CHALLENGES OF REGULATING A RIGHT TO BE FORGOTTEN WITH PARTICULAR REFERENCE TO FACEBOOK

by

ANDRA GIURGIU*

This paper seeks to analyse the right to be forgotten that has been officially introduced by the European Commission on the 25th of January 2012. By discussing the origins and legal grounds of this right, the article will argue that the right to be forgotten is merely a re-branding of long-standing data protection principles. Furthermore it will present the different views according to which the right to be forgotten means the deletion of data in due time or the right to a clean slate, before pointing out to the implications it may have on social networking sites like Facebook. Here it will draw attention to Facebook's noncompliance with the purpose specification principle as well as to the legal uncertainties in identifying the controller on Facebook. Finally the paper will look at the problems regarding the practicability of the right to be forgotten, supporting the opinion that enforceability can only be assured through the combination of legal and technical measures, before concluding to the questionability of its successful enforcement due to the European-American clash with regard to privacy.

KEYWORDS

privacy, right to be forgotten, Facebook, de-contextualization, chilling effect, privacy by design, expiration dates

1. INTRODUCTION

In an era in which storing digital information has become much cheaper than deleting it, whilst personal data is regarded as being the new currency

* andra.giurgiu@ulbsibiu.ro / andra.giurgiu@gmail.com
PhD student at Lucian Blaga University, Faculty of Law, Sibiu, Romania, Lawyer and Legal translator.

on the Internet[1], there is no wonder that people grow more and more concerned when it comes to protecting their privacy.

From the "right to be let alone", as it was initially brought forward by the famous American lawyers Warren and Brandais[2], the concept of privacy developed to the extent that it included the individual's right to self-determination[3], understood as a right to construct, control and organize one's private life according to one's own wishes and conceptions.

In a digitalized world however, where we buy our clothes and pay our bills over the Internet, relying on it for the satisfaction of our daily needs, our secret wishes or simply for keeping up the illusion of not being alone through online chats with friends, acquaintances or even with strangers, the amount of information we put out there about ourselves is enormous. The digital reflection of our personality, the digital traces we are leaving every day have grown to become a threat to our future development.

A worrying evolution of social relations with regard to people's right to privacy and data protection is social networking. There is nothing new about your future employer looking you up on the Internet and stumbling upon photos of you on Facebook in which you act anything but professional and thus refusing you the chance of a job you have so eagerly wanted. This is one of the most feared scenarios among individuals and it is anything but unreasonable as the *Drunken Pirate case*[4] demonstrates.

The main problem relies in the fact that the rapidly changing societal model has not allowed for legal norms to catch up, just yet. The Data Protection Directive[5] was adopted at times when technology was less evolved and the flow of personal information significantly lower. Nowadays, widespread data storage and data mining pose serious threats to the individual's

---

1 Ausloos, J. 2012, The „Right to be Forgotten – Worth Remembering?", *Computer Law and Security Review*, vol. 28, no. 2, pp. 143-152.

2 Warren, S. D., Brandeis, L. D. 1890, "The Right to Privacy", *Harvard Law Review* vol. 4, no. 5, pp. 193-220.

3 Hornung, G., Schnabel, C. 2009, „Data protection in Germany I: The population census decision and the right to informational self-determination", *Computer Law and Security Review*, vol. 25, no. 1, pp. 84-88.

4 This is the case of Stacy Snyder, an aspiring teacher who was denied her teaching certificate because of an online photo that showed her in costume wearing a pirate's hat and drinking from a plastic cup. The university administration considered it to be improper and unprofessional behaviour for a teacher thus refusing her the teaching certificate. Removing the photo was no option to repare the damage as it has been catalogued by search engines and achieved by web crawlers. This case is very well described by Mayer-Schönberger, V. 2009, *Delete. The Virtue of Forgetting in the Digital Age*, Princeton and Oxford, pp. 1-2.

5 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 (Data Protection Directive), O.J. L 281, 23.11.1995, pp. 0031-0050.

rights to privacy and data protection and the directive seems especially outdated when it comes to protecting these rights in the online environment.

European regulators have long understood the need for adaptation and there have been many discussions around a new European framework for protecting people's privacy. These have resulted in the Commission's Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data, also known as General Data Protection Regulation[6], which was officially released on the 25th of January 2012. Among other novelties the proposed regulation intends to strengthen individuals' rights by introducing a so-called "right to be forgotten"[7]. According to Viviane Reding the right to be forgotten is intended to cope with privacy risks online by empowering individuals to control their own identity in the online environment. Thus, "If an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system"[8]. Although welcomed, regulating a right to be forgotten is easier said than done.

