engine operators are not able to distinguish between personal data and other data[32]. These features were and still are the main reasons for opposing the new finding of CJEU in Google Spain that Internet search engines are to be characterised as data controllers within meaning of Article 2(d)[33]. Instead of further discussing applicability of the data controller's definition to search engine operators (which is a prerequisite for applicability of other provisions of the Data Protection Directive), as this issue is already recognized in scholarly writings[34], the issue is tackled from a different angle.

29 The CJEU's mentions the profitability as an important feature in the context of territorial scope of the Directive. See judgment in *Google Spain SL and Google Inc.*, ECLI: ECLI:EU:C:2014:317, paragraphs 56 and 57.

30 See *supra* n. 26.

31 Judgment in *Google Spain SL and Google Inc.*, ECLI: ECLI:EU:C:2014:317, paragraph 80.

32 Opinion of Advocate General Jääskinen, 25.6.2013, ECLI:EU:C:2013:424, paragraph 86.

33 Opinion of Advocate General Jääskinen, ECLI:EU:C:2013:424, paragraphs 84-90.

34 See e.g. Lindsay, D. (2014). The 'Right to be Forgotten' by Search Engines under Data Privacy Law: A Legal Analysis of the Costeja Ruling. *Journal of Media Law*, 6(2), 159-179; Minero Alejandre, G. (2014). A vueltas con el «derecho al olvido». Construcción normativa y jurispru-

2.2.2. Balancing test

Assuming that Internet search engine operator is indeed a data controller within meaning of the Data Protection Directive, in order to process the data it has to rely on one of the legal grounds in Article 7. In case of Article 7(f), suggested by CJEU as the most likely ground applicable to Internet search engine operators, the balancing test has to be performed. Importance of the balancing test has been emphasised by the Article 29 WP when stating that «[t]he outcome of this balancing test will determine whether Article 7(f) may be relied upon as a legal ground for processing»[35]. It has also been confirmed by the CJEU that application of Article 7(f) «necessitates a balancing of the opposing rights and interests concerned»[36]. Like the notion of the «legitimate interest», the balancing test is largely undefined under the Data Protection Directive. Therefore, one has to turn to guidelines provided in the case law and the explanatory documents. There are two essential issues related to the balancing test: factors to be taken into consideration in performing the test and the time when the test is to be performed.

a) Factors in the balancing test

Balancing test requires assessment of several factors, namely: 1) legitimate interests of data controller or third party to whom data are disclosed, 2) impact on data subject, 3) possible provisional balance and 4) possible additional safeguards applied by controller to prevent any undue impact on data subjects[37]. Although for theoretical reasons these requirements are discussed separately, overlaps are possible since the balancing test is integral test of weighing contrasted interests. It is important to note that the balancing test is made on case-to-case basis, meaning that the legitimate interest in specific data processing has to be contrasted with the data subject's actual interest for fundamental rights and freedoms.

With regard to the first factor, it is important to note that once the interest has been qualified as legitimate it enters into the balancing test and has to be weighed against data

dencial del derecho de protección de datos de carácter personal en el entorno digital. *Revista Jurídica de la Universidad Autónoma de Madrid*, 30(II), 129-155; Gilbert, F. (2015). The Right of Erasure or Right to Be Forgotten: What the Recent Laws, Cases, and Guidelines Mean for Global Companies. *Journal of Internet Law*, 18(8), 1 and 14-20. See also Bennett, S. C. (2012). The «Right to Be Forgotten»: Reconciling EU and US Perspectives. *Berkeley Journal of International Law*, 30(1), 161-195.

35 Opinion WP 217, p. 3 (see also p. 25).

36 Judgment in *Google Spain SL and Google Inc.*, ECLI:EU:C:2014:317, paragraph 74.

37 Opinion WP 217, at 33.

subject's interest. In deciding which interest prevails, it is important to justify data processing in question against the principles of necessity and proportionality. On the first level, the interest cannot prevail if data processing is not necessary for attainment of the legitimate interest. If such interest may be attained without data processing, the interest cannot prevail. On the second level, even if data processing is necessary, the interest still cannot prevail if the same interest can be achieved by processing the data in another manner, which entails lesser interference with protected rights and freedoms.

