The Right to be Forgotten and the Informational Autonomy in the Digital Environment

Prof. Dr. Cécile de Terwangne

2013

Report EUR 26434 EN

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Ângela Guimarães Pereira
Address: Joint Research Centre, Via Enrico Fermi 2749, TP 361 , 21027 Ispra (VA), Italy
E-mail: angela.pereira@jrc.ec.europa.eu
Tel.: +39 0332 78 5340

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC 86750

EUR 26434 EN
ISBN 978-92-79-35086-3
ISSN 1831-9424

doi: 10.2788/54562

Luxembourg: Publications Office of the European Union, 2013

Printed in Italy

The Right to be Forgotten and the Informational Autonomy in the Digital Environment

Prof. dr. Cécile de Terwangne

University of Namur, Belgium

1. Definition and context of the right to be forgotten

1.1. What is meant by the "right to be forgotten"?

The right to be forgotten, equally called right to oblivion, is today at the heart of intense debate in high level spheres. The European Union legislators have been discussing the relevance of such a right in the digital environment since months, the Council of Europe authorities have expressed their concern on the subject, national politicians raised their voices, data protection authorities, entities working in the field of human rights, academics and experts have joined the procession coming from different geographical horizons.

What is at stake is the right for natural persons to have information about them deleted after a certain period of time.

This has already been in some way recognised as a right under two different angles: as regards the criminal past and as part of the data protection legislation (see hereunder, point 4.1. and 4.2.). But the development of the information and communication technologies (ICT) has been determining as regards the necessity to re-think the extension of the scope of that right. Technological progress has had a considerable impact in this field. The Internet has brought with it a need of new balances between the free dissemination of information and the individual self-determination. This balance is precisely what is at stake today with the right to be forgotten.

It is important to rightly understand what is really meant by the right to be forgotten. The idea is not to allow someone to re-write the past and to erase (unpleasant) traces of his/her time on earth.[1] The idea is to see to it that someone's present is not cluttered up by his/her past. The past is the past and should not recurrently come to the surface. Change and maturation are part of human being nature. Individuals should not be reduced to their past. The right to be forgotten does not mean erasure of the information. It rather means to stop bringing back data from the past. This is the first understanding of the right to oblivion. This right is conditioned by the elapsing of time and concerns information (re)made publicly available.

But another sense is given today to this notion. The notion of "right to be forgotten" is used, at least in the framework of the European Union institutions, as we will see later in this study, to cover a wider reality than the link between past and present. In its communication preceding the process of revision of the general directive 95/46 on personal data protection, the European

[1] At the 'Innovation Conference Digital, Life, Design' in Munich on 22 January 2012, Viviane Reding, Vice-President of the European Commission and EU Justice Commissioner, announced the insertion of a right to be forgotten in the Data Protection Reform. She stated: "It is clear that the right to be forgotten cannot amount to a right of the total erasure of history. » (V. Reding, "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age", *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF)

Commission refers to the right to be forgotten as "the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes. This is the case, for example, when processing is based on the person's consent and when he or she withdraws consent or when the storage period has expired. "[2] The right to oblivion in that sense is linked to the purpose of the processing of data and to the end of usefulness of the data with regard to that purpose. The data subject's will can also be the triggering factor of this newly sketched right to oblivion. The proposal issued in 2012 by the European Commission for a general data protection Regulation[3] to replace the Directive 95/46[4] accentuates even more the determining role of the individual's will as regards the right to be forgotten.

This evolution recognises the right to be forgotten as an element of the informational self-determination (see developments at point 2 hereunder). Given that meaning, this right is no more conditioned by the elapsing of time and does not necessarily concern information (re)made publicly available. It is rather the right to obtain from someone that he/she forgets (deletes) what he/she knew because it is not legitimate to keep knowing it. We will see that this presentation of the right to be forgotten by the European Commission is simplistic. In several cases this right will not imply to "stop knowing" but rather to stop disseminating or to de-index data.

1.2. Specific context of the Internet

The eternity effect

The infallibility of the "total memory" of the Internet contrasts with the limits of human memory.[5] Now memory can be the one of rancor, vengeance or belittlement. Thanks to its "eternity effect"[6], the Internet preserves bad memories, past errors, writings, photos or videos which we would like to deny later. "The transparency of the information on someone's errors of trajectory, condemnations and lifestyles could affect and disturb the life of other related people. Unfortunate or dishonest links become very easy on the Net. They can be used by whoever wants to put his/her fellow man in trouble."[7] The European Commissioner for Justice Viviane Reding stated some time ago: "As somebody once said: "God forgives and forgets but the Web never does!" This is why the "right to be forgotten" is so important for me. With more

[2] European Commission Communication, "A comprehensive approach on personal data protection in the European Union", 4 November 2010, COM(2010) 609 final, p. 8. Also, "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." (V. Reding, *op. cit.*).

[3] 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), 2012/0011 (COD).

[4] 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. *Official Journal*. L 281, 23/11/1995, p. 31 – 50.

[5] I. Székely, "The right to forget, the right to be forgotten. Personal reflections on the fate of personal data in the information society", in S. Gutwirth, R. Leenes, P. De Hert and Y. Poullet (eds.), *European data protection: in good health?*, Dordrecht, Springer, 2012, pp. 347-363.

[6] WALZ, S. (1997). « Relationship between the freedom of the press and the right to informational privacy in the emerging Information Society », 19th International Data Protection Commissars Conference, Brussels, 17-19 September 1997, p. 3.

[7] ETTIGHOFFER, D. « Les droits de l'homme numérique : le droit à l'oubli », 2, http://www.eurotechnopolis.org/fr/oubli.html (our translation).

and more private data floating around the Web – especially on social networking sites – people should have the right to have their data completely removed."[8]

The de-contextualisation

The "new" digital right to be forgotten claimed today and sketched in the regulation proposal of the European Commission is clearly linked to certain Internet specificities. The "eternity effect" of the electronic memory is to be combined with the efficiency of search engines to bring to the surface of the Net the slightest piece of information, removed out of its initial context, and to gather all the pieces to offer a recomposed though often heterogeneous portrait. Linked to the "absolute memory" of the Internet, such portrait may consist of past characteristics eternally present. Result can be sometimes some way or other harmful. And it is not only information on you disclosed by third persons that can raise concerns. Troubles can ensue from what we once brought ourselves into the light of the Web. What you have agreed to disclose to certain recipients because they belong to a determined circle (friends, family, members of an interest group, etc.), you do not necessarily want it to be accessible to anyone else in a different context. But thanks to search engines it does become accessible outside of the initial circle and context. It appears that you could suffer from information you had spontaneously disclosed yourself at an earlier stage.[9]

As a matter of fact, certain companies specialised in the managing of the "e-reputation" of individuals and legal entities on the Web have appeared. They offer to do one-shot or long term cleaning operations to protect, maintain or restore one's reputation and image.

The necessity of a decision to erase

Another specificity of the Internet is that, contrary to what happens in the physical life, erasing data in the digital world needs a decision to be taken. It is a conscious and desired process. You must have the will to delete.

The economic cost of erasing

Moreover, it has become less expensive to store data than to destroy it or to anonymise it. Storage capacities have indeed exponentially grown while their costs have diminished. At the same time, "nowadays forgetting is a costly affair"[10]. Selection and assessment of data are indispensable processes before deleting it. But these operations are costly and labour-

[8] REDING, V. Vice-President of the European Commission, responsible for Justice, Fundamental Rights and Citizenship Privacy matters. (2010). "Why the EU needs new personal data protection rules?". The European Data Protection and Privacy Conference, Brussels, 30 November 2010, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700.

[9] On the risk of de-contextualisation in SNS, see Franck Dumortier. 2009. "Facebook and risks of "de-contextualization" of information", available at: http://works.bepress.com/franck_dumortier/1. On social network sites, it has been demonstrated that a user's loss of control is to be noticed at three levels: the creation of personal data, their accessibility and their deletion (J.-P. Moiny, 'Cloud based Social Network Sites : under whose Control ?', *Investigating cyber law and cyber ethics*, 2012, pp. 147-219).

