THE EU „ RIGHT TO BE FORGOTTEN”

Assistant professor **Andreea SEUCAN**[1]

Abstract

The scientific paper aims at presenting the relevant legal aspects related to data protection in the EU (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) in view of the ruling of the Court of justice of the European Union (C131/12), the content of the judgement of the court, how it has been enforced so far by Google and its impact on EU citizen and future legislation.

Keywords: *ruling, guidelines, reform proposals*

JEL Classification: *K33, K36*

The “Right to be Forgotten” is a concept which has become worldwide famous following the ruling of the Court of Justice of the European Union - C131/12. Nobody could predict its huge impact, although at some point one could imagine that excessive sharing of information on the internet and unrestricted access to it will lead to an attempt by an EU citizen to block the data through a court`s decision.

The story goes back to 2010, when a Spanish citizen complained to the Spanish Data Protection Agency about a situation in connection with a Spanish newspaper, Google Spain and Google Inc. His complaint described the fact that an auction notice of his repossessed home, which was mentioned in a Spanish newspaper, and appeared on Google`s search, even though the proceedings referring to his case were completed, had not been removed and was still to be found in the newspaper and on the internet. This situation infringed his privacy rights. He required the newspaper to erase that reference and Google Spain or Google Inc. to make the necessary adjustments in order to remove his name in connection with the auction notice as a result of Google search. The Director of the Spanish Data Protection Agency rejected the complaint against the newspaper but upheld the complaint against Google Spain and Google Inc., demanding the removal of the links.

Google brought an appeal on the grounds[2] that:

(1) Google Inc., as the provider of the search engine, was not within the scope 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 (1995 Data Protection Directive) and Google Spain, its local subsidiary, was not responsible for the search engine (although it promoted advertising on the service);

(2) there was no processing of personal data in the search function;

(3) even if there was processing, neither Google entity could be regarded as a data controller;

(4) in any event, the data subject had no general right to the removal of lawfully published material.

The Spanish court referred the case to the Court of Justice of the European Union and asked[3]:

(a) whether the EU’s 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 applied to search engines such as Google;

(b) whether EU law (the Directive) applied to Google Spain, given that the company’s data processing server was in the United States;

(c) whether an individual has the right to request that his or her personal data be removed from accessibility via a search engine. Formally, it requested the Court to make the interpretation of

[1] Andreea Seucan - Bucharest University of Economic Studies, Department of Law, andreea.seucan@cig.ase.ro.

[2] Jay, Rosemary, "EU Court of Justice Advocate-General Issues Opinion in Google Search Case". Hunton & Williams LLP, https://www.huntonprivacyblog.com/2013/07/articles/eu-court-of-justice-advocate-general-issues-opinion, accessed on November 20, 2014.

[3] Factsheet on the “Right to be Forgotten” Ruling (C131/12)

Article 2(b)[4] and (d)[5], Article 4(1)(a) and (c) [6], Article 12(b)[7] and subparagraph (a) of the first paragraph of Article 14[8] of 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 and Article 8 of the Charter of Fundamental Rights of the European Union[9].

The legal main instrument for the case has been the above-mentioned 1995 Data Protection Directive, which has its roots in Article 16(1) of Treaty on the Functioning of the European Union (TFEU), as introduced by the Lisbon Treaty, which establishes the principle of the protection of personal data. With Article 16(2) TFEU, the Lisbon Treaty introduced a specific legal ground for the adoption of rules on the protection of personal data. Article 8 of the Charter of Fundamental Rights of the EU states the protection of personal data as a fundamental right.

The 1995 Data Protection Directive protects the fundamental rights and freedoms of natural persons in connection with processing of personal data, while trying to ensure an obstacle-free movement of that data. It states in Art. 1 that Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. The directive protects only the rights of natural persons.

Art. 2 explains the meaning of several concepts, among them "personal data" and "data subject": any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, 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.

According to Art. 3 (1), it relates 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. Article 3 (2) mentions that the Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law and in any case to processing operations concerning public security, defence, state security (including the economic well-being of the State when the processing operation relates to state security matters) and the activities of the State in areas of criminal law,

[4] Article 2(b) 'processing of personal data' ('processing') shall mean 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;

[5] Article 2(d) 'controller' shall mean 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; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

[6] Article 4-1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; 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;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

[7] Article 12: Member States shall guarantee every data subject the right to obtain from the controller:

(b) 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;

[8] Article 14-1:Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

[9] Art. 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.

- by a natural person in the course of a purely personal or household activity.