In order to determine the impact on data subject, which constitutes the second factor in the balancing test, both positive and negative impacts, of internal and external nature, have to be taken into consideration. According to Article 29 WP, although methodology from traditional risk scenarios relying on quantitative impact assessment can be helpful, it cannot be entirely replicated to this assessment, because the assessment has to take into account the impact on even a single individual[38]. Two key elements of impact assessment are likelihood of the risk and severity of possible consequences. Furthermore, for determining the impact on data subject the nature of personal data processed plays important role: The impact is greater if special categories of personal data referred to in Article 8[39] of the Data Protection Directive or other sensitive data[40] are being processed. In assessing the level of impact on data subject other factors have also to be taken into account, including the way data is being processed (by making them publicly available to large number of audience, e.g. on the Internet and/or by combining different data such as profiling etc.), reasonable expectations of data subjects, as well as data subject's personal status (e.g. child as opposed to adult public figure) and data controller's professional status (multinational entity with dominant power as opposed to small local enterprise or individual)[41].

The third factor, so-called provisional balance, requires compliance with general obligations from the Data Protection Directive, such are transparency and proportionality (horizontal compliance), and possible additional measures beyond the horizontal compliance (e.g. user friendly unconditional opt-out mechanism). This factor is explained in a way that data controller's full compliance with the Directive results in reduced impact on data subject and contributes to ensuring that requirements of Article

38 Opinion WP 217, at 38.

39 Article 8 of Directive, lists special data categories, the first includes data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health and sex life; the second includes data relating to offences, criminal convictions or security measures, and the third (optional) includes the data on a national identification number or any other identifier of general application.

40 Although not regulated under special categories, some personal data are also perceived as sensitive, e.g. data on location or geolocation, biometric data, etc.

41 Opinion WP 217, at 39-41.

7(f) are met[42]. As appealing as this explanation might seem at first glance, it is hard to see the connection between the two. All the more, it should go without saying that other obligations under the Directive have to be fulfilled (as obligatory precondition) regardless of the ground on which the data processing is being justified. Recognising that the balancing test integrates all factors and is in practice more complex than in theory and entails concurrent assessments of all factors, it is still unfortunate that clearer separation line between additional measure in provisional balance factor and ensuring additional safeguards under the fourth factor is lost.

The fourth factor of the Article 7(f) balancing test relates to additional safeguards applied by the data controller to prevent any undue impact on data subjects. These may be adequate technical and organizational measures (e.g. encryption, pseudonymisation, functional separation), aggregation of data, privacy-enhancing technologies (PET's), privacy by design, etc. This factor seems to be overlapping with the second factor and could perhaps be more efficiently dealt with directly and in conjunction with other elements relevant to impact data subjects. For the same reason, additional measure segment of the provisional balance factor should be combined with the fourth factor and included in the second factor. The difference in nature of the measures (legal consisting in opt-out and technical consisting in the measures mentioned under the fourth factor) does not justify separation because it is often the case that the same effect might be achieved by both legal and technical measure and this should beat the option of the data controller. Logically, these aspects should be decided together.

Based on the above, the balancing test may prove a rather convoluted process, not only because it depends on the circumstances of each particular case, but also because of the vagueness of applicable criteria. With the aim of making it less ambiguous and more logical, the proposal is here submitted that the assessment is made on the basis of only the first two factors initially proposed by the Article 29 WP: 1) legitimate interests of data controller or third party to whom the data are disclosed and 2) impact on data subject. The latter factor would also include assessment of elements which the Article 29 WP included in the part of the third factor (e.g. opt-out mechanism) and the entire fourth factor. The part of the third factor which relates to fulfilment of duties under the Directive other than those under Article 7(f) should be a matter of separate procedure and evaluation, as they need to be complied with in all circumstances and with respect to all Article 7 legal grounds.