In the following the article will present an overview of this right, with regard to its origins, its legal grounds and the different conceptions about it, before proceeding to a further analysis of the meaning and impact of the right to be forgotten with regard to social networks, more specifically to Facebook.

2. DANGERS OF THE INFORMATION SOCIETY

As Victor Mayer-Schönberger eloquently points out, in the digital age the balance has shifted from forgetting as a norm to the default of remembering due to cheap storage, easy retrieval and the global reach of information through global digital networks; in other words, "Today, forgetting has become costly and difficult, while remembering is inexpensive and easy"[9].

---

[6] 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) 11 final, Brussels, 25.01.2012, viewed 14.07.2012, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF>.

[7] Art. 17 of the General Data Protection Regulation COM(2012) 11 final.

[8] Speech Reding, V., The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, Innovation Conference Digital, Life, Design, Munich, 22 January 2012.

[9] Mayer-Schönberger, V. 2009, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton and Oxford, pp. 62-92.

This social phenomenon has resulted in the accumulation of more and more personal data risking to be misused. Digitalization is said to have a "chilling effect" (Mayer-Schönberger, 2009, p. 12) on the individual's present actions. His freedom of expression and the right to self-development are threatened by constant auto-censorship for fear of future negative consequences.

Another major risk recognized in the build-up of personal data is that of de-contextualization of information. Mayer-Schönberger (2009, p. 89) speaks of the dangers of de- and re-contextualization of digital information escaping the control of the original creator when describing the phenomenon of rearrangement and redistribution of Michael Wesch's video Web 2.0. The term is also used by Dumortier with regard to Facebook "to conceptualize what happens when behaviours or information are used in a context other than that for which they were intended."[10] This represents a major risk on a social networking site (SNS) like Facebook that requires individuals to provide real name and information when registering. According to Facebook's Statement of Rights and Responsibilities', Section 4 Registration and Account Security, "Facebook users provide their real names and information"[11]. A recent practice of the social networking site was asking other users whether their friends use the account under their real names or not[12].

The interdiction of using pseudonyms as well as the verification of the real identities of users by asking friends to confirm it seems especially questionable with regard to people's right to privacy and personal data protection. According to Article 29 WP[13] "SNS should consider carefully if they can justify forcing their users to act under their real identity rather than under a pseudonym. There are strong arguments in favor of giving users choice in this respect and in at least one Member State, this is a legal requirement. The arguments are particularly strong in the case of SNS with wide membership." This is especially the case of Facebook with millions of members worldwide.

---

[10] Dumortier, F. 2010, "Facebook and Risks of "De-contextualization" of Information", in Gutwirth, S., Poullet, Y. & De Hert, P, *Data Protection in a Profiled World*, Springer, pp. 119-137.

[11] http://www.facebook.com/legal/terms, viewed 17.07.2012.

[12] Smith, H. 2011, *Facebook 'to ask users to identify friends as security measure'*, viewed 22.07.2012, <http://www.metro.co.uk/tech/853846-facebook-to-ask-users-to-identify-friends-as-security-measure>.

[13] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, WP 163, 12.06.2009, viewed 23.07.2012, <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf>.

The site connects the "virtual bodies" of their members with their "real-world" correspondents using "real world identification signs" such as pictures, videos, and other such communication forms (Dumortier, 2009) so that for the avarage Facebook member who uses the site more than once every day this means leaving an endlessly long digital trail. Deleting this trail, or even just parts and bits of it, becomes therefore extremely difficult.

3. ORIGINS AND LEGAL GROUND OF THE RIGHT TO BE FORGOTTEN

3.1 ORIGINS

As regards the origins of the right to be forgotten, the dominant opinion is that advocating for its development from the right to privacy[14]. The right to be forgotten is said to rely on the collection limitation principle, the purpose specification principle and the use limitation principle as set down in the Data Protection Directive.

There are however voices linking it not to the right to privacy but to the right to identity[15]. Andrade (2012) is sharing Gutwirth's view that "it is very doubtful that such a 'right to be forgotten' could be construed as a spin off of the right to privacy, since most of the time conflicts concern public facts (for instance, persons involved as victims or as witnesses of a crime) that are not protected by privacy rights"[16].

