Old and new domains of privacy: towards the "right to be forgotten"

Estrella Gutiérrez David

Visiting Lecturer, Universidad Rey Juan Carlos

(Department of Public Law I and Political Science)

EJC Judgment of 13 May 2014, Case C-131/12 Google Spain SL. and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González. Privacy, personal data, right to be forgotten, search engines, freedom of expression.

An old social security debt already paid a long time ago but still owed on the Internet; an unbalanced struggle between an ordinary citizen and a giant tech company; two different cultural approaches on privacy face to face –the Anglo-American "right to be let alone" *versus* the far-reaching "right to be forgotten" embraced by Europe- have turned the well-known "Google Case" into a landmark decision.

As the Advocate General noted to this case in his delivered opinion on 25 June 2013, the dispute to decide is meant to be "the first case" in which the ECJ has been requested to construct the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data (hereinafter, the "**Directive**") in the context of Internet search engines (Advocate, para. 7)

In fact, when the Directive was adopted "the internet in the present sense of the World Wide Web, did not exist, and nor were there any search engines" –observed the Advocate. At those times, "the first rudimentary search engines started to appear, but nobody could foresee how profoundly it would revolutionise the world (Advocate, para. 10)"

Due to the implications of this case for the activity of search engines and, ultimately, for the current functioning and development of the Internet, this approach on Google decision will encompass not only the analysis of the main findings of the ECJ decision, but also the opinion issued by the Advocate General in relation to those aspects splitting away from the ECJ's arguments.

1.- Implications of search engines activities

One of the main questions referred to the ECJ is whether the primary activity of search engines consisting of crawling on the Internet, locating information included on third parties' websites, indexing it automatically, storing it temporarily and finally making it available to internet users according to a particular order of preference may be deemed as data processing when such retrieved information contains personal data if any of the web pages does.

The relevance of the aforesaid activities has been explained by the Advocate General: "[…] universal accessibility of information on the internet relies on internet search

engines, because finding relevant information without them would be too complicated and difficult, and would produce limited results (see Advocate, para. 45)"

To understand the real implications of search engines on privacy, it is of importance to examine some of the issues decided by Courts in matters of the Internet. In this sense, the facts of the English Case *Max Mosley v News Groups Newspapers Ltd* (2008) and the fatalistic concluding remarks of the High Court of England and Wales (hereinafter, "**EWHC**") may illustrate how information can be rapidly accessed, widespread and traced over the architecture of the Internet and search engines.

In effect, the News of the World had published a front page article including very intimate photographs taken from a secretly recorded video footage about a well-known figure in the Formula One. After its publication, in only one day, the on-line version of the article had been visited approximately 435,000 times, whereas the edited footage itself had been viewed about 1,424,959 times.

Considering that such intrusive and demeaning information was "so widely and generally accessible in the public domain" of the Internet, the EWHC asked itself rhetorically "what [could] be achieved by an injunction in [those] circumstances". The answer was entirely resigned: "[…] such an injunction would make no practical difference". Moreover, in the view of the Court, the claimant no longer had "any reasonable expectation of privacy in respect of this now widely familiar material or that, even if he has, it has entered the public domain to the extent that there is, in practical terms, no longer anything which the law can protect". This seems to be a devastating and hopeless conclusion for individuals to be said by a Court of law, doesn´t it?

2- Far beyond the "right to be let alone"

Privacy and technologies have had always a controversial relationship. "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops." Such a statement could have been said by a guru of the Internet, but the quote is more of one century old and its maternity must be attributed to the prominent American jurists, Louis Brandeis and Samuel Warren.

In their famous written, "The right to privacy" (1890), both jurists expressed their concern about the protection of privacy against the impact of technology and economic interests of enterprises: "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right «to be let alone»".