b) Timing of the balancing test

Important question in applying the balancing test and determining whether the requirements of Article 7(f) are met *in casu*, is a moment when the balancing test is to be

42 Opinion WP 217, at 41.

performed. Although it seems undisputed that the balancing test is to be performed taking account of the circumstances existing from the beginning and throughout the data processing, the question that remains open is whether it has to be performed prior to the processing or later on, upon data subjects' objections. Having in mind the wording of Article 7, which allows for data processing only if particular legal ground exists, as well as the fact that the balancing test is necessary to determine whether the requirements of Article 7(f) are fulfilled, it can be logically concluded that the balancing test should be performed prior to any data processing and not (only) afterwards, e.g. upon possible data subject's objection. In its Opinion WP 217, the Article 29 WP seems to confirm such understanding by stating that «the balancing test of Article 7(f) [...] is made 'a priori'» and that «[t]o ensure protection from the start, and to avoid the shifting of the burden of proof is circumvented, it is important that steps are taken before the processing starts, and not only in the course of *ex-post* objection procedure»[43].

Having in mind the purpose of the provision of Article 7 (f) and clear statements as to the timing of the balancing test, the Article 29 WP's comment upon the judgment in *Google Spain* comes as a true surprise. In its Guidelines on implementation of the CJEU's judgement in *Google Spain*, the Article 29 WP simply states: «The ruling does not oblige search engines to permanently carry out that assessment in relation to all the information they process, but only when they have to respond to data subjects' requests for the exercise of their rights»[44]. While this statement causes significant controversy, it lacks any explanation as to its reasons.

In this context, it seems necessary to make a clear distinction between legal grounds for lawful data processing under Article 7 of the Data Protection Directive, and explicit data subjects' rights granted by the same Directive. The data subjects' right in question include rights referred to in Article 12 of the Directive (in particular paragraph (b) relating to rectifying, erasing or blocking of data under certain conditions), as well as data subject's right to object referred to in Article 14 (in particular paragraph (a) relating to right to object to data processing in certain cases, especially in cases captured by Article 7(f)). These rights do not constitute criteria and/or legal grounds for lawful data processing additional to those in Article 7. Nevertheless, these data subject's rights are often mistaken for an additional legal ground for lawful data processing, in particular the right to object, which is sometimes understood as opt-out mechanism mentioned in the third factor of the balancing test. This follows from the CJEU case law in which it is stated

43 Opinion WP 217, at 45 and 53.

44 ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on the implementation of the Court of Justice of the European Union Judgment on «*Google Spain and Inc. v. Agencia Espanola de Preccion de datos (AEPD) and Mario Costeja Gonzalez*» C-131/12, 14/EN, WP 225, 26.11.2014, retrieved on March 18th, 2015 from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf, at 6.

that Article 7 of Directive 95/46/EC sets out «an exhaustive and restrictive list» of cases in which the processing of personal data can be regarded as being lawful[45], implying there are no further legal grounds for data processing. In its judgment in *Google Spain*, the CJEU did not discuss this matter in much detail, but it appears as if its position has not changed[46]. Article 12 actually allows recourse by the data subject who believes that certain data processing is unlawful[47]. If data are processed by the controller not complying with the Directive, data subject has the right to have them deleted[48]. Under Article 14, even in cases where data subjects' consent is not a prerequisite for lawful processing, data subject retains participation in the form of the right to object. Data subject may block use of her/his data in explicitly mentioned circumstances and such objection supersedes otherwise lawful processing, including that under the Article 7(f), provided (s) he has a compelling legitimate ground. This counterbalances vaguely phrased criteria for lawful processing (in the absence of the consent)[49]. Exercise by data subjects of these additional rights in the course of data processing, triggers verification of legal ground, and if Article 7(f) is relied on by the data controller, this also involves assessment of the balancing test factors (under the circumstances existing from the moment data processing commenced, until it is completed). This, however, does not remove the duty of the data controller to determine whether requirements of Article 7(f) are met ahead of and in the course of data processing[50].