There is also the proprietary approach to privacy[17] according to which one is the owner of his personal data thus having a certain control right over it. The right to be forgotten is said to be taking this approach as it allows individuals to decide what happens with the information and to maintain control after disclosure (Ausloos, 2012). The proprietary approach is therefore considered to be more effective as it gives individuals affirmative rights without the need to demonstrate harm. Moreover the "erga omnes"

---

[14] Bernal, 2011, Wong, 2008, Dumortier 2009, Rosen, 2012, Castellano 2012, Weber, 2011 etc.

[15] Andrade, N. N. G. 2012, "Oblivion: The Right to be Different from Oneself – Reproposing the Right to be Forgotten, VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet, Revista de Internet, Derecho y Política, no. 13, pp. 122-137, viewed 05.07.2012, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2033155>.

[16] Gutwirth, S. 2009, "Beyond identity?", *Identity in the Information Society*, vol. 1, no. 1, pp. 122-133.

[17] Purtova, N. 2010, "Property in personal data: Second life of an old idea in the age of cloud computing, chain informatisation, and ambient intelligence", in Gutwirth, S., Poullet, Y., De Hert, P. & Leenes, R. (eds.), *Computers, Privacy and Data Protection: an Element of Choice*, Springer, Dordrecht, Heidelberg, London and New York, pp. 39-64.

effect containing a general obligation of refraining from any action that could impede on the subject's right to property over his data would be better suited for the enforcement of the right to be forgotten[18].

3.2 LEGAL GROUNDS

The right to be forgotten is said to be a new right that was introduced for the first time by the proposed Data Protection Regulation. This paper argues however in favour of the fact that it is a mere re-branding of long standing data protection rules. To support this argument we would like to point out to the Data Protection Directive which, under the title "Right of access"[19], grants data subjects' the right of rectification, erasure or blocking. The Directive refers to processing operations, which do not comply with its provisions, "in particular because of the incomplete or inaccurate nature of the data". The lack of compliance can also result from violations of the general rules on the lawfulness of the processing, including the infringement of the principles relating to data quality as stated in article 6 of the Directive, of the criteria for legitimate data processing listed in article 7 as well as of the conditions for processing special categories of data.

The proposed regulation for data protection refers in article 17 to the right to be forgotten and the right to erasure. The text of the provision speaks however only of the right to erasure, which is granted to data subjects in four cases:

a. When the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b. When the data subject withdraws consent on which the processing is based or when the storage period consented to has expired, and where there is no legal ground for the processing of the data;
c. When the data subject objects to the processing; and
d. When the processing does not comply with the Regulation for other reasons.

By comparing these provisions to the ones from the current Data Protection Directive one may find the sole reaffirmation of long standing data protection principles such as the purpose limitation principle, the principle of

[18] Koops, B.-J. 2011, „Forgetting Footprints, Shunning Shadows. A critical analysis of the „Right to be Forgotten" in Big Data Practice", SCRIPTed, vol. 8, no. 3, pp. 229-256, viewed 05.07.2012, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986719>.

[19] Article 12 (b) of the Data Protection Directive.

lawful processing based on the subject's consent and his right to object. So far, apparently nothing new.

The Regulation introduces however a provision that obliges the controller, if he has made the above mentioned data public, "to take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing the data, that a data subject requests them to erase any links to, or copy or replication of that personal data"[20]. This is actually the key provision when relating to the right to be forgotten. In its current form however an actual right to delete, respectively to be forgotten is not contained. For that we have to look back at the draft Regulation from November 2011. There it is stated that "Where the controller […] has made the data public, it shall in particular ensure the erasure of any public Internet link to, copy of, or replication of the personal data relating to the data subject contained in any publicly available communication service which allows or facilitates the search of or access to this personal data"[21].

By comparing the two provisions it becomes clear that the officially released proposal contains merely an obligation to inform third parties about the request of erasure whereas it is the older version, which actually contains a true right to be forgotten.

The infeasibility of an obligation on behalf of the controller to ensure the erasure of any public reference to the personal data must have struck the European legislator so that he has reviewed his position in the officially released document. This European Data Protection Supervisor, Peter Hustinx, also recognizes the more realistic nature of the obligation of endeavour contained in article 17 rather than the initial obligation of result[22].

4 WHAT IS THE RIGHT TO BE FORGOTTEN?

4.1 PERSPECTIVES ON THE RIGHT TO BE FORGOTTEN

Although many references have been made to the right to be forgotten, it is still unclear what it means, in which conditions it can be invoked and against whom. The doctrine seems to distinguish between two different conceptions regarding this right: the deletion of data in due time and the

[20] Article 17 General Data Protection Regulation COM(2012) 11 final.