At present the decision of the ECJ in Google Case seems to express the same old concerns with little differences. Instantaneous photographs and newspaper enterprises of then have led to the Internet and search engines. Along with privacy other fundamental rights are at stake, namely, personal data whose processing

through lists of results provided by search engines on the basis of individual´s name enables to build profiles of individuals. In addition, within the scope of personal data protection it must be included the "right to be forgotten", which would involve the right of data subject to erase, to block and/or to object indexing of and linking to the information relating to him personally, and published on third parties' web pages (ECJ, para. 20.3)

"[…] [T]he processing of personal data –says the ECJ- carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data which encompasses the right to be forgotten when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet —information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty— and thereby to establish a more or less detailed profile of him (ECJ, para. 80)".

Not only does the ECJ go back to such old concerns but it also warns against the new perils of the ubiquity of information provided by search engines. "Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous (*Ibidem*)."

Finally "business methods" –as referred by Warren and Brandeis- have been substituted by what the Advocate General calls as "business model of internet search engine service providers" (Advocate, para. 64) or the "economic interest" of search engines in taking advantage of their main activity (indexing and providing lists of results) and including, in return for payment, promotion and sale of advertising associated with the internet users' search terms.

Nevertheless, the fact that both activities are offered by two different but linked undertakings (a parent company and its subsidiary) located in different jurisdictions raises the question of which is the applicable law to the Internet controversies in matters of personal data processing. This is of importance especially when such offshoring of business may seek "to prevent individuals from being deprived of the protection guaranteed by the [Directive] and that protection from being circumvented, by prescribing a particularly broad territorial scope (ECJ, para. 54)"

3.- David against Goliath: facts and subject matter of the case

The facts of the case were as follows. In 2010, a Spanish citizen, Mario Costeja, filed with the Spanish Data Protection Agency, Agencia Española de Protección de Datos (hereinafter, the "**AEPD**") a complaint against a daily newspaper with large circulation in Spain, especially in Catalonia, La Vanguardia, and against the search engine operator, Google Inc., located in California, and its subsidiary and representative in

Spain, Google Spain. Mr Costeja claimed that, when an Internet user entered his name in Google search engine, the list of results displayed links to two pages of the said newspaper, published on January and March 1998. Those pages in particular contained an announcement for a real-estate auction due to attachment proceedings for the recovery of social security debts owed by the Claimant. Nevertheless, according to Mr Costeja, those attachment proceedings had been resolved some years ago and such reference to them was now entirely irrelevant.

The AEPD dismissed the complaint against La Vanguardia, because in the view of the Agency that controversial information in question had been lawfully published by the newspaper. In fact, Spanish regulation on social security revenue has usually prescribed maximum publicity in mass media for auctions of attached assets belonging to a social security debtor in order to ensure as many bidders as possible. Conversely, the AEPD upheld the complaint against Google Spain and Google Inc. and the AEPD ordered both companies to remove data from their index and to prevent any access to them in future. Google Spain and Google Inc. brought two separate appeals before the Audiencia Nacional (National High Court in Spain) against the Agency decision. In those circumstances, the Court decided to stay the proceedings and to refer the following questions to the ECJ for a preliminary ruling.

The questions referred to the ECJ fall into three categories:

(1) The nature of search engines activity as data processing and, consequently the possible role of data controller –that is the natural or legal person who determines the purposes and means of data processing– of search engines operators in the light of the Directive, especially in terms of its *scope of application ratione materiae*;

(2) The *territorial scope of* the Directive and its application to a company located in a jurisdiction outside the European Union when such company has a subsidiary and representative in the territory of a Member State;

(3) The scope of the so-called *right to be forgotten* and whether a data subject can request that some or all search results concerning him are no longer accessible through search engine, regardless such personal information displayed in the list of results of the search engine has been published lawfully by a third party.

4.- Search engines as data controllers

The referring Spanish Court asked whether the activity of a search engine as a content provider which consists in finding information published or placed on third parties' web pages, indexing it automatically, storing it temporarily and, finally, making it available to internet users in a list of results must be deemed as personal data processing within the meaning of the Directive when such indexed information contains personal data. If so, the referring Court sought to determine whether under the Directive the operator of a search engine had to be regarded as the "data controller" in respect of that processing of the personal data.