45 Judgement in *ASNEF and FECEMD*, ECLI:EU:C:2011:777, paragraph 30.

46 Judgment in *Google Spain SL and Google Inc.*, ECLI: ECLI:EU:C:2014:317, paragraph 75.

47 Article 12(b) mentions examples of processing not in compliance with the Directive, but the CJEU points out that this provision also covers to the processing contrary to the data quality principles under Article 6 or legal grounds under Article 7. Judgment in *Google Spain SL and Google Inc.*, ECLI: ECLI:EU:C:2014:317, paragraphs 70 and 71.

48 Horn, B. et al. (2011). An Outline of the Technical Requirements on Governmental Electronic Record Systems Derived from the European Legal Environment. In: Klun, M./Decman, M./Jukić, T. (eds.). *The Proceedings of the 11th European Conference on EGovernment*. Reading (UK): Academic Publishing Ltd., 303-309, at 307. On differences between erasing or deleting the data, and restricting the access to the data, see Lindsay, D. (2014). The «Right to be Forgotten» in European Data Protection Law'. In: Witzleb, N. et al., *Emerging Challenges in Privacy Law: Comparative Perspectives*. Cambridge: Cambridge University Press, 290-337.

49 Simitis, S. (2001). Data protection in the European Union – The Quest for Common Rules. In: *Collected Courses on the Academy of European Law*, Vol. III, Book 1. The Hague: Kluwer Law International, 95-142, at 130.

50 «[The data subject's right to object] should not be seen as contradicting the balancing test of Article 7(f), which is made 'a priori': it rather complements the balance, in the sense that, where the processing is allowed further to a reasonable and objective assessment of the different rights and interests at stake, the data subject still has an additional possibility to object on grounds relating to his/her particular situation. This will then have to lead to a new assessment taking

Applying the balancing test to the circumstances in *Google Spain* presupposes establishing the legitimate interests of Google as Internet search engine operator and the interest for the «right to be forgotten» of Gonzales as data subject. If these two interests are established, the balancing test may take place. It entails weighting of the two conflicting interests based on the above factors. Knowing that Google was not aware of the content of neither or countless web pages included in natural search results generated by the search based on the Gonzales' personal name, including web pages of La Vanguardia's newspaper, one is puzzled as to how was Google to assess, for instance, the necessity and proportionality of such processing or the impact on individual data subject? If Google were was to follow the CJEU's opinion expressed in the judgment in question, Google would have to assess legitimacy of the interest and all elements of the balancing test with regard to every single personal data related to every single data subject contained on all Internet pages. This is because, at least in theory, all Internet pages might prove relevant in any one of the searches done by Google Search users. Having in mind the abovementioned nature of personal data processing by Internet search engine operators and vast amount of personal data processed by them in the course of providing the search engine services, it is evident that the balancing test is virtually impossible, at least prior to data processing. Being intermediaries, the Internet search engine operators do not have knowledge of exact personal data posted on web pages they make available to its users, let alone can they assess a possible impact of such processing on all data subjects in advance. The knowledge they have on personal data relates to their users (e.g. geolocation), and as a rule they process such data in the meaning of the Data Protection Directive. Imposing a duty on Internet search engine operators to verify legal ground for lawful data processing regarding every personal data possibly contained in web pages included in their natural search results would make them liable for such data processing related to all persons in the world. This would most likely call into question the whole functioning and purpose of Internet search engines.

What follows from the impossibility of applying the balancing test to Internet search engine operators? Most certainly, it should not lead to a conclusion that these operators cannot rely on Article 7(f), but merely on other grounds for lawful data processing, not only because this would contradict CJEU's explicit wording, but also because it would discriminate them against other data controllers. Instead, the only viable explanation is that initial qualification of Internet search engine operators as data controllers was erroneous.

into account the particular arguments submitted by the data subject. This new assessment is in principle again subject to verification by a data protection authority or the courts.» Opinion WP 217, at 45.