[21] Article 15 parag. 2 General Data Protection Regulation COM(2011) Version 56.

[22] Hustinx, P., European Data Protection Supervisor, Opinion on the data protection reform package, Brussels, 7.03.2012.

clean slate vision. The latter can be again subdivided in a perspective that outdated personal data should not be used against people and an individual self-development perspective (Koops, 2011).

The right to have data deleted in due time might mean according to Koops (2011) the deletion after use, when no longer relevant, when an expiry date elapses or when the drawbacks of retention start outweighing the advantages. He too shares the opinion that in this form the right to be forgotten seems to already be part of the current data protection framework, by granting subjects the right to have personal data deleted when they are no longer relevant, accurate, or following a justified objection.

The perspective of a claim on a clean slate may be traced back to the French law's "*droit a l'oubli*", where it has the meaning of "the right to silence on past events in life that are no longer occurring"[23]. It is based on the individual's right to claim that outdated negative information is not used against him (Koops, 2011). In this manner it is usually linked to the interest of criminal offenders not to be confronted with negative information from the past. From this perspective, the right to be forgotten seems to function like a period of prescription.

By citing Rouvroy, Koops (2011) refers to the self-development perspective of the right to be forgotten and describes it as "a right to speak and write freely, without fear of your person(ality) being fixed by what you express; it implies the sense of liberty of writing today and being able to change your mind tomorrow". According to Koops (2011) the right to be forgotten would imply from this perspective "the sense of liberty of expressing yourself freely in the here and now without fear that this might be used against you in the future."

Also from the self-development perspective, Andrade (2012) links the right to be forgotten not to the right to privacy but to the right to identity, when speaking of the right to oblivion as "the right to be different from others, but also the right to be different from oneself, namely from one's past self." Other authors also see the right to be forgotten from the clean slate perspective, from which it tries to ensure the privacy of individuals by allowing them to escape the constant persecution of the past[24].

---

[23] Bernal, P.A. 2011, "A Right to Delete?", *European Journal of Law and Technology*, vol. 2, no.2, viewed 24.07.2012, <http://ejlt.org//article/view/75/144>.

[24] Castellano, P.S. 2012, „The right to be forgotten under European Law: a Constitutional debate", *Lex Electronica*, vol. 16, no.1, viewed 03.07.2012, <http://www.lex-electronica.org/docs/articles_300.pdf>.

4.2 DIFFERENT OFFICIAL VIEWS

There is anything but a unitary vision regarding this right. According to Viviane Reding herself this is not a new right but "builds on already existing rules which are unfortunately not clear, nor adapted to the Internet age"[25]. In her view the right to be forgotten seems to apply only to the online environment in situations where people have given out that personal information themselves[26].

The existence of the right to be forgotten in the actual data protection framework is also recognized by the European Digital Rights organization, EDRi. The organization expresses however its concerns about the fact that the right to be forgotten has not been respected. It considers that the proper analysis of the causes for the lack of compliance and the effective implementation of the principle of "privacy by design" are the key for future respect of the right to be forgotten[27].

The European Data protection Supervisor sees the right to be forgotten as a strengthened right of erasure which would allow for a better enforcement in the digital environment but questions its effectivity and enforceability[28].

The Article 29 Working Party also welcomes the strengthening of the right to erasure but it too questions the effectiveness of the right to be forgotten in its current form[29].

From the official standpoint the right to be forgotten is mainly seen as a strengthening of individuals' rights in order to enable them to protect their privacy in the online environment better. In this context we feel that it is of particular interest to examine its impact on social networks. However, due

---

[25] Speech Reding, V. 2012, The importance of strong data protection rules for growth and competitiveness, London, 1 March, viewed 05.07.2012, <http://europa.eu/rapid/press-ReleasesAction.do?reference=SPEECH/12/171&format=HTML&aged=0&language=EN &guiLanguage=en>.

[26] „If an individual wants to take its data off a service – the data the individual had put on the service – he should be capable of doing so. People will be able to erase the data they have given out if there are no legitimate grounds for retaining it." Speech Reding, V. 2012, The EU Data Protection Reform 2012: Safeguarding Privacy in a Connected World, Brussels, 25 January, viewed 24.07.2012, <http://ec.europa.eu/commission_2010-2014/reding/pdf/ speeches/ data-protection -reform2012_en.pdf>.

[27] EDRi response to EC consultation on the review of the Data Protection Directive, 15.01.2011, viewed 20.07.2012, <http://www.edri.org/files/20110115_EDRi_data_protection_final.pdf>.