[10] I. Szeleky, *op. cit.*

intensive.[11] The exercise of the right to be forgotten therefore goes against the natural economic trend.[12]

In the same way, erasing personal data goes against the Internet economic model. One of the targets of the right to oblivion is the traces Internet surfers unconsciously leave behind them while circulating on the Net. Associated with cookies, IP address retention, surf analyses, storage of search requests on search engines, etc., all these data are highly valuable in an economic perspective. The long lasting keeping by most Internet actors of all these unconscious traces is precious to them given the economic model of service offer on the Net: most of the informational products or services are apparently for free whereas they are financed by individually targeted advertising and behavioural advertising. This definitely limits the enthusiasm to erase such information.

2. The informational autonomy or informational self-determination

2.1. The notion of informational autonomy/self-determination

The informational autonomy or self-determination means the control over one's personal information, that is to say the individuals' right to determine which information about themselves will be disclosed, to whom and for which purpose[13]. 'Control' could also signify, not so much the possibility to decide over the use of one's data, but at least the right to be aware of their fate, to get informed about who knows what about you and for what to do.[14]

The informational autonomy is derived from the right to privacy, but not in the classical meaning of 'privacy' read as 'intimacy' or 'secrecy'. It rather refers to another dimension of privacy, i.e. the individual autonomy[15], the capacity to make choices, to take informed

[11] *Ibidem*.

[12] European Data Protection Supervisor, Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union", 14 January 2011.

[13] C. de Terwangne, 'Internet Privacy and the Right to Be Forgotten/Right to Oblivion', *Revista de Internet, Derecho y Politica*, 2012, p. 112; A. Rouvroy and Y. Poullet, "The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy", in S. Gutwirth, P. De Hert, Y. Poullet (ed.), *Reinventing Data Protection*, Springer, 2009, available at: http://works.bepress.com/antoinette_rouvroy/7; G Hornung, C Schnabel, « Data protection in Germany I: The population census decision and the right to informational self-determination », *Computer Law & Security Review*, 2009, pp. 84-88; P. Schwartz, "The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination", *The American Journal of Comparative Law*, Vol. 37, No. 4, 1989, pp. 675-701, available at: http://scholarship.law.berkeley.edu/facpubs/866; H. Burkert, « Le jugement du tribunal constitutionnel fédéral allemand sur le recensement démographique », *Droit de l'Informatique et des Télécoms*, 1985, 8-16 ; C. de Terwangne, « Le rapport de la vie privée à l'information », in *Droit des technologies de l'information. Regards prospectifs* (dir. E. Montero), Cahiers du CRID n° 16, Bruxelles, Bruylant, 1999, p. 144 ; Th. Leonard et Y. Poullet, « Les libertés comme fondement de la protection des données nominatives », in F. Rigaux, *La vie privée : une liberté parmi les autres ?*, Travaux de la faculté de Droit de Namur, n° 17, Bruxelles, Larcier, 1992, pp. 231 et s.

[14] The Court stated that "if one cannot with sufficient surety be aware of who knows what about them. Those who are unsure if differing attitudes and actions are ubiquitously noted and permanently stored, processed or distributed will try not to stand out with their behavior. Those who count with the possibility that their presence at a meeting or participation in a civil initiation might be registered by the authority, may perhaps abandon practicing their basic rights."

[15] For the explicit recognition of a right to self-determination or to personal autonomy as enshrined into the right to respect of private life of article 8 ECHR, see ECtHR, *Evans v. United-Kingdom*, 7 March 2006, req. n° 6339/05

decisions, in other words to keep control over certain aspects of one's life. Related to personal information, this individual autonomy means informational autonomy or 'informational self-determination' as was first stated by the German constitutional Court in its crucial decision in 1983[16]. In its "Declaration on mass communication media and human rights", in Resolution 428 (1970), the Parliamentary Assembly of the Council of Europe defined the right to privacy as "the right to live one's own life with a minimum of interference". Almost 30 years later, the Assembly specified in Resolution 1165 (1998) that, "in view of the new communication technologies which make it possible to store and use personal data, the right to control one's own data should be added to this definition".

In Europe, this informational self-determination has been recognized and protected as a right, i.e. the right to protection of personal data. The European Court of Human Rights has derived this new dimension of privacy from article 8 ECHR[17]. The Council of Europe Convention 108[18] has established since 1981 the right to protection as regards the automated processing of personal data. The European Union Charter of Fundamental Rights[19] is the first general international catalogue of fundamental freedoms and rights that mentions the right to data protection as an autonomous right, protected as such. Its article 8.1 states that "Everyone has the right to the protection of personal data concerning him or her." Finally, the EU directive 95/46 relating to the protection of individuals with regard to the processing of personal data and on the free movement of such data offers a very detailed legal regime which is currently under revision.

Of course, this right to informational self-determination is not absolute. Overriding public or private interests are to be taken into consideration resulting in possible exceptions or limits to the individual control over the data.

In the digital environment, and especially on the Internet, huge quantities of information relating to individuals are processed: it is disclosed, disseminated, shared; one can select it, download it, register it and use it in all kinds of ways. Control over who you are disclosing your information to is pretty delicate.[20] As said here-above, search engines like Google today bring together information coming from various contexts. Doing so, they take data out of the initial circles and render it highly difficult to control who you disclose information to. The other difficulty concerns the moment at which disclosure occurs. What you have disclosed at one

(confirmed by the judgement of Grand Chamber on 10 April 2007) ; *Tysiac v. Poland*, 20 March 2007, req. n° 5410/03 ; *Daroczy v. Hongary*, 1 July 2008, req. n° 44378/05.

[16] BundesVerfassungsGericht, 15.12.1983, *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1 ff: "[...] in the context of modern data processing, the protection of the individual against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general personal rights of the [German Constitution]. This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data. Limitations to this informational self-determination are allowed only in case of overriding public interest."

[17] See among others E.Ct.H.R., *Rotaru v. Romania*, 4 May 2000, appl. no 28341/95, § 43; *Amann v. Switzerland*, 16 February 2000.

[18] Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data, ETS No 108, 28.1.1981.

[19] Charter of Fundamental Rights of the European Union, *Official Journal*, 18 December 2000, C-364/1.

[20] "In open networks such as the Internet, *information accessible to the public typically cannot be kept under the control of the user who originated the data. The reason is that data can be digitally copied, stored locally, and re-entered into the Internet, often in different locations for different purposes*." (ENISA, "The right to be forgotten - between expectations and practice", 20 November 2012, p. 10, available at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/)

stage of your life you do not necessarily want it to be permanently available. This raises the very question of the recognition or not of a right to be forgotten.

Before focusing on this last point, there remains a term to precise. The concept of personal information or personal data is to be considered very widely since it should not be linked to the idea of intimacy as in a 'classical' approach of privacy. It rather means *any* information related to a natural person. It thus covers professional data, commercial data and published data.

2.2. The right to be forgotten as linked to the informational self-determination

As stated above (point 1.), the right to be forgotten has been at first linked to the elapsing of time. It is presented today as a part of the informational autonomy.

The European Commission has shown concerns about the problems raised by the interrelation of the Internet specificities. Perfect memory and de-contextualisation of data have proved to be source of problems for individuals. And users of social network services have complained not to be able to obtain the complete erasure of their data stored by the service provider. In its proposal for a general Regulation on data protection, the Commission tackles these problems by guaranteeing notably a digital right to be forgotten (Article 17 of the Regulation proposal).

One notices that it is not so much a problem of erasure of the past that is at stake in these cases. As regards the problem of de-contextualisation for example, it is true that the elements brought to the surface by search engines have necessarily been previously disclosed somewhere on the Net. But 'previously' could mean some minutes before, which is not what is ordinarily meant by the 'past'. It is not the length of time passed since the initial processing of the data that matters.

The right to be forgotten in that sense does not even imply the erasure of the data. If remaining in its initial context, the data is not necessarily problematic. One does not necessarily desire its erasure but much more the erasure of the link that allows search engines to select this data while dredging the Web.

The right to be forgotten in that approach is much wider than a concern about the link between past and present. It has to do with informational autonomy.

When this autonomy is exerted on data that one had previously disclosed about him/herself, the right to be forgotten could then be partially described as a "right to change one's mind" and a "right to remorse".

All these aspects of a right not to be permanently remembered one's past, a right to have someone forget what he/she knew because it is no more legitimate, a right to refuse de-contextualisation of data and a right to remorse and to change one's mind form the newly sketched right to be forgotten.