3. LIABILITY OF INTERNET SEARCH ENGINE OPERATORS

In characterising Google as the data controller in the context of Google search services, the CJEU choose to stick closely to the wording of definition of the data controller provided for in Article 2 of the Data Protection Directive. Avoiding to directly negate relevance of the lack of control over personal data for the purpose of defining the data controller, it merely stated that «[it] would be contrary to […] that provision […] to exclude operator of search engine from that definition on the ground that *it does not exercise control* over personal data published on the web pages of third parties»[51]. Although the Article 2 definition does not refer explicitly to control, control is most likely though implied in its wording. In construing such meaning, one has to bear in mind that this definition dates back to 1995, when information technology and Internet business models were tremendously different from today. There are also other arguments more closely related to the legal structure of liability of intermediaries.

Characterising Internet search engine operators as data controllers within the meaning of Article 2 of Data Protection Directive, has much broader implications on their duties and obligations under the Directive than simply to accommodate data subjects' rights provided under Articles 12 and 14. It imposes on them all other obligations of data controllers under the EU data protection legislation. Perhaps even more important are the sanctions for non-compliance with these duties. According to Article 23 of the Data Protection Directive, controllers are in principle liable for damages resulting from unlawful data processing. Liability is excluded in situations where controller is not responsible for the event giving rise to damage, the burden of proof being on the controller. Similar liability provisions are included in the current proposal of the new data protection framework with an important amendment that liability is placed not only on the data controller, but also on data processor[52]. Thus, the result of the CJEU's judgment in *Google Spain* is that Internet search engine operators, acting as controllers, are in principle liable for all personal data published by third parties on all web pages they generate in their search results.

Prior to the judgment in *Google Spain*, situation with respect to liability of Internet search engine operators was substantially different. In its Opinion 1/2008 on data protection issues related to search engines (further in text: Opinion WP 148)[53], the Article

51 Judgment in *Google Spain SL and Google Inc.*, ECLI: ECLI:EU:C:2014:317, paragraph 34.

52 Article 77 of the EP legislative resolution on the GDPR.

53 ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 1/2008 on data protection issues related to search engines, 00737/EN, WP 148, 4.4.2008, retrieved on March 10th, 2015 from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf.

29 WP stated that when Internet search engine providers act[54] as providers of content data (as in case of Google Search) they are generally not to be held primary responsible under the EU data protection law[55]. The reason for this was found *inter alia* in the lack of legal and factual control that an Internet search engine operator has over personal data when the content including personal data is provided by web publishers. Furthermore, the Data Protection Directive recognizes that controller of personal data contained in the message will normally be considered to be the person from whom the message originates, rather than person offering transmission services (telecom and e-mail though)[56]. As stated by the Advocate General Jäskinen, the aforementioned «[b]uilds on the legal principle according to which automated, technical and passive relationships to electronically stored or transmitted content do not create control or liability over it»[57].

This principle is to be also found in the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (further in the text: the E-Commerce Directive)[58]. Aware of the fact that this Directive excludes questions relating to information society services covered by the Data Protection Directive,[59] the two legal regimes are compared here in order to assess whether more convergence would be appropriate. Additionally, although the scope of the E-Commerce Directive does not include linking or search engine services[60], some countries have enacted laws in these fields in the similar vein as the E-Commerce Directive[61]. In a view of the intermediate function of Internet search engine operators, under these national laws they would

54 However, according to Article 29 WP, there are situations where Internet search engine operators can be defined as data controllers and are subject to data protection law (e.g. when they collect IP addresses of Internet users, etc.), but these are completely different situations from the one in which they act as intermediaries.

55 Opinion WP 148, at 24.

56 Recital 47 of the Data Protection Directive.

57 Opinion of Advocate General Jääskinen, ECLI:EU:C:2013:424, paragraph 87.

58 OJ L 178, 17.7.2000, 1–16.

59 Article 1(5)(b) of the E-Commerce Directive. Some authors claim that this provision might be construed to permit the applicability of the E-Commerce Directive to immunity from liability of the Internet search engine operators. See e.g. Sartor, G. (2014), Search engines as controllers: inconvenient implications of a questionable classification, *Maastricht Journal of European and Comparative Law*, 21(3), 574.