[28] Hustinx, P., European Data Protection Supervisor, Opinion on the data protection reform package, Brussels, 7.03.2012.

[29] Article 29 Data Protection Working Party, Opinion 01/2012 on the data protection reform proposals, WP 191, 23.03.2012, viewed 04.07.2012, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf>.

to the variety of social networking sites (SNS) and their different ways of functioning, we would like to concentrate on Facebook as it is the one with the greatest social impact because of its widespread worldwide usage. According to a recent article, Facebook is supposed to have surpassed 900 million active users in 2012[30].

5. THE RIGHT TO BE FORGOTTEN AND FACEBOOK

5.1 FACEBOOK AND THE PURPOSE SPECIFICATION PRINCIPLE

One of the core principles of data protection is that of lawful processing based on the consent of the data subject. This is the legal ground for collecting and processing personal data by social networks, including Facebook. By signing up to Facebook the subject agrees to the terms and conditions of the company, including to its data use policy with regard to the processing of personal data.

However, according to the purpose specification principle personal data shall be collected for specified, lawful and/or legitimate reasons and not be subsequently processed in ways that are incompatible with those purposes. The main problem with Facebook as with other social networks is the fact that the purpose of the data collection and processing is either not clear, or too broadly formulated[31]. According to Facebook, its mission is "to give people the power to share and make the world more open and connected"[32]. But the purpose of connecting people is far too broad to correspond to the purpose specification principle. According to the proposed regulation the data subject has the right to obtain from the controller the erasure of his personal data "when the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed"[33].

Moreover Facebook's data use policy states "We store data for as long as it is necessary to provide products and services to you and others, including those described above. Typically, information associated with your account will be kept until your account is deleted. For certain categories of data, we may also tell you about specific data retention practices".

---

[30] Goldman, D. 2012, „Facebook tops 900 million users", viewed 27.07.2012, <http://money.cnn.com/2012/04/23/technology/facebook-q1/index.htm>.

[31] Karg, M., Fahl, C, 2011, „Rechtsgrundlagen für den Datenschutz in sozialen Netzwerken", *Kommunikation und Recht*, vol. 7-8, pp. 453-458.

[32] http://www.facebook.com/facebook/info, viewed 27.07.2012.

[33] Article 17 (a) General Data Protection Regulation COM(2012) 11 final.

Koops (2011) recognizes the danger of "Big Data" which "implies that data processing is based on vague purpose definition to allow unforeseen future uses, and that the data are increasingly used for secondary purposes". In that he sees a challenge to the purpose limitation principle and to the effectiveness of the right to be forgotten.

Having in mind the above mentioned about the neglection of the purpose specification principle by Facebook, it appears very unlikely for the right to be forgotten to be effectively enforced on the grounds of article 17(a) of the proposed regulation when the data is no longer necessary in relation to the purposes for which they were collected or otherwise processed.

5.2 WHO IS DATA CONTROLLER ON FACEBOOK?

Another problem with Facebook is determining against whom the right to be forgotten is enforceable. In order to solve that problem one has to turn to the concept of "controller".

According to the regulation "controller means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data".[34]

Analysing this concept in the cases of social network services, Article 29 Working Party distinguishes between 3 types of controllers: the SNS providers, the application providers and the users.

As data controller, Facebook provides the "means for the processing of user data" as well as the "basic services related to user management" and also determines "the use that may be made of user data for advertising and marketing purposes – including advertising provided by third parties"[35].

When an individual posts a picture of himself on Facebook, the SNS has the role of a controller and the user is the data subject. The right to be forgotten by deletion of the photo is uncontroversial in this situation as Facebook allows for the user himself to take down the post at any given time. A problem may arise however if the photo has in the meanwhile been copied or reposted by a "friend". Koops (2011) clearly distinguishes between "digital footprints", as data created by users themselves, and "data shadows", as data generated about users by others.

---

[34] Art. 4(5) General Data Protection Regulation COM(2012) 11 final.

[35] Art. 29 WP Opinion 5/2009 on online social networking.

In the case of "data shadows", when the photo has been copied and reposted, the user has the first option of requesting the deletion from the friend himself, who is the primary data controller. Should he refuse, the user could turn to Facebook, who also takes the position of a data controller, and ask it to take down the photo. The question remains however if Facebook is entitled to take down a photo against the consent of the person who posted it, in this case the friend who copied/reposted the deleted photo. Such a post could be protected by the right to freedom of expression, so that the data subject would have to prove an infringement to his right to privacy and there would be a need to strike a balance between the friend's right to freedom of expression and the data subjects' right to privacy. Even if the user's takedown request is successful, the drawback of the right to be forgotten is that it has effect only for the future.