This right is to be comprehended considering two different situations:

- When the processing of data is based on the data subject's consent (point 3 hereunder)
- and when the processing relies on another ground (point 4 hereunder).

3. The right to be forgotten in case of data processing based on the data subject's consent

3.1. The right to be forgotten as a right to remorse and a right to change one's mind

One aspect of the right to be forgotten is specifically linked to the Web 2.0 even if it is not limited to this context. The Web 2.0 allows interactivity. People have the possibility to express themselves, to manifest ideas and opinions and to disclose information, pictures, videos,… Many emblematic Internet services illustrate the public craze for interactivity: Wikipedia, Youtube and all the crowded social network sites.

But, as in the ordinary life, it happens that you regret what you have expressed or disclosed thanks to this Web interactivity. Or it occurs that you change your mind.

Such situations are particularly frequent when expression is spontaneous and unhesitating (as it is often the case on social network sites). It is to be noted that it is the first time in the history of public communication that this type of spontaneous expression does not vanish and, on the contrary, remains continuously available to the public or to a certain part of the public long after it has been made.

Remorse or change also often arises as regards information or pictures shared while the issuer was young. Grown up young people may be willing to erase traces of their online activities as teenagers that they consider today immature, irresponsible, incorrect or improper.

But it appears pretty difficult to do this sound exercise of correcting your past stupidities. We have even discovered that it was impossible to entirely erase data once posted on Facebook.[21] The European Commission itself stated that it "has received various queries from individuals who have not always been able to retrieve personal data from online service providers, such as their pictures."[22]

Right to withdraw consent leading to erasure of data

In view of these difficulties, the European Commission clarified in the Article 17 of its Proposal for a General Data Protection Regulation dedicated to the "Right to be forgotten and to erasure" that data subjects should be granted the right to have their personal data erased where they have withdrawn their consent for processing. This clarification of the possibility to withdraw the consent previously given is welcome since this question still raises some discussion in the current situation. Article 7,§ 3 of the Regulation proposal already expressly provides for the right to withdraw consent at any time[23]. Article 17 nonetheless states that this withdrawal can be considered as part of the right to be forgotten. Most of all, it brings additional information as to the effect of the withdrawal in terms of erasure or restricted use.

The text specifies that deletion of data will occur after withdrawal of consent only if where there is no other legal ground for the processing of the data.

---

[21] See the complaints against Facebook filed by Max Schrems, an Austrian Law student, and some others, with the Irish Data Protection Commissioner about pokes, postings, messages and even friends, kept by Facebook long after the user "removes" them, available at http://www.europe-v-facebook.org/EN/Complaints/complaints.html. Also Brendan Van Alsenoy, Joris Ballet, Aleksandra Kuczerawy, Jos Dumortier 'Social networks and web 2.0: are users also bound by data protection regulations?', *Identity in the Information Society Journal - IDIS* (2009) 2, pp. 65–79.

[22] European Commission Communication, 'A comprehensive approach on personal data protection in the European Union' 4 novembre 2010, COM(2010) 609 final, p. 7.

[23] Article 7,§ 3 of the Regulation proposal already provides : « The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. »

This withdrawal of consent is an important tool of the right to be forgotten in the context of social networks since data processing in that context mainly relies on the data subject's consent or on contractual relations. The obligation to erase data as a consequence of the right to be forgotten is intended to be an appropriate answer to the problem of social networks like Facebook that do not really delete data "removed" by users but only make it no more publicly available.

This right to erasure in cases where information has been disclosed on the data subject's initiative seems quite logic and evident, even to Peter Fleisher (Google's Global Privacy Counsel) who is yet a fervent opponent to the right to oblivion. According to him, "If I post something online, should I have the right to delete it again? I think most of us agree with this, as the simplest, least controversial case. If I post a photo to my album, I should then later be able to delete it, if I have second-thoughts about it."[24]

Special attention to consent given as a child

The authors of the Regulation proposal underline that "*This right is particularly relevant, when the data subject has given their consent as a child*, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet".[25] Consideration is thus given to the situation mentioned above concerning data disclosed by young people. That being said, one does not see well the real legal implication of saying that "this right is particularly relevant" and that data subjects have the right to obtain from the controller the erasure of personal data "especially in relation to personal data which are made available by the data subject while he or she was a child," as inserted in article 17 of the Regulation Proposal. Does it mean that the exceptions provided for in article 17, § 3 should be admitted with greater difficulty? Does it mean for example that a heavier weight should be given to the interest of erasure when balancing it with the freedom of expression as far as the controversial data was made available when the data subject was a child? Or should erasure be systematic in that case? The proposed text is not clear at all on this point.

The draft report of the Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) on the Regulation Proposal has stressed in the same way that there appears to be little specific value to demand "particular" attention for children[26]. The Parliament is even concerned that this portion of text could have the effect of implying a lesser protection for adults. A member of the European Parliament proposes to shift the word "especially" to "including". She explains that *"The word 'especially' hints at a stronger importance of the right to be forgotten when involving a child than when not involving a child. This nuance is irrelevant. 'Including' enables to point out the particularity of a child being the data subject without making any differentiation of importance of the general right to be forgotten."*[27] These reactions show that the legal implication of the special attention to be given to data from children needs a clarification. The intention of the European Commission is not clear for the Parliament.

[24] P. Fleisher, "Foggy thinking about the Right to Oblivion", Peter Fleisher's Blog. 9 March 2011.
[25] Recital 53 (I underline).
[26] European Parliament, Draft Report on the Proposal for a General Data Protection Regulation, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht, 17 December 2012, Amendment 34.
[27] European Parliament, Committee on Industry, Research and Energy, Draft opinion on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Rapporteur: Sean Kelly, 21December 2012, Amendment 482 from Amelia Andersdotter.

Right to object if processing does not correspond to consent

If the processing of personal data is based on the data subject's consent, consent covers only situations respecting the elements included in it: the type of data, the agreed storing period, the purposes of the processing,... If some element does not correspond anymore to what was consented to, withdrawal of consent will not be the correct tool. In such a situation the data subject can instead object to the processing of personal data.[28] (See the developments on the right to objet under point 4 hereunder)

3.2. Effect

3.2.1. Erasure or...

Article 17, § 1 of the Regulation Proposal guarantees to the data subject, in the name of the right to be forgotten, the right to obtain from the controller "the erasure of personal data relating to them and the abstention from further dissemination of such data". The data subject is thus entitled to demand that his/her personal data be deleted, and not only rendered inaccessible as the practise of social network services has shown to be.

The data subject may also prefer not to see the data erased but requests to transmit the personal data into another automated processing system (article 17, § 4, d).

One regrets that this hypothesis is the only one diverging from erasure that has been envisaged in the draft regulation[29]. As a matter of fact, other cases may be where the data subject withdrawing his/her consent does not intend to see his/her data erased:

- Not to be associated anymore to the data could suffice. **Anonymisation** of the data would then be an adequate answer to such aspiration.
- Or the problem could ensue from the public disclosing of personal data but not from an internal processing of it. The data subject could in such case be willing to **stop the publication** of the data but accepts the data remaining stored and used by the controller. **Restricted access to the data** could lead to the same result. External accesses would be blocked. Perhaps the authors of the draft regulation envisaged two different effects of the right to be forgotten: the erasure of data OR the **abstention from further dissemination**. This would have been a better solution because more nuanced than the systematic linking of both effects deriving from the use of AND in article 17, § 1. However, nothing in the recitals nor in the Explanatory memorandum allows to understand that article 17, § 1 presents two different, unlinked effects. On the contrary, there is no other reference to the abstention from further dissemination anywhere else in those texts. This abstention is never presented as a possible autonomous effect of the right to be forgotten.
- Or the data subject could also ask to **stop certain forms of publication** but accepts other forms (a person has consented to be filmed and accepts that the film

[28] The data subject can also file a complaint or sue the controller in case of illegal processing (if no other ground than consent covers the aspects of the processing not based on what was agreed by the data subject).
[29] Other hypotheses are listed in article 17, § 4 but none of them fits the withdrawing of consent.

is projected on TV on an agreed day and time; but refuses to see this film permanently available on the Net thereafter).