60 See Article 21(2) of the E-Commerce Directive.

61 E.g. Austria (*Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäftsund Rechtsverkehrs geregelt, und das Signaturgesetz sowie die Zivilprozessordnung geändert werden*, BGBL, I 2001/152) and Croatia (*Zakon o elektroničkoj trgovini*, NN, 173/03, 67/08, 36/09, 130/11 and 30/1).

be considered intermediary service providers, equivalent to the meaning of the Section 4 of the E-Commerce Directive. While the Directive does not provide for the grounds and conditions of their liability, as this question is left to the national laws, it harmonises the exemptions from such liability.

According to the E-Commerce Directive provisions, intermediary service providers are in general not liable for the content of information they transmit/store[62], provided their role is merely technical, active and passive, which implies they have neither knowledge nor control over transmitted/stored information[63]. Indeed, the CJEU held that, in providing the AdWords service, Google might rely on the exemption under Article 14 in the case where it has not played an active role of such a kind as to give it knowledge of, or control over, the data stored. Google's only duty in such situation is to act expeditiously upon having obtained knowledge of the unlawful nature of those data. If it fails to act, it becomes liable[64]. Thus, under the respective national laws which have extended the E-Commerce Directive scope (but probably not within the realm of the Data Protection Directive!), the Internet search engine operator would not be liable for damages unless taking an active role in providing services or failing to act upon becoming aware of unlawfulness. This obligation to act relates simply to expeditious removal or disabling of the access to the data concerned. As such, it corresponds to the Article 29 WP's earlier understanding of the control, which an Internet search engine operator has over personal data, and which is usually limited to the possibility of removing data from its servers[65]. Under no circumstances can there be a monitoring duty on the part of the Internet search engine providers when acting as intermediaries[66].

In situation in which Google provides Internet search services and within it displays the relevant hyperlinks, as an Internet search engine operator under the national laws of certain Member States, it might have the technical means to remove data from the search list, but as a rule does not have awareness or control prior to data subject's

62 Articles 12-14 of the E-Commerce Directive.

63 Recital 42 of the E-Commerce Directive. The main reason for this was to boost the development of the, among other, e-commerce industry in the EU. See Recital 2 of the E-Commerce Directive.

64 Judgment in *Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08)*, 23.3.2010, ECLI:EU:C:2010:159, operative part 3. See also subsequent Judgment in *Interflora Inc. and Interflora British Unit v Marks & Spencer plc and Flowers Direct Online Ltd.*, 22.9.2011, ECLI:EU:C:2011:604.

65 Opinion WP 148, at 14.

66 Article 15 of the E-Commerce Directive; Judgement in *L'Oréal SA and Others v eBay International AG and Others*, 12.6.2011, ECLI:EU:C:2011:474, paragraph 139.

request. Because of these characteristics, the liability legal regime for the Internet search engine operators when dealing with protected data in the sense of the Data Protection Directive should be more convergent with the one they would have under the (by the national laws extended) E-Commerce Directive. Thus, the judgment in *Google Spain* might have fitted the E-Commerce Directive framework better than the one of the Data Protection Directive where lawful ground for processing has to exist at the time of processing, an impossible requirement to be met by the Internet search engine operators.