Strictly speaking in the view of the ECJ it was undeniable that: "[…]in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results." The ECJ concluded that "as those operations are referred to expressly and unconditionally in the Directive, they must be classified as data processing (ECJ para. 28)"

As to the question whether the operator of a search engine service must be regarded as the "data controller" in respect of the processing of personal data carried out by the search engine, the Court found that "it is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing."

Moreover, according to the ECJ the fact that publishers of websites had the option of requesting search engines, (by means in particular of exclusion protocols such as 'robot.txt' or codes such as 'noindex' or 'noarchive') to exclude wholly or partially specific information from being indexed did not mean that, "if publishers of websites [did] not so indicate, the operator of a search engine [was] released from its responsibility for the processing of personal data that it carries out in the context of the engine's activity" (ECJ, para. 39)

Interestingly, it must be noted that the approach of Advocate General had been the opposite. When examining the technical operations carried out by a search engine (crawling with the search bot software, indexing information which may include personal data, application of search algorithms to assess the relevance of search results, coping of the web pages on the cache memory and displaying them when an internet user makes a search), the Advocate came to the conclusion that Google search engine worked "without any human interaction with the data gathered" (Advocate, para. 72 in relation to 73-75). And this meant that a search engine service provider nor exercises "control over personal data included on third-party web pages" –as the service provider is "not 'aware' of the existence of personal data in any other sense than as a statistical fact web pages are likely to include personal data"- nor is able to "distinguish between personal data, in the sense of the Directive, that relates to an identifiable living natural person, and other data (Advocate, paras. 84, 86)"

5.- The "inextricable link": avoiding circumvention

Google Search, which is operated by Google, Inc. (located in California), indexes websites worldwide, including websites hosted in Spain. According to the ECJ decision, the information indexed by its 'web crawlers' is stored temporarily "on servers whose

State of location is unknown, that being kept secret for reasons of competition". In addition, Google Search "takes advantage of that activity and includes, in return for payment, advertising associated with the internet users' search terms". In doing so, Google group has set up its subsidiary, Google Spain, for promoting the sale of advertising space generated on the website 'www.google.com', targeting such activities essentially at undertakings based in Spain.

Given these facts, the question at issue is whether Google, Inc., as data controller, is subject or not to the Directive, inasmuch it has set up a subsidiary in Spain whose object is the promotion and sale of advertising space.

As the Advocate General recalled, the territorial scope of application of the Directive and the national implementing legislation is determined by any of the following conditions: (i) the placement of the "establishment of the data controller"; (ii) the location of the "means or equipment being used" when the controller is established outside the EEA. Specifically, when a data controller is not established on EU territory (as it is the case of Google, Inc.) but uses means or equipment situated on the territory of a Member State for processing of personal data, the legislation of that Member State applies unless such equipment or means is used only for purposes of transit through the territory of the EU (Advocate, para. 55, 60).

In order to determine if Google, Inc. fell under the territorial scope of the Directive, the ECJ had to analyse to which extent the parent company in California met any of the two aforementioned conditions. The ECJ concluded that Google, Inc. met the first condition, that is the "processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State". To justify this finding the ECJ assumed the argument of the claimant supported by the European Commission that there is an "*inextricable link* between the activity of the search engine operated by Google Inc. and the activity of Google Spain", to such extent that "the latter must be regarded as an establishment of the former and the processing of personal data is carried out in context of the activities of that establishment (ECJ, para. 47)"

"In such circumstances, -concluded the ECJ- the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed (ECJ, para. 56)"

In other words, the application of the Directive does not require the processing of personal data in question to be carried out 'by' the establishment concerned itself (that is Google, Inc.), but only that it be carried out 'in the context of the activities' of

the establishment. This means that the data processing carried out by the operator of the search engine is to be deemed in the context of the activities of Google Spain, an establishment of Google, Inc. Such wide interpretation of the wording of the Directive, as the ECJ admitted, seeks to "prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented, by prescribing a particularly broad territorial scope (ECJ, para. 54)"

Considering that the very display of personal data on a search results page constitutes processing of such data, the ECJ argued: "Since that display of results is accompanied, on the same page, by the display of advertising linked to the search terms, it is clear that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State, in this instance Spanish territory (ECJ para. 57)"

It follows from the foregoing that the Directive is to be interpreted as meaning that "processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, […] 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" (ECJ, para. 60)

6.- Is there a right to be forgotten on the Internet?