- Or the data subject wants to act against de-contextualisation and would be happy with just his/her **data being de-referenced, de-indexed, links to it being suppressed**. This would be the right tool against de-contextualisation of data without depriving members of the initial circle of the possibility to access to this data provided that they remain inside the circle.

3.2.2. Information to third parties

"*To strengthen the 'right to be forgotten' in the online environment*"[30], article 17, § 2[31] of the Regulation proposal extends the right to erasure *"in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible."*[32]

This has been presented by some commentators as the real innovation of the Regulation proposal as regards the so-called "right to be forgotten". But one must note that this provision is not so distinct form article 12, c) of directive 95/46 that guarantees to every data subject the right to obtain from the controller "c) notification to third parties to whom the data have been disclosed of any […] erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort".

The principle of a duty to further inform persons who process the controversial data downstream from the initial processing is already present in the directive 95/46. Certain divergences are noticeable:

- article 17, § 2 makes it clear that the duty to inform automatically ensues from an erasure without the data subject having to ask for it, whereas this is not that clear in the directive;
- moreover, article 17, § 2 is aimed at the case of data made public while article 12, c) concerns data disclosed to third parties. The case of a controller disclosing data to one or several identified recipients is not covered by the making public of data. So this hypothesis is outside the scope of article 17, § 2. This is probably not what was aimed at by the authors of the Regulation proposal. It means that there will be no duty to inform the applications designers having obtained by contract with a social network service access to personal data of the users of this service in view of "feeding" their application. In fact, this would paradoxically correspond to cases where such a duty to inform would not raise major problems of practicability.
- Furthermore, the controller is held liable to inform in cases where he has made himself personal data public or has authorized a third party publication of the data. But in many cases, the provider of a social network service for example will not be the one who makes data public. The data subject (who is not to be considered as a third party) will

[30] Recital 54 of the proposal of a Regulation.

[31] Article 17, § 2 of the Regulation proposal states that "Where the controller […] has made the personal data public, it shall 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 such data, that a data subject requests them to erase any links to, or copy or replication of that personal data."

[32] Recital 54 of the proposal of a Regulation.

be that one. Many cases will in consequence fall outside the duty to inform. Again, it is questionable whether this is meant by the legislator.

Parliament amendments proposals show that for Members of European Parliament article 17, § 2 *"targets particularly the transfer of data that are object of an erasure request"*[33]. They propose to widen the scope of this provision so as not to limit it to cases where data are made public but to encompass also cases where data are "transferred".[34] According to their justification, "*the controller is responsible for applying this provision also to data that have been voluntarily transferred or released to third parties that have no relation with the data subject."*[35] Amendment proposed in the Albrecht Report for the LIBE Committee of the Parliament[36] also provides to refer to "transfer" but this notion would come in addition to the making public of data and is then not viewed as an all-encompassing notion.

This proposition of widening is welcome even if the notion of "transfer of data" should not be adopted. This term would need a definition if it were to be adopted since it is ambiguous. For example, is it supposed to cover cases where the controller offers access to the data to third parties with authorisation to copy the data? The terms "disclosing" of directive 95/46 – also proposed by members of another Parliament Committee[37] - or "making available" to third parties seem to be more appropriate.

Some additional comments can still be made concerning article 17, § 2.

First, one has to clarify that the controller would not be responsible for ensuring that the third parties comply with the deletion request. Article 17, § 2 creates only a duty to inform. This is appropriate if one considers notably that third parties could be in a position to argue against the request for erasure even if the controller himself would not be (see *infra* the exceptions to the right to be forgotten).

Some members of the Parliament would like to go further and to complete the duty to inform with a duty to follow what is happening and to inform back the data subject: "*The rights of data subjects must be reinforced. Article 17(2) imposes an obligation of responsibility on the controller. This must be accompanied at the very least by a duty to inform regarding the action taken by third parties processing the personal data in question."*[38] We will see hereunder that the practicability of the duty to inform is already heavily contested. It is sure that obtaining information as to the result of the information would seem even less realistic.

Then, even if the data subject's request to delete is addressed to the controller, it is considered to be addressed to third parties as well ("the controller […] should be obliged to inform third parties which are processing such data that a data subject requests *them* to erase [...]"). The wording of article 17 is quite pragmatic even so it does not correspond to reality. A problem lies in that some situations where third parties process personal data are not covered by the data subject's initial consent. This is notably the case when the disclosing of data to third parties does not enter into the reasonable expectations of the data subject, or when the latter contests the disclosing of data as being unlawful. Then other grounds for a deletion request than the withdrawal of consent will apply, such as the objection to the processing. But to object to a

[33] European Parliament, Opinion on the Proposal for a General Data Protection Regulation, Committee on the Internal Market and Consumer Protection, Rapporteur: Lara Comi, 28 January 2013, Amendment 120.
[34] "Where the controller referred to in paragraph 1 has ***transferred*** the personal data***, or has made such data*** public ***without the consent of the data subject […]",*** *Ibid.*
[35] *Ibid*.
[36] Albrecht Report, *op. cit*., amendment 147.
[37] Kelly Report, amendment 488 from Adina-Ioana Vălean, Jürgen Creutzmann.
[38] Comi Report, amendment 121.

processing you have to mention grounds relating to your personal situation, which you won't have done if you simply withdraw your consent. If you contest the lawfulness of the processing you will likewise have to demonstrate some breach of the regulation. The mixing of possible different grounds for a request for erasure makes it sometimes uneasy to extend purely and simply a request addressed to the controller to all the recipients of the data.

Moreover, while the data subject asks for "the erasure of personal data relating to them and the abstention from further dissemination of such data", as provided in § 1, he is presented in § 2 as requesting "to erase any links to, or copies or replications of that personal data", which is not the same.

Finally, the practicability of this requirement on the Internet has been heavily questioned.[39] It is obvious that once data are made available on the Internet, it is a pure challenge to know where the data have been disseminated and who may be processing this data[40]. And entering in contact with these persons could prove to be pretty difficult or even impossible. The Commission envisages possible technical solutions to tackle this difficulty and, more realistically, the obligation upon the controller has been formulated as an obligation of *endeavour* rather than an obligation of *result*.

Not only the practicability but even the legitimacy of such a duty to further inform has been called into question. Parliament Committee LIBE proposes indeed to shift the duty to inform into a duty to "*take all necessary steps to have the data erased"*[41] and to restrict the scope of the duty to situations where he controller *"has transferred or made the personal data public* ***without a justification based on Article 6(1)****."*[42] It justifies that proposition in that way: *"if a publication of personal data took place based on legal grounds as referred to in Article 6(1), a "right to be forgotten" is neither realistic nor legitimate. […] This does not imply that third parties can further process published personal data if there is no legal ground for them.* This argumentation demonstrates the problem of a confused approach of the right to be forgotten, especially in the justification given. It seems that this right (at least as concerns this duty in case of publication of the data) is confused with the right to erasure as this one is perceived in directive 95/46. It is then a tool to act against unlawful processing of data (here unlawful transfer or publication of data). But the right to be forgotten is not limited to unlawful processing of data (see *infra*). Exercising it towards controllers who publish data based on a legal ground is perfectly legitimate. Withdrawing consent or objecting to the processing of data are both done as regards lawful processing of data. Restricting the right to be forgotten to acting against unlawful publication of one's data would limit this right to a pure right to erasure as understood in the current directive. It would just be a tool to see to compliance.

A strange element of Albrecht's approach is the fact that certain justifications he brings do not correspond to any change he proposes in the text of the Regulation proposal. In this way, he proposes that *"In the case of published data, the original data controller shall only be obliged to inform those third parties which it can reasonably expect to be further processing the data* ***and also inform the data subject about them****. This also allows for the data subject to contact them directly and request from them to inform further third parties and it also gives the data subject a fuller understanding of the spreading of his/her personal data*."(bold characters added) Nowhere in the text does he propose to establish a duty to inform the data subject about

[39] See notably EDPS opinion, *op. cit.*, §§ 146-147.
[40] See ENISA, "The right to be forgotten - between expectations and practice", 20 November 2012, available at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/
[41] Albrecht Report, *op. cit.*, amendments 35 and 147.
[42] *Ibidem*.

who are the third parties. Besides, this piece of justification is incoherent with the rest of Albrecht's proposals who do not talk of any duty to inform.