Article 6 points out the obligations of the Member States in relation with personal data of the natural persons: personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(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;

(e) 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. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

In the case of the "Right to be Forgotten", the most important provision is to be found in Article 12 ("The right of access") which provides that Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) 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;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

The Directive provides in Art. 13 the exemptions and restrictions:

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research

or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

Art.14 explains the data`s subject to object: Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

The Directive describes in Article 28 the role of the national supervisory authority, which monitors, as an independent organism, the enforcement of the local legislation adopted according to the provisions of the Directive[10]. In Romania the Directive has been transposed into national legislation through Law No.677/2001 and the national supervisory authority is The National Supervisory Authority for Personal Data Processing.

The Court of Justice of the European Union decided that Google, as a search engine, is a controller of personal data and, as such, is bound to apply the provisions of the Directive, like any other search engine. Even though Google has its seat in a non-Member State, it operates through Google Spain, which is an establishment created to represent Google`s economic interest in a specific territory. A natural person can request that specific information about her/him be removed from public access if the data appears inaccurate, inadequate, irrelevant or no longer relevant or excessive. The aim is to achieve a fair balance between the legitimate interest of the internet users potentially interested in having access to specific information and the natural person`s fundamental rights, in particular the right to privacy and the right to protection of personal data. The Court indicates that an important criterion to be taken into consideration is if the natural person is part of public life or not.

---

[10] Article 28. Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

The decision to erase the data belongs to the controller, which must examine all the aspects of the requests, on a case-by-case basis. If the controller denies the erasure, the person can bring the matter to higher jurisdiction.

As a result of the ruling of the Court, Google proceeded to the erasure of the auction notice of the Spanish citizen, although some news agencies claim that the notice does no longer appear if you type the name of the Spanish citizen, but you will still be able to find it if you use words from the notice as search criterion.

Google has also set a webform to be filled for those persons who want to have their data removed. Currently[11], Google`s team has received about 170,000 requests to erase data related to them, and has evaluated for removal over 580,000 links. So far, about 42 % of the requests have been granted, while about 58 % were denied by the team, which makes the analyses on a case-by-case basis[12]. The problem Google has is the fact that it does not want to take by itself the decision about what is to be kept and what is to be erased and, as such, is waiting for new regulation which should make the decision easier.

Since the Court`s decision (29 May 2014), concerning Romania, Google has received 3,085 requests demanding 11,870 links to be removed. 74,1% of the designated links have been erased.

One concern[13] lies in the fact that the links weren't removed from the main.com domain, which provides worldwide coverage. Google decided not to do it because it considers that other courts in other parts of the world would never have decided similarly to the Court of Justice of the European Union. The links to be removed are those from all 28 EU member states, as well as from Iceland, Liechtenstein, Norway and Switzerland, countries belonging to the European Free Trade Association (EFTA). Another highlighted issue is Google's practice of telling a site's webmaster that a link to their site was removed from the search results, without telling them why. In this case, Google claims that the removal of a link can result in less traffic for a site and, as such, it feels obliged to alert the owner[14].

An important body in which the legal consequences of the court`s decision are being discussed is The Article 29 Data Protection Working Party, which was set up under the 1995 Directive. The Article 29 Working Party (WP29), which represents the national data protection authorities, is planning to provide in the near future common guidelines for dealing with right-to-be-forgotten requests.

In our opinion, alongside with the criterion related to the connection of the individual to public life, it could be useful to make the analysis by taking into consideration the timeframe of the data, meaning how much time should the information be made available (for example for criminal records) or its offensive or non-offensive character.

The European Commission has set in 2012 a 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) (replacing Directive 95/46/EC), setting out a general EU framework for data protection, and for a Directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities (Data Protection Directive). The choice to have a regulation was given by the fact that, as opposed to a directive, a regulation is to be applied in its full content by Member States and should insure uniform application of the legal rules.

When announcing the regulations in 2012, Viviane Reding, the European Commission's vice-president, said: "It is clear that the right to be forgotten cannot amount to a right of the total erasure of history."

---

[11] November 2014

[12] Google. Transparency Report - https://www.google.com/transparencyreport/removals/europeprivacy/, accessed on November 20, 2014.

[13] Loek Essers, This is how Google is dealing with 'right to be forgotten' requests, http://www.pcworld.com/article/2850072/this-is-how-google-is-dealing-with-right-to-be-forgotten-requests.html, accessed on November 20, 2014.

[14] Loek Essers, op. cit., accessed on November 20, 2014.

The reform proposed several innovations[15]:

- One continent, one law: one legislation for all EU member states.
- One-shop-stop: companies will approach one single supervisory authority at EU level
- Similar rules for all companies (doing business on the Single Market) - regardless of their headquarters/establishment
- The right to be forgotten: if there are no legitimate grounds for retaining the data, an individual can ask the data to be erased.
- Easier access to own data: a right to data portability, which means the possibility to transfer data between service providers
- Possibility to control: the need for explicit consent of the individual in order to process the data
- Data protection first: data protection safeguards should be built into products from the creation and privacy-friendly default settings should be the norm.