Given that search engine activities are engaged in data processing when the search engine operator indexes and displays personal information published by third parties, and once determined the application of the Directive to the activities carried out by Google, Inc., the last question at issue was focused on the so-called "right to be forgotten" and its scope under the Directive.

In this sense, the ECJ analysed whether 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 its publication on those pages is lawful.

If the first question was affirmative, it was also necessary to determine whether the fundamental right to personal data protection also encompasses the individual's right to request search engines the erasure of hyperlinks to his personal information and/or to prevent indexing of personal details related to him published lawfully on third parties' web pages, even if such information does not cause prejudice to the data subject, but it is inaccurate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing carried out by the search engine.

Put it in more simple way, the question at issue would be whether Google, Altavista or Bing are to withdraw from the list of results the links to web pages containing information related to an individual published by third parties, even when the publication of such information is lawful, for example, for journalistic purposes, but it is no longer relevant or updated.

In the view of the Advocate General, the answer to this question must be balanced with other interests at stake, basically, freedom of expression and right to information of web sites' publishers, that of the Internet users and that of the search engine service providers. But specific attention was drawn on freedom to conduct business and freedom of expression of search engines. In particular, the Advocate discouraged the ECJ from concluding that these competing interests –particularly personal data protection and freedom of expression- "could satisfactorily be balanced in individual cases on a case-by-case basis, with the judgment to be left to the internet search engine service provider". "Such 'notice and take down procedures', if required by the Court, -observed the Advocate- are likely either to lead to the automatic withdrawal of links to any objected contents or to an unmanageable number of requests handled by the most popular and important internet search engine service providers (Advocate, para. 133")

Despite the Advocate refusal of a case-by-case approach, the ECJ ruled otherwise. For the ECJ it was clear that far beyond the interest of internet users in having access to information or the economic interest of the search engine operator, the activity performed by the former entails a "potential seriousness" of interference with privacy and data protection of individuals, precisely because search engines make possible the ubiquity of information. In such a situation "a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter [of the European Union]".

The ECJ subtly rejected the Advocate´s argument of preponderance of freedom of expression and right to information. Otherwise, the ECJ supported a fair balance between the competing interests and a case-by-case approach based upon the public interest of the personal information displayed in the lists of results of a search engine: "Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life(ECJ, para. 81)"

In conclusion, the ECJ ruled that "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 (ECJ, para. 88)"

And the erasure of links will be owed, even when the personal information displayed by the search in the list of results does not causes "prejudice to the data subject" but such 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 (ECJ para. 96 in relation to 94)"

But this would not be the case if information upon a search relating to the data subject's name appeared, for particular reasons, such as the role played by the data subject in public life. Under such circumstances "the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question (ECJ, para. 100.4)"

This means that the operator obligation to remove from the list of results hyperlinks to personal information ceases when such information has a public interest. And though not mentioned by the ECJ, it must be added that, according to the well-stablished jurisprudence of the ECHR, such a public interest of personal information displayed by search engines must be understood in the context of a democratic society.

7.- Concluding remarks

At the core of the current debate on the right to be forgotten is the potential risk for freedom of expression, which allegedly would amount to a falsification of history written in books and newspapers. Ultimately, this has been one of the main arguments amongst absolutists of freedom of speech and libertarians of the Internet.