4. Right to be forgotten in case of data processing based on another ground

In case of processing of personal data based on another ground than on the data subject's consent, the interests of the data subject protected by the right to be forgotten enter into conflict with other interests, rights and freedoms. In particular, it conflicts with freedom of expression and freedom of the press. It impinges on the conservation of full archives, as will be developed under point 4.2.3. of the present paper relating to the Internet newspapers archives. For the same reason, it hurts the duty of memory. It is a hindrance to historical research. It has also an impact on business continuity, management of employee files, the duty to keep evidence, etc.[43] And one inevitably has to take into account the obligation to retain data for public security purposes.

The legal answer when facing such conflicts consists in balancing the competing values and interests in view of reaching a fairly balanced result. There is indeed no a priori hierarchy among human rights. This signifies that conflicts of rights cannot be solved by giving systematic priority to one right over the other one. Answer to a conflict always passes through a balancing test. Conflicting rights are put into scales so as to reach a balanced result. The infringement incurred by the sacrificed value should not be disproportionate with regard to the benefice obtained by the conflicting value.

4.1. Balancing test and the right to oblivion of the judicial past

The first meaning of the right to be forgotten is linked to an individual's judicial or criminal past. It is the most classical facet of this right. It was at first mostly linked to the creation of criminal records. Today the right to oblivion of the judicial past has widely gone beyond these criminal records. It has been recognized by case law in several countries, based on the right to privacy or as part of the personality rights. As mentioned in point 1 of this paper, it is justified by faith in human being's capacity of changing and improving as well as on the conviction that man should not be reduced to his past. Once you have paid what was due, the society must offer you the possibility to rehabilitate and restart without bearing all life long the weight of your past errors.

This right conflicts with the right to information, time being the criterion to resolve the conflict.

4.1.1. The criterion of newsworthiness or of historical interest

The right to be forgotten must give priority to the requirements of the right to information when the facts that are revealed present a topical interest for disclosure. The interest is thus linked to the newsworthiness of the facts. This is so when a judicial decision pronounced by a court or by a tribunal is part of judicial news. It is then legitimate to evoke this decision mentioning parties' names (except if they are minors, in which case different rules of protection apply). But as soon as time has passed and it is no more a question of news or current events, as soon as

[43] *Ibidem*

news necessity does no more justify re-disclosure of the information, the right to oblivion overrides the right to information. Mention of the case may still be done but should not include parties' names or identified data. So the newsworthiness of a case tips the balance in favour of the right to disseminate instead of the right to be forgotten. And as soon as it is no more newsworthy, scales tilt the other way.

Two exceptions can be admitted to this. This means that the right to information will override in spite of elapsing of time

- for facts pertaining to history or concerning a matter of historical interest and

- for facts linked to the exercise of a public activity by a public figure.

Historical interest and public interest are also to be taken into consideration to solve the conflict between right to be forgotten and right to information.

4.1.2. Impact of Technical Developments on the balancing test: the power of search engines

Technical developments have radically changed the balance reached before between necessity to disclose judicial information and the individual right to be forgotten. As said earlier, every slightest piece of information can be brought to the surface and can be gathered with other pieces. This implies a radical change.

It is worth citing a US Supreme Court decision[44] pronounced more than twenty years ago but nevertheless very enlightening for today, where the Supreme Court underlined that change. The case concerned a journalist who asked for access to FBI documents relating to the condemnations incurred by four persons. Three of them had died and for the fourth the FBI refused to disclose pieces of information that were stored in a compiled format, considering that this would breach this person's privacy. The Supreme Court unanimously upheld this decision, contrary to the Court of Appeal that had stated that there was no more privacy interest since information had been published. The Supreme Court ruled: "But the issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, country archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[45] In the same sense a Californian Appeal Court stated that "It is the aggregate nature of the information which makes it valuable to respondent; it is the same quality which makes its dissemination constitutionally dangerous."[46]

The power of Internet search engines to gather any data concerning a targeted individual at any time, from anywhere, without any administrative procedure, without revealing his own identity and for free raises an even greater danger. We must carefully reconsider the balance to be reached. On the precise point of data about judicial past, a first answer is the anonymisation of case law databases available on the Net[47]. Such anonymisation is now the rule in the majority

[44] *Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989).

[45] 489 U.S., 764.

[46] *Westbrook v. Los Angeles County*, 32 Cal. Rptr. 2d 382 (Cal. App. 1994)

[47] On this question that cannot be deeper developped in the present paper see de TERWANGNE, C. (2005). « Diffusion de la jurisprudence via Internet dans les pays de l'Union européenne et règles applicables aux données personnelles ». *Petites Affiches*, n°194, pp. 40-48.

of European countries. But another important source of concern is the question of newspapers archives. This problem will be dealt under the coming point 4.2.2.

4.2. Balancing test and Article 17 of the Regulation proposal dedicated to the "Right to be forgotten and to erasure"

Article 17, § 1[48] of the European Commission proposal for a general data protection Regulation presents two cases where a balancing test can take place: when the data subject objects to the processing of personal data; and when the processing of the data does not comply with the Regulation proposal for other reasons, more specifically when the processing does not comply with article 6.1.f. The exceptions to the right to be forgotten provided for at § 3 of article 17 are also opportunities of balancing the competing values. They will be addressed under point 5 *infra*.

4.2.1. The right to object to the processing of data

Commentators said that the newly clamoured digital right to be forgotten is perhaps simply the « lyric » translation of the already existing right to object[49].

The right to object is indeed already guaranteed today by article 14 of the directive 95/46. This provision states that every data subject is granted the right "*to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him*". If the data are meant to be processed for the purposes of direct marketing, the right to object is then not conditioned to any justification[50].

Article 17 of the Regulation proposal actually mentions the right to object to the processing of personal data as one of the grounds of the right to be forgotten. But this right to object, as newly outlined by article 19 of the Regulation proposal, presents a major change compared with the way it is formulated in article 14 of directive 95/46. The grounds the data subject has to present when objecting must no more be "compelling and legitimate". They only have to relate to the particular situation of the data subject.[51] Recital 56 clearly states it: "*The burden of proof should be on the controller to demonstrate that their legitimate interests may override the interests or*

---

[48] Art. 17.1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:
(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
(c) the data subject objects to the processing of personal data pursuant to Article 19;
(d) the processing of the data does not comply with this Regulation for other reasons.

[49] CYBERLEX, L'Association du Droit et des Nouvelles Technologies. (2010). « Contribution dans le cadre des travaux sur le droit a l'oubli numérique. L'oubli numérique est-il de droit face à une mémoire numérique illimitée? ». p. 10. http://www.cyberlex.org/images/stories/pdf/contribution_cyberlex_dao.pdf

[50] Art. 14, § 1, b) of the directive 95/46.

[51] Article 19.1 of the Regulation Proposal states : « The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject. »

the fundamental rights and freedoms of the data subject".[52] The right to object will consequently be easier to exercise for the data subject. The controller must by contrast demonstrate compelling legitimate grounds for the processing which override the interests and rights of the data subject if he/she wants to go on processing data. This shifting of the burden of proof is to be welcomed since the controller is better placed to know all the implications of the processing.

The right to obtain from the controller the erasure of personal data will only be effective after determining whether the grounds for further processing override the interests in favour of the right to be forgotten. It means that an inevitable balancing test between these contrasting interests will have to take place.

Article 19 allows the controller to demonstrate and put into the scales any grounds provided they are compelling and legitimate. On this point, the writing of article 17 is problematic since it raises confusion. Article 17, § 1 presents the fact that the data subject objects to the processing pursuant to article 19 as one of the grounds of the right to be forgotten. In its § 3, article 17 lists the admitted exceptions to the immediate erasure of data. This list is far from allowing the controller to demonstrate any compelling legitimate interest whenever he wants to refuse to erase data as asked by the data subject on the basis of article 17 (see developments on the exceptions to the right to be forgotten *infra*). The solution probably lies in understanding the words "pursuant to article 19" as referring to the whole mechanism of article 19 including the possible refusal of the controller and a result of the balancing test in favour of the objection to the processing.