According to Art. 29 WP application providers may also act as controllers "if they develop applications which run in addition to the ones from the SNS and users decide to use that application"[36].

A different category of data controllers is formed by the users themselves as indicated in the example above. Although in the majority of cases they act as data subjects, there are situations when they take the position of a data controller. It has been generally argued that individuals who process personal data of others on social networks act as data controllers. They are however usually covered by the "household exemption", the processing being considered to be taking place "in the cause of a purely personal or household activity" of a natural person[37]. The scope of this exemption set down in the Data Protection Directive has been narrowed by the proposed regulation, which speaks of processing of personal data "by a natural person without any gainful interest in the course of its own exclusively personal or household activity"[38], emphasizing the unprofitable character of the activity.

According to Article 29 Working Party (Opinion 5/2009) the exemption does however not apply if someone uses Facebook as a collaboration plattform for an association or a company and acts on their behalf or for the purpose of advancing commercial, political or charitable goals. In these cases

[36] Art. 29 WP Opinion 5/2009 on online social networking.
[37] Article 3 (1) Data Protection Directive.
[38] Article 2 (2) (d) General Data Protection Regulation.

the user is considered to act as a controller and therefore needs consent or some other legitimate grounds for the processing.

A high number of contacts would also make the household exemption non applicable[39], access to profile information being a key element with regard to the application of the household exemption. It is considered by the Article 29 WP (Opinion 5/2009) that "when access to a profile is provided to all members within a SNS or the data is indexable by search engines, access goes beyond the personal or household sphere" resulting in the application of the same legal regime as when any person uses technology platforms to publish personal data on the web.

Even if the household exemption fails to apply, the user may still be protected by the exemption for journalistic purposes, artistic or literary expression and a balance has to be struck between the right to privacy and freedom of expression.

Other exceptions to the right to be forgotten and to erasure set down in the proposed regulation regard reasons of public interest in the area of public health, historical, statistical and scientific purposes, legal data protection obligations and cases when the data processing is restricted[40].

As the Article 29 WP has already stressed out (Opinion 5/2009 on online social networking) access and rectification rights, including the right to be forgotten, are not limited to the users of the SNS. Accordingly non-members must also have a means to exercise their right of access, correction and deletion.

There are many situations when Facebook users "tag" a non-member on a photo they post or link them to a specific location like a city, restaurant or bar using location services. One of the main problems is the fact that the person being tagged is not even aware of that action, thus not even realizing the disclosure of his/her personal data.

Moreover through Facebook's "Like-button" data sets can be created about people who are not members of Facebook based on their browsing behaviour. Even more worrying is the fact that the simple existence of the "Like-button" on a certain web page allows Facebook to place cookies and to track the web user, regardless of whether he actually uses the button or not, and that the database thus created can be later linked to the individual'-

[39] Art. 29 WP Opinion 5/2009 on online social networking.

[40] Art. 17 (3) General Data Protection Regulation COM(2012) 11 final.

s newly created Facebook profile, should he decide to join the network[41]. The data collection through the "Like-button" takes place in the absence of any consent from Facebook non-members and, as Roosendaal eloquently (2012) points out, one cannot assume that non-members have agreed to being subject of the collection by the mere use of the Internet. Moreover there is no specified purpose for the collection of the data. As a non-member of Facebook the data subject has no possibility to exercise his right to access and rectification and thus obtain the deletion of his personal data.

6. PRACTICALITY AND ENFORCEABILITY OF THE RIGHT TO BE FORGOTTEN

6.1 THE NEED FOR A TECHNICAL APPROACH

Even if one disregards the existing doctrinal controversies over the different approaches to the right to be forgotten, one directly stumbles across the problems regarding its enforceability. In order for it to be effective, there is need for a combination between legal and technical regulatory measures (Koops, 2011). The legal provisions comprised in the proposed regulation have been already analysed above. But the right to be forgotten needs to be strengthened by appropriate technical measures.

The Commission itself recognized the need to set out obligations for data controllers in form of technical and organizational measures in the design and operation of ICT according to the principles of privacy by design and privacy by default[42]. Although having been around for about twenty-five years, PETs as means of enhancing privacy or control, have proved to be quite unsuccessful due to weak consumer demand, high implementation costs and the fact that online advertising enable firms to make huge profits based on the collection, analysis and sharing of consumer data[43].