Some have even described the forthcoming right to be forgotten as the apocalypse of the Internet: "[…] it could precipitate a dramatic clash between European and American conceptions of the proper balance between privacy and free speech, leading to a far less open Internet (Rossen: 2012)." In this sense, the right to be forgotten has been said to be "the biggest threat to free speech on the Internet in the coming decade (*Ibidem*)".

In fact, some Spanish newspapers have come to say in a very simplistic way that the enforcement of such right will entail removing information about someone prosecuted, indicted or convicted in many of the corruption cases happened in Spain if requested by the interested.

What is clear is that the different approaches on data privacy in the United States and Europe are based on different political choices.

The approach favoured in the United States is "designed to put the individual in the centre of the action to let him a large voice in decisions as to what information will be collected, used and disseminated about him (Lloyd, 2011)" in a context of flexible, friendly and lenient public policies specifically drafted in favour of big tech companies' which actually are the engine of the Internet.

Since *Griswold v Connecticut*, 381 U.S. 479 (1965), the original idea of privacy in Anglo-American Law has been long engaged with the protection of individuals against government interferences. Conversely, Congress did not extend data privacy requirements to the private sector. Instead, protection of personal data has been governed by voluntary enforceable codes of conduct enforced by the Federal Trade Commission (FTC) together with sectorial privacy laws covering certain information categories (e.g. health, finance, education).

Ultimately, the United States has adopted a policy of "flexible approach" to privacy protection, which seeks to facilitate "innovation" and spur "technologically advanced services (Green Paper of the US Department of Commerce, 2010)." As Friedman J. observed for the District Court of Columbia in *Blumenthal v Drudge and AOL* (1998) when he referred to the immunity granted to online intermediaries for illegal contents published by third parties under the exemption liability regime established by Communications Decency Act of 1996: "In some sort of tacit *quid pro quo* arrangement with the service provider community, Congress has conferred immunity from tort liability as an incentive to Internet service providers to self-police the Internet."

By contrast, in the view of the German Data Protection Commissioner for the Lander of Schleswig-Holstein, "the objective of [European] data protection law is the protection of individuals, not of companies (Weichert, 2013)."

In this sense, European data protection model has taken a more "paternalistic approach" (Lloyd, 2011) which is based on consent as a manifestation of individual control (Tene and Polonetsky, 2012). Albeit strongly linked to privacy, the right to personal data protection is different from the former. Relying on the principles of human dignity and personal liberty, it protects the freedom of an individual to decide for himself whether data concerning his person may be accessed and used by third parties.

Strongly introduced in European constitutional traditions, the rationale behind personal data protection –highlights the Spanish Constitutional Court in its landmark Judgment 292/2000- is "preventing data from being unlawfully and unfairly traded in a harmful way for dignity and fundamental rights of data subject."

After the devastating and terrifying conclusion of the EWHC in the Mosley Case referred above one may wonder whether or not the right to be forgotten -as established by the ECJ in Google decision- is actually the solution.

The ECJ expressed such concern and the rationale behind the right to be forgotten: "Given the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, effective and complete protection of data users could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the publishers of websites." (ECJ, para. 84)

Today, Max Mosley is still litigating against the replication over the Internet of the controversial but intimate images of him. No public interest has been recognised by Courts deciding this issue across different European jurisdictions. Recently, the Hamburg District Court (January 2014) has ordered Google to block all access in the country to such outrageous footage not on grounds of the right to be forgotten, but on grounds of Google liability as an accomplice of interference with intimate sphere of the claimant: "[…] it contributes with the search function offered by willingly and causally to the distribution of likenesses which –as shown – seriously breach the general personality right of the plaintiff (Crossley, 2014)."

The irony of Google Case is this: the Claimant Mr. Costeja wanted the information related to his past judicial proceedings not to be display by Google search engine thus recovering his online anonymity. Nevertheless, the impact of the ECJ ruling on search engines activities echoed by mass media has had the opposite effect: the claimant has gained a far-reaching notoriety, even much more than that notoriety he precisely wanted to avoid when his struggle against Google just started.