In the same sense, members of the European Parliament would like to see article 17.1.c. amended as follows: "(c) *the data subject objects to the processing of personal data pursuant to Article 19**, and the objection is upheld".***[53] According to them, such an amendment is *"designed to ensure that a data subject cannot simply make an objection under Article 19, therefore triggering the principle of the Right to be Forgotten, where the objection would be without merit.*[54]

Anyway, the link between articles 17 and 19 needs to be clarified, especially on the reasons that can be put forward to counter a request to erase personal data (based on article 17) or to refuse to enforce an objection to the processing (based on article 19).

4.2.2. The right to be forgotten if the retention of the data is not in compliance with article 6.1.f) of the Regulation

Article 17.1.d) accepts as last ground for the right to be forgotten the fact that the processing of data "does not comply with the Regulation for other reasons" than the extinction of the legitimate period of retention of the data, the withdrawal of the data subject's consent and the data subject's objection to the processing.

Among the situations where the retention of personal data would not comply with the Regulation to come is the non-compliance with article 6 on the lawfulness of processing.

---

[52] See also Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012, § 153: "The burden of proof would shift to the controller whenever he would refuse to enforce the objection received from a data subject."

[53] Comi Report *op. cit.*; Kelly Report, *op. cit.*, amendment 486 from Adina-Ioana Vălean, Jürgen Creutzmann.

[54] Comi Report, *op. cit.*

If the controller relies on article 6, § 1, f) to process personal data, the challenging of this ground necessarily implies a balancing test.

Actually, article 6.1.f) provides that processing of personal data is lawful if "processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data [...]". A data subject can demand the erasure of his/her data on the ground that processing does not comply with this provision whereas none of the other hypotheses of article 6, § 1 applies. He/she will have to demonstrate that the legitimate interests pursued by the controller are overridden by his/her own interests, rights and freedoms.

This second hypothesis of balancing test to exercise the right to be forgotten offers a particular interest. Unlike with the right to object, the data subject is not required this time to put forward grounds relating to his/her particular situation. The data subject may be more general and put forward fundamental rights or freedoms.

4.2.3. Example of Internet newspapers archives. Criteria for the balancing test: newsworthiness, historical interest and public interest

Internet newspapers archives are a source of all kinds of information that were once news. Many of them concern individuals. They are not limited to judicial data of course.

The fate of personal data once mentioned in a newspaper and then eternally available on the archives website of this newspaper raises the problem of a possible conflict between the person's right to be forgotten and the freedom of the press.

As regards the conflict raised by Internet newspapers archives, consideration must be given to the above-mentioned criteria of

- newsworthiness,
- historical interest
- and public interest.[55]

By definition, newspapers archives are no more supposed to present any value of newsworthiness. When considering the historical value of the facts, one should notably take into account whether other sources of information exist. As regards judicial data, special attention must also be paid as to whether appeal has been made against judicial decisions stored in newspapers archives. If it is the case, the first judgement could be kept but should be accompanied by a notice specifying that the decision is under revision.

In the *Times Newspapers* case, the European Court of Human Rights brought some very interesting light as regards the way the balancing test should be implemented. Even if the right to be forgotten was not at stake in this case[56], the statement of the Court could be usefully applied to hypotheses implying a conflict between the freedom of the press and the right to be forgotten in presence of publicly available newspapers archives. The Court said that holding archives is of great interest for society but is nevertheless a secondary role of the press. As such, this aspect of freedom of the press weighs less when striking the balance with another value

[55] On these criteria see European Court HR, *Osterreichischer Rundfunk*, 7 March 2007.

[56] It was a question of potential defamation linked to information maintained in the Internet archives of The Times; the original articles had been presented without any warning notice as to the fact that they were subject to a libel action.

than if the main function, that of the famous watchdog, were at stake. The Court said it "*agrees at the outset with the applicant's submissions as to the substantial contribution made by Internet archives to preserving and making available news and information. Such archives constitute an important source for education and historical research, particularly as they are readily accessible to the public and are generally free. The Court therefore considers that, while the primary function of the press in a democracy is to act as a "public watchdog", it has a valuable secondary role in maintaining and making available to the public archives containing news which has previously been reported.* ***However, the margin of appreciation afforded to States in striking the balance between the competing rights is likely to be greater where news archives of past events, rather than news reporting of current affairs, are concerned***. […]"[57]

Contrary to article 17 that only provides for the erasure of data and abstention from further dissemination of it, one can envisage different outcomes of a balancing test concerning the right to be forgotten (see point 4.4. Effects). Here, the outcome could for example be the obligation that identifying data be erased from an article in publicly available Internet newspapers archives. A non-expurgated version would be maintained with restricted access (for research purposes, notably). Or the outcome could be the requirement that additional information be linked to the data (warning or data subject's view, for example). Conclusion should always be reached on a case-by-case basis.

It should be kept in mind that this problem is mainly linked to the public availability through the Net of the controversial information. The balance reached on the Web does not necessarily correspond to what is to be done in classical formats. Certain solutions will very likely consist in giving priority to the right to be forgotten as concerns Internet archives whereas priority will be given to freedom of the press, historical, educational and public interests for archives in formats not accessible on the Net. The harm deriving from the eternal and universal availability of the data via the Internet will much more often be considered disproportionate than the harm ensuing from a local publicity subject to procedures.

4.3. Other answers of Article 17 of the Regulation proposal

4.3.1. Obligation to delete personal data derived from the purpose principle

Both hypotheses of right to be forgotten presented here above are left to the data subject's initiative. Another way of achieving the right to be forgotten is normally not demanding any initiative from the data subject. To benefit from the right to be forgotten deriving from the purpose principle, the data subject has no effort to do. It is to the data controller to see to it that personal data are erased when the purpose of processing is achieved.

One of the basic principles of the data protection regime is the purpose principle. This principle specifies that personal data must be processed for a determined, legitimate and transparent purpose. The right to oblivion directly ensues from the purpose principle since, according to one application of this principle, the controller of the data may keep personal data "in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed"[58]. This means that personal data may be kept as such if it is justified to achieve the purpose of processing. It should be either

[57] E.Ct. H.R., *Times Newspapers Limited (Nos. 1 and 2) v. the United Kingdom*, 10 March 2009, appl. no. 3002/03 and no. 23676/03, § 45 (our italics).
[58] Art. 5, e) of the Regulation proposal (which is quasi identical to the current article 6.1.e) of directive 95/46.

anonymised or deleted once the purpose has been achieved or as soon as it is no more necessary to keep the link with identifiable persons to achieve that purpose.

Data subjects are entitled to check the respect of this rule. They are granted by article 17.1.a) of the Regulation proposal the right to obtain from the controller the erasure of data the processing of which does not comply with the retention limitation ensuing from the purpose principle.

4.3.2. The right to erasure sensu stricto

Article 17 of the Regulation proposal has been elaborated by merging a right already existing – the right to erasure – with a right newly drafted, even if the elements composing this new right were already part of the data protection regime – the right to be forgotten. This brings an unhappy effect of mixing two different contexts:

- The right to erasure is part of article 12, b) of directive 95/46 that provides that every data subject has the right to obtain from the controller "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". Erasure or blocking[59] of data is, in directive 95/46, a way for the data subject to act against non-compliance with the protection rules. Importing this right into a provision devoted to the right to be forgotten has justified these words of recital 53 that states: "Any person should have […] a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation".
- But in fact for two grounds included into the right to be forgotten – the withdrawing of consent and the objection to processing – the retention of data is compliant with the protection rules at the time when these grounds apply. Indeed, at the moment one considers withdrawing consent, the processing of data is still lawfully based on the said consent. Article 7.3 expressly states: "The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.". And the same reasoning applies for an objection. Till the moment you object, the processing of your data is supposed to be compliant.

Possibility to withdraw consent and to object is given to the data subject with regard to lawful processing of their data. The context is not at all the same as that of the right to erasure stricto sensu that intervenes in case of non-compliant processing. Unlike the right to change one's mind and the right to object, the right to erasure is a tool in view of achieving compliance.(See also the Conclusive remarks of this paper)

4.4. Effects

4.4.1. Erasure or…

One notes that, in the same way as for cases of withdrawal of consent (see point 3.2. *supra*), the "right to be forgotten" in principle means obligation to deletion of data.