Mayer-Schönberger (2009, p. 171), sees a possible solution[44] to the problem of digital remembering in the introduction of expiration dates, under

[41] Roseendaal, A. 2012, „We Are All Connected to Facebook...by Facebook!", in Gutwirth, S., Poullet, Y., De Hert, P. & Leenes, R. (eds.), *European Data Protection: In Good Health?*, Springer, Dordrecht, Heidelberg, London and New York, pp. 3-19.

[42] Art. 23 General Data Protection Regulation COM(2012) 11 final.

[43] For the difference between PETs and privacy by design and their classification see Rubinstein, I. S., 2011, „Regulating Privacy by Design", in Berkley Technology Law Journal, vol. 26, no. 3, pp. 1409-1455.

[44] Other solutions he discusses are digital abstinence, information privacy rights empowering people to maintain digital control, a digital privacy rights infrastructure based on the principle of digital rights management, cognitive adjustment, information ecology and perfect contextualization. Mayer-Schönberger, 2009, pp. 128-168.

the form of meta-information associated with a piece of information, which would be determined by the subjects and thus allow for automatic deletion of the information. In his book he even proposed the solution of negotiating expiration dates between transactional parties (2009, p. 185).

Andrade (2012) has pointed out to already existing initiatives in this direction such as the software Vanish, that enabled users to control the "lifetime" of any kind of data stored in the cloud, including information on Facebook[45]. Another possible approach is seen in the German start-up-X-pire which developed software that enables users to attach expiry dates to digital content [46], including to images uploaded to Facebook.

Other possible ways of "being forgotten" by the Internet have been seen in newly developed services to bury information (Weber, 2011) so that the retrieval becomes extremely difficult, if not impossible. This is considered to be an option to the actual deletion of the information. There are also companies specializing in online reputation management like reputation.com whose task it is to make people and businesses look their best on the Internet.

Dumortier (2009) suggests increasing the responsibility of operators of SNS like Facebook by making them accountable for the design of the site. He proposes that European authorities demand Facebook to adapt the architecture of the site according to the user's interests in order to limit the data collection according to a more specific purpose and allow for the collection of adequate, non-excessive and relevant data according to that purpose. He too is an advocate of using pseudonyms.

6.2 EUROPEAN-AMERICAN GULF REGARDING PRIVACY

Even if the right to be forgotten would be properly defined, its scope clear, the conditions in which it could be asserted properly determined and its enforcement unproblematic, the clash between the American and the European conceptions of balance between privacy and free speech would still remain.

The fact that, as Werro (2009) put it, "the Europeans trust in the government and distrust the market, while Americans take precisely the opposite

[45] Markhoff, J. 2009, „New Technology to Make Digital Data Self-Destruct", viewed 23.07.2012, <http://www.nytimes.com/2009/07/21/science/21crypto.html>.

[46] http://www.backes-srt.de/produkte/x-pire/, viewed 20.07.2012.

view" resulted in different approaches to the right to privacy on the two continents.

Under U.S. law the utmost importance is granted to freedom of speech and freedom of the press, to the possible detriment of the individual's right to privacy. According to the First Amendment of the American Bill of Rights "Congress shall make no law […] abridging the freedom of speech, or of the press […]"[47] leaving the right to be forgotten unprotected in the United States[48].

The European approach is different. The protection of the individual's private and family life is stated in the European Convention on Human Rights (Article 8)[49] and in the Charter of Fundamental Rights of the European Union (Article 7)[50]. Moreover the Council's Convention 108[51] and the Data Protection Directive grant subjects the right to the protection of their personal data recognizing a right to erasure while the proposed Regulation foresees a right to be forgotten.

The scope of the application of the European data protection rules has been extended to include controllers not established in the Union, as long as the data subject resides in the Union and the processing activities concern "the offering of goods and services to such data subjects" or "the monitoring of their behaviour"[52].

However the unilateral statement on behalf of the European legislator, that companies like Google and Facebook shall fall under European jurisdiction if their activities concern European citizens, is far from being an easily enforceable provision.

The case of Yahoo! v. LICRA is a very good example for a situation in which European jurisdiction is denied by American courts because of different views. In the case concerning the sale of memorabilia from the Nazi

---

[47] Bill of Rights of the United States of America (1791), viewed 14.07.2012, <http://billofrightsinstitute.org/founding-documents/bill-of-rights/>.