The proposed General Data Protection Regulation continues to have in view the processing of personal data of natural persons. Article 3 explains its territorial scope, showing that it applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, but also to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behavior. Article 4 contains definitions of the terms used. The Regulation introduces new terms like, for example, "personal data breach".

According to Article 7 (1), the controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. This provision means that it shall no longer be necessary for the data subject (the plaintiff) to prove that data must be erased, but to the controller (the defendant) that it is relevant and must be kept. This is an important change of legislation.

According to Article 12 (2), the controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise requested by the data subject.

Article 17 provides the data subject`s right to be forgotten and to erasure, including the obligation of the controller which has made the personal data public to inform third parties on the data subject`s request to erase the data.

Article 35 introduces a mandatory data protection officer for the public sector and, in the private sector, for large enterprises.

Article 53, which provides extended powers for the national supervisory authority, includes also the power to sanction administrative offences.

Section 3 Articles 64-72 aims to upgrade the Article 29 Working Party to an independent European Data Protection Board to improve its contribution to consistent application of data protection law and to provide a strong basis for cooperation among data protection authorities, including the European Data Protection Supervisor.

According to Article 79, data protection authorities are allowed to impose fines of up to 2% of annual worldwide turnover where companies do not respect the rights of citizens, such as the right to be forgotten.

[15] European Commission Memo, Progress on EU data protection reform now irreversible following European Parliament vote, Strasbourg, 12 March 2014.

Article 80 of the proposed Regulation includes a specific clause which obliges Member States to pass national legislation to reconcile data protection with the right to freedom of expression, including the processing of data for journalistic purposes.

The limitations to the right to be forgotten, to be found in Article 83, are in connection with the reasons of public interest that would justify keeping data online. These include the exercise of the right of freedom of expression, the interests of public health as well as cases in which data is processed for historical, statistical and scientific purposes.

The Parliament of the European Union has approved the proposal for new legislation, but it made changes to the initial text. As regards Article 79, it has proposed that the data protection authorities be able to impose fines up to 5% of the annual worldwide turnover of a company (up from 2% in the Commission`s proposal). It also strengthens the right to be forgotten by allowing EU citizens to obtain from third parties (who also have the data) the removal of any links to, or copy or replication of that data.

The Council of the European Union has proposed amendments to Chapter IV ("Controller and Processor") as it relates to compliance obligations of data controllers and data processors. As such, privacy impact assessments will only be required for processing activities likely to involve high risk to the rights and freedoms of individuals (such as discrimination, identity theft, fraud, or financial loss). Only processing which would point out a high degree of risk would require prior consulting of the data authority before the beginning of the processing activities. The appointment of a data protection officer must be voluntary unless the national law of the relevant member state provides otherwise.

The latest developments in the field of the right to be forgotten underline the importance of reaching a legal balance between the need to know (and to grow) and the need to protect. The recent ruling of the Court is a clear sign that even though one can not escape personal history, at least in the public eye there is the possibility of redemption.

Judgment of the Court (Grand Chamber) of 13 May 2014 (operative part) (C121/12)

1. 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' when that information contains personal data and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing.

2. 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, within the meaning of that provision, 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.

3. In order to comply with the rights laid down in those provisions and in so far as the conditions laid down by those provisions are in fact satisfied, 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.

4. When appraising the conditions for the application of those provisions, it should inter alia be examined whether the data subject has a right that the information in question 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, without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject. As the data subject may, in the light of his fundamental rights under Articles 7[16] and 8 of the Charter,

[16] Article 7: Respect for private and family life: Everyone has the right to respect for his or her private and family life, home and communications.

request that the information in question no longer be made available to the general public on account of its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that 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.

Bibliography

1. Jay, Rosemary, "EU Court of Justice Advocate-General Issues Opinion in Google Search Case". Hunton & Williams LLP, https://www.huntonprivacyblog.com/2013/07/articles/eu-court-of-justice-advocate-general-issues-opinion, accessed on November 20, 2014
2. The ruling of the Court of Justice of the European Union - C131/12, www.curia.eu.
3. 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 (1995 Data Protection Directive), Official Journal L 281 , 23/11/1995
4. European Commission Memo, Progress on EU data protection reform now irreversible following European Parliament vote, Strasbourg, 12 March 2014
5. Google. Transparency Report - https://www.google.com/transparencyreport/removals/europeprivacy/, accessed on November 20, 2014
6. Loek Essers, This is how Google is dealing with 'right to be forgotten' requests, http://www.pcworld.com/article/2850072/this-is-how-google-is-dealing-with-right-to-be-forgotten-requests.html, accessed on November 20, 2014