[59] The term « blocking » was pointed at as being ambiguous. The Regulation proposal opts for "restricted processing" which is not totally clearer…

The same comments as those concerning the effects of the withdrawing of consent may be made here. Notably the fact that for the other hypotheses of exercising the right to be forgotten, different results should also be envisaged instead of only erasure of data. A better legal answer, better respecting the proportionality principle, could be:

- anonymisation of the data
- restricted access to the data
- abstention from further dissemination
- suppression of any link towards the data
- other form of publicity (offer the possibility to opt for a form of publicity that respects the proportionality principle instead of another form where harm would be too serious as regards the benefits for competing values)
- additional information linked to the data (warning or data subject's view, for example).

Article 17, § 4 provides that instead of erasure, the controller shall restrict processing of personal data in certain circumstances. The terms "restrict processing" are meant to be clearer than "blocking" processing previously used in article 12 of directive 95/46. According to the Explanatory memorandum, "[article 17] also integrates the right to have the processing restricted in certain cases, avoiding the ambiguous terminology 'blocking'."[60] The restricted processing is to be understood[61] as the simple retention, storage of data and, except in certain very limited circumstances, no other operation performed anymore upon personal data.

The LIBE Committee of the Parliament proposes to clarify some more the notion of "restricted processing". It proposes to state that when the controller restricts processing of personal data it is "*in such a way that it is not subject to the normal data access and processing operations of the controller and cannot be changed anymore"*[62]. It focuses on the kind of operations that are still allowed to be performed upon the data. Paragraph 5 of article 17, instead, does not focus on a limited set of operations (except to say that storage is the minimum admitted for restricted processing) but on a limited set of purposes allowing processing of data: it may be processed for purposes of proof, for the protection of the rights of another person or for an objective of public interest. On a less coherent way, this provision allows also the processing "*with the data subject's consent*". The LIBE amendment proposal brings some precision as to the operations allowed for the purposes listed. But the way it is formulated is problematic: what are "normal" access to data and "normal" operations? Why only mention the operations "of the controller" while a processor could intervene as well as third parties?

Another amendment from the LIBE Committee is much more relevant: instead of allowing processing "for an objective of public interest" it should be allowed "*for compliance with a legal obligation to process the personal data by the Union or national law to which the controller is subject"*[63]. The LIBE Committee specifies that in fact "*Any public interest must be laid down in law in order to create a legal obligation for the data controller to outweigh the right to erasure of the data subject".* It is true that allowing the retention of the data should not just be authorised for any objective of public interest without any guarantee concerning this interest.

The main cases where restricted processing is envisaged in article 17.4 are temporary cases: data may be kept when their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data; and data may be maintained beyond the

[60] Explanatory Memorandum of the Regulation proposal, p. 9.
[61] Clarification is offered in § 5 of article 17.
[62] Albrecht Report, *op. cit*., amendment 149.
[63] *Ibid*., amendment 151.

period necessary for the accomplishment of the controller's task for purposes of proof. The data subject may also prefer not to see the data erased but requests to transmit the personal data into another automated processing system. One guesses that once data has been transmitted it must be erased from the first automated processing system, unless there is another legitimate ground to keep processing the data.

The last hypothesis is that of a choice made by the data subject in case of unlawful processing. Why only unlawful processing, why not when withdrawing consent? A restricted processing, i.e. simply the retention of data, would be particularly useful when processing data for marketing purposes (see the examples of Robinson lists or orange lists, hereunder at point 4.4.3. Data subjects can choose to see their data included in those lists to avoid it being used again for marketing purpose. It is a clear example of restricted processing of data. But before asking to be included in these opt-out lists, the processing of data was not unlawful.). It is difficult to understand the limitation of that hypothesis of restricted processing.

These cases of restricted processing are welcome but are insufficient to offer the necessary nuanced solutions to a legitimate exercising of the right to be forgotten. The above-mentioned list of solutions should be available for the data subject, the controller and the authority potentially invited to find a balanced result in case of disagreement between both parties.

4.4.2. Information to third parties

The reasoning made in case of withdrawal of consent is fully valid for the other grounds of the right to be forgotten. See point 3.2. *supra*.

4.4.3. "[…] the controller shall not otherwise process such personal data"

Except for the limited and mainly temporary cases of article 17, § 4, the right to be forgotten means, as guaranteed in the Regulation proposal, a right to erasure. So data should be deleted, destroyed once a data subject exercises his/her right to be forgotten.

We know that one of the grounds of the right to be forgotten is when the data subject objects to the processing of data, pursuant to article 19 guaranteeing the right to object. However, article 19.3 provides a different effect of the right to object than erasure. It states that "*Where an objection is upheld,* [...] *the controller shall no longer use or otherwise process the personal data concerned*". In consequence, the right to object is not totally equivalent to a right to delete one's personal data. It amounts to a right to cease the processing of the involved data. It is true that in many cases this will imply to erase the data since a processing includes the storage of data. But it will not systematically be the case.

In the direct marketing sector, for example, the data subject who objects to direct marketing by phone will be put on a special list of persons whose phone number may not be used for direct marketing purposes (called for example 'orange list' or 'Robinson list'). This well-admitted system is in fact more a system of restricted processing than of stopping processing since, as said before, storage of data is one of the operations listed in the definition of "processing"[64].

[64] Article 2, b) of directive 95/46 and article 4.3 of regulation proposal.

The Parliament LIBE Committee has proposed that "*it should be clarified that the right to object, if upheld by the data subject, should result in the erasure of the data by the controller"*[65]. Even if this would lead to apparent consistency between articles 17 and 19 as regards the result of exercising both rights, it is perhaps not the best thing to do.

The restricted processing of data, limited to retention, could indeed be opportune, as seen in the example of direct marketing and if one considers the requirement of article 17, § 8 of the Regulation proposal. This provision states in terms very near to article 19: "*Where the erasure is carried out, the controller shall not otherwise process such personal data."* This provision seems actually strange. Saying "where the erasure is carried out" raises a problem. Once you have erased data, deleted it, how could you still otherwise process it? Why do you need to be told not to do anything with something you do not have anymore? The only way to give sense to this § 8 is to understand that you are required not to process the same data in the future if you happen to be in contact with it again. The way to respect such a requirement is precisely to retain data in view of checking future processing of data to possibly expurgate the "erased" data and be sure not to actively process it.

4.4.4. *Relation between articles 17 and 19 of the Regulation proposal in case of disagreement about an objection*

The relation between Article 17 and Article 19 as to the practical consequences in case of disagreement about the objection should also be clarified. What can be done with the data in dispute? Deletion, restricted use?

According to the EDPS, "*it is not made explicit what the controller is supposed to do with the data if there is disagreement with the data subject and no decision by, for instance, a supervisory authority has yet been taken. From Article 17(1)(c) it seems to follow that the data should in principle be erased […]. It is not clear whether the exceptions provided in Article 17(4)(b), which allow the restriction instead of erasure of data, can be invoked if there is disagreement about whether the right to object should be upheld*."[66]

Here again, provisory restricted processing till the decision solving the disagreement would be the right answer.

4.4.5. Relation between article 17 and article 5.e) of the Regulation proposal

Article 5, e) expressly requires that data are not « *kept in a form which permits identification of data subjects* » beyond the time necessary for the purposes for which the personal data are processed. This implies anonymisation of data (deletion of the identifying elements) or erasing of it (deletion of the data itself) whereas article 17 does not mention anonymisation as a possible result of the right to be forgotten.

As said above, compliance with article 5, e) should be automatic and not depending on a request from the data subject. Requests would then occur when the controller does not spontaneously comply with this requirement. But it is not coherent to offer one possible result in article 5 that is not present anymore in article 17.

---

[65] Albrecht Report, *op. cit.*, amendment 157.
[66] EDPS Opinion, *op. cit*., § 149.

4.5. Exceptions

As already said, the right to be forgotten is not absolute. Exceptions are listed in § 3 of article 17 of the Regulation proposal. As summarised in recital 53, "*the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law* […]".

4.5.1. What should be allowed? Only retention of data?

Parliament amendment proposals made by members of the Committee on Industry, Research and Energy, intend to widen the admissible operations upon the data when an exception to the right to be forgotten applies. Paragraph 3 of article 17 would state that the controller must carry out the erasure "*except to the extent that the retention* ***and dissemination*** *of the personal data is necessary*" to protect the values listed in this provision[67]. It is true that it ensues from the initial text that only retention of data will be allowed as an exception to erasure. It could be relevant to clarify that where an exception applies, all the operations necessary to protect the higher value should be admissible. This means that dissemination of data could be one of these operations but other justified operations could also be envisaged such as disclosure to restricted recipients (researchers for example) or access to the data,… A drafting correctly reflecting this could be "*except to the extent that* ***processing*** *of the personal data is necessary*".