[48] Werro, F. 2009, "The Right to Inform v. The Right to be Forgotten: A Transatlantic Clash", in *Liability in the Third Millenium, Colombi Ciacchi*, A., Godt, C., Rott, P. & Smith, L.J. (eds.), Baden-Baden, F.R.G., Nomos, viewed 14.07.2012, <http://ssrn.com/abstract=1401357>.

[49] European Convention on Human Rights, viewed 13.07.2012, <http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/CONVENTION_ENG_WEB.pdf>.

[50] Charter of Fundamental Rights of the European Union, viewed 13.07.2012, <http://www.europarl.europa.eu/charter/pdf/text_en.pdf>.

[51] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.01.1981, viewed 23.07.2012, <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.

[52] Article 3(2) of the General Data Protection Regulation COM(2012) 11 final.

period through Yahoo's auction site to French citizens, the High Court of Paris concluded that Yahoo violated the French Criminal Code and sought a Motion to Dismiss. On the other side of the Atlantic however, the United States District Court for the Northern District of California found the decision of the French court to be inconsistent with the First Amendment to the U.S. Constitution relating to freedom of expression and thus inapplicable in the U.S.[53]

Considering the clash of approaches between Europeans and Americans with regard to the right to privacy and the impossibility of an actual enforcement of European principles onto American companies, as illustrated in the Yahoo! v. LICRA case, it remains doubtful if the proposed right to be forgotten will actually have an impact on SNS like Facebook and be able to protect individual rights as it was intended to.

7 CONCLUSIONS

In today's digital era our past has become ubiquitous. Every move we have made has been indexed, analysed, evaluated, resulting in a complex digital image which risks overgrowing who we are in the present.

The need to counteract this development by explicitly regulating a right to be forgotten comes as no surprise. However, considering the Data Protection Directive's provisions regarding the right of access, in particular the right to request erasure, and the already existing collection limitation, purpose specification, data quality and use limitation principles, advertising a supposedly newly introduced right is rather unsupported. The right to be forgotten appears as a way of strengthening already existing data principles and the right to erasure. The discussion should rather be focused on the reasons for the failure of the rights and principles contained in the Data Protection Directive.

Expressly addressing the need to forget by the European legislator is nevertheless welcomed. But it remains quite doubtful if the mentioned right will be successful in the context of its blurry regulation. Does it mean the deletion of data in due time or the right to a clean slate? Does the latter approach suggest that outdated personal data should not be used against

[53] For details see Mankowski, P., 2002, „U.S. District Court for the Northern District of California: Yahoo vs. LICRA" Rechtsprechung, in MMR – MultiMedia und Recht, vol. 1, pp. 26-30 and also Greenberg, M., H. 2003 „A Return to Lilliput: The LICRA V. Yahoo! Case And The Regulation Of Online Content In The World Market", in Berkeley Technology Law Journal, vol. 18, pp. 1191-1258, viewed 14.07.2012, <http://www.btlj.org/data/articles/18_04_05.pdf>.

people or rather a right to self-development? Neither official authorities nor legal doctrine have adopted a well-defined position regarding the concept of the right to be forgotten. Under these circumstances it is only natural for further enforcement issues to arise.

There is no greater need of protecting the individual's privacy by allowing him to be forgotten than within social networks. Facebook allows for the collection of huge amounts of personal data so that the subject needs legal aid in order to enforce his right to privacy and to be forgotten.

To support this argument one needs only consider Facebook's lack of compliance with the purpose specification principle, which increases the risk of de-contextualization of information and may lead to what is called a "chilling effect" on the individual's development.

Moreover the absence of a clear unitary approach regarding the concept of "controller", against whom the right to be forgotten is to be asserted, and the resulting problems of liability and responsibility still have be tackled.

Only, after having solved these conceptual aspects, one still stumbles against enforcement problems. In order to be effective, the legal measures regarding the right to be forgotten have to be strengthened by appropriate technical measures.

The legal approach towards regulating privacy by design takes the right to be forgotten a step further, however only theoretical. Theoretically we stumble on further unclarities regarding the implementation of this principle. Options like introducing expiration dates for digital information, services to "bury information", online reputation management, making Facebook responsible for the architecture of the SNS have been considered as possible solutions.

Presuming that all these hurdles have been overcome, the effectiveness of the right to be forgotten remains extremely questionable in the context of Europeans and Americans having different views on privacy and the impossibility of imposing European legal solutions on American courts[54].

[54] This work was supported by the strategic grant POSDRU/6/1.5/S/26, co-financed by the European Social Fund, within the Sectoral Operational Programme Human Resources Development 2007 – 2013.