4. CONCLUSION

Legal grounds for lawful personal data processing in EU law are insufficiently clear and intensively debated within the process of rendering new EU data protection framework (GDPR). The CJEU judgment in *Google Spain* comes as an additional stumbling stone in subjecting the Internet search engine operators under the data controller category. Because in circumstances in which Article 7(f) is invoked, the role of data controller entails *ex ante* and constant assessment of the lawfulness of data processing, in particular carrying out the balancing test, the situation of legal and practical incoherence is created. While Article 7(f) of the Data Protection Directive requires the data controller to assure legitimate ground for lawful personal data processing ahead of and during the processing in question, the CJEU's judgment in *Google Spain* requires the same assurances to be made by Internet search engine operators who are neither aware nor have control over personal data. By qualifying them as data controllers, it also makes them liable for damages in cases of unlawful processing with respect to personal data published by third parties. All the more, the Article 29 WP in its Guidelines on the judgment in *Google Spain,* adds a further confusing factor by stating that Internet search engine operators need not assure the legitimate ground for lawful data processing in advance, but merely upon the data subject's request. While the judgment in *Google Spain* puts the Internet search engine operators in completely illogical legal position, the Article 29 WP Guidelines creates contradiction in the data processing scheme under the Data Protection Directive. The common initial source of these difficulties is in qualifying the Internet search engine operators as data controllers.

The opportunity should not be missed to correct this legal situation in the course of the legislative process of adopting the GDPR. If, however, which is realistically the most probable scenario, such twist will not happen, it is suggested that the new regulatory scheme for Internet search engine (and alike) operators should be explicitly included in the GDPR because of the legal certainty[67]. To be precise, a provision to that effect should

67 In that respect, very interesting is the recent proposal of Germany with respect to GDPR and legitimate interest legal ground. Germany proposed explicit inclusion in the GDPR of the pre-

make the following clear: a) that the Internet search engine operators when acting as intermediaries are not under any duty to assess legal grounds for lawful data processing, b) that they might be asked to carry out such assessment only upon data subject's request, and c) that, if it is found that the data processing is unlawful, such operator might only be subject to injunctions for removal or blocking the access to the respective data, but not to damages, unless it fails to remove or block the access to the data expeditiously upon becoming aware of the subject data's legitimate interest in doing so.

5. BIBLIOGRAPHY

(2015). *Data Protection Broken Badly*. EDRi/Access/Panoptykon Foundation/Privacy International. Retrieved March 16th, 2015 from https://edri.org/files/DP_BrokenBadly.pdf.

Bennett, S. C. (2012). The «Right to Be Forgotten»: Reconciling EU and US Perspectives. *Berkeley Journal of International Law*, 30(1), 161-195.

Bergkam, L. (2003). *European Community Law for the New Economy*. Antwerp: Intersentia.

Gilbert, F. (2015). The Right of Erasure or Right to Be Forgotten: What the Recent Laws, Cases, and Guidelines Mean for Global Companies. *Journal of Internet Law*, 18(8), 1 and 14-20.

Horn, B. et al. (2011). An Outline of the Technical Requirements on Governmental Electronic Record Systems Derived from the European Legal Environment. In: Klun, M./Decman, M./Jukić, T. (eds.). *The Proceedings of the 11th European Conference on EGovernment*. Reading (UK): Academic Publishing Ltd., 303-309.

Lindsay, D. (2014). The 'Right to be Forgotten' by Search Engines under Data Privacy Law: A Legal Analysis of the Costeja Ruling. *Journal of Media Law*, 6(2), 159-179.

Lindsay, D. (2014). The «Right to be Forgotten» in European Data Protection Law'. In: Witzleb, N. et al., *Emerging Challenges in Privacy Law: Comparative Perspectives*. Cambridge: Cambridge University Press, 290-337.

Minero Alejandre, G. (2014). A vueltas con el «derecho al olvido». Construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en

sumption that the subject's interest and fundamental rights and freedoms do not override the controller's interests in case of pseudonymisation of personal data that are being processed. Without prejudice as to whether pseudonymisation is a proper tool for presumption of the legal ground in question or not, this proposal at least adds some legal certainty to this erratic state of affairs.

el entorno digital. *Revista Jurídica de la Universidad Autónoma de Madrid*, 30(II), 129-155.

Sartor, G. (2014), Search engines as controllers: inconvenient implications of a questionable classification, *Maastricht Journal of European and Comparative Law*, 21(3), 564-575.

Simitis, S. (2001). Data protection in the European Union – The Quest for Common Rules. In: *Collected Courses on the Academy of European Law*, Vol. III, Book 1. The Hague: Kluwer Law International, 95-142.