4.5.2. Relation between article 17.3 and article 21 of the Regulation proposal

The articulation of this provision with article 21 of the Regulation proposal which provides grounds for restrictions to certain articles of the text, including article 17, should be clarified.

It is pretty misleading since the lists of admitted grounds are not the same. For example, freedom of expression is the only individual freedom taken into account in article 17 while article 21, § 1, f) accepts restrictions that aim at "the protection of the data subject or the rights and freedoms of others". It is important to allow to take into consideration the rights of others. For example, if we only rely on article 17 what could we do regarding a request of erasure of data that concerns also other data subjects? If the right to be forgotten is exercised through the right to object, we mentioned earlier the necessity to allow the controller, pursuant to article 19, to demonstrate an overriding interest to refuse to erase data. He should not be limited to the list of article 17, § 3 to contest the request for erasure.

Moreover, to be admissible, the law mentioned at article 17, § 3, b) "*shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued*" whereas according to article 21, § 1, Union or Member State law may restrict by way of a legislative measure the scope of certain articles when such a restriction constitutes a necessary and proportionate measure in a

[67] Kelly Report, *op. cit.*, amendment 495 from Alejo Vidal-Quadras and amendment 496 from Adina-Ioana Vălean, Jürgen Creutzmann.

democratic society to safeguard certain public or private interests. Requirements concerning the law are not completely the same.

In the same line, the EDPS has indicated: "*Article 17(3) provides grounds for an exception to erase the data without delay. This paragraph duplicates, and hence has no added value for, the system of exemptions, restrictions and specific rules already foreseen in the proposed Regulation (see also the comments in part II.2.a.(iii)). In particular Article 17(3)(d) will only create confusion. A restriction of the purpose limitation principle and of the rights of the data subject (including Article 17) should be based on Article 21, subject to the comments made in part II.5.f below. Therefore, the EDPS recommends deleting Article 17(3).*"[68]

Parliament members' propositions of amendments show their uneasiness towards the strange list of article 17.3 of interests deserving to be taken into consideration to refuse to erase data. Different propositions ask to add to that list the "*prevention or detection of fraud or other financial crime, confirming identity, and/or determining creditworthiness*"[69] (which is useless since this would be covered by article 21), the "*keeping [of] documentary evidence of a given case history, when the data controller is a public authority*"[70] (idem), or other situations in fact entering into the scopeof article 21[71]

The Albrecht Report expresses a general statement on the uselessness of § 3: *"The exceptions in paragraph 3 are only a duplication of the general limitations in Article 21 and do not add any value here"*[72]. But surprisingly no consequence is drawn from this statement in the text itself. There is no indication whether this § 3 should simply be deleted since it has no added-value.

5. Right of automatic deletion of the data in the electronic environment

In response to the new developments of Internet services and to the problematic situation deriving from the specificities of the Internet pointed out in point 1.2 of this paper, the same proposition has been made in different political, institutional or experts circles to grant data subjects an automatic right to be forgotten after the expiration of a certain period of time.

It has been proposed notably by the European Data Protection Supervisor to widen the existing right to be forgotten so as to ensure that the information automatically disappears after a certain period of time, even if the data subject does not take action or is not even aware data concerning

---

[68] EDPS Opinion, *op. cit.*, § 149.

[69] Comi Report, *op. cit*., amendment 122; the same amendment proposal in European Parliament, Opinion of the Committee on Employment and Social Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) Rapporteur: Nadja Hirsch, 4 March 2013, amendment 499 from Adina-Ioana Vălean, Jürgen Creutzmann, Jens Rohde.

[70] This specific additional exception is also proposed in the Hirsch report. They propose not considering it as an exception added in the list of § 3 but adding a new paragraph – very poorly drafted – and unfortunately without any justification: "6 a. While complying with the data requirements of this Regulation, especially privacy by design, the provisions in paragraph 4 and 6 of this Article do not change the right of public authorities to store data for documentary evidence of a given case history." (Hirsch report, *op. cit*. amendment 10).

[71] Kelly Report, *op. cit*., Amendment 481 from Eija-Riitta Korhola; amendment 500 from Adina-Ioana Vălean, Jürgen Creutzmann, Jens Rohde.

[72] Albrecht Report, *op.cit.*, justification given p. 99 with no link with the amendment proposal it is supposed to justify.

him was ever stored.[73] The Deputy-Secretary General of the Council of Europe reached the same conclusion: "The increase in storage and processing capacities enables information concerning an individual to circulate within the network, even though it may no longer be valid. This makes the current principles of accuracy and proportionality of data obsolete. *A new right to oblivion or automatic 'data erasers'* would enable individuals to take control over the use of their own personal data."[74] The Vice-President of the European Commission, V. Reding, said in her turn: "I want to introduce the 'right to be forgotten'. Social network sites are a great way to stay in touch with friends and share information. But if people no longer want to use a service, they should have no problem wiping out their profiles. The right to be forgotten is particularly relevant to personal data that is no longer needed for the purposes for which it was collected. *This right should also apply when a storage period, which the user agreed to, has expired*."[75]

These similar propositions amount to attribute some kind of expiration date to the data without need for a prior analysis on a case by case basis. A certain period of time could be fixed, for example, for data stored on terminal equipments such as mobile devices or computers: data would be automatically deleted or blocked after the fixed period of time if the equipments are no more in the possession of their initial owner.

This system already applies in some States for certain files or registers such as criminal files and police registers. This encounters what the European Court of Human Rights has underlined in the *Rotaru* case : data pertaining to the distant past of an individual raises a particular concern as regards the "private life" protected by Article 8, § 1 of the ECHR. It should not be kept without a very strict analysis of the necessity as regards democratic requirements.[76]

The automaticity of the deletion or of the prohibition to further use would need to be translated into a "privacy by default" setting for the processing of personal data. In this sense, aside the right to have one's data erased on request, the right to be forgotten could turn to become a ' 'data protection by default' rule. Article 23.2. of the Regulation proposal provides that "the controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not […] retained beyond the minimum necessary for those purposes, […] in terms of […] the time of their storage"[77]. Moreover, article 17, § 7 asks in the same sense the controller to implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.

Technical mechanisms should thus foresee that data storage automatically comes to an end as soon as the time necessary to achieve the announced purposes has passed.

---

[73] European Data Protection Supervisor. (2011). Opinion on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions "A comprehensive approach on personal data protection in the European Union". 14 January 2011, § 85.

[74] Council of Europe, Deputy Secretary General. (2010). Speaking Points for the Opening the 21st T-Pd Bureau Meeting. Strasbourg: 15 November 2010. http://www.coe.int/t/dghl/standardsetting/dataprotection/151110%20DSG%20speaking%20notes%20data%20protection%20meeting%20T-PD.pdf (our italics)

[75] REDING, V. Vice-President of the European Commission, responsible for Justice, Fundamental Rights and Citizenship Privacy matters. (2010). "Why the EU needs new personal data protection rules?". The European Data Protection and Privacy Conference, Brussels, 30 November 2010, http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700 (our italics).

[76] E.Ct.H.R., *Rotaru v. Romania*, 4 May 2000, appl. no 28341/95. See also the concurring opinion of Judge Wildhaber joined by Judges Makarczyk, Türmen, Costa, Tulkens, Casadevall and Weber.

77 Also Article 17, § 7 : 'The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.'

Such possibilities to implement an automatic system of destruction of data with the data subject's consent already exist.[78] As an illustration of such a system, the software X-Pire has been launched in Germany. It enables users to attach a digital expiry date to the images uploaded to social networking sites like Facebook.

It is clear that such a technical way of achieving the right to be forgotten cannot offer an adequate answer in all circumstances where the data subject would like to benefit from the right to be forgotten. First, because cases like the withdrawal of consent and the objection to the processing of data cannot be foreseen and turned into a systematic expiry date. Secondly, because the data subject does not necessarily want to see his/her data erased. He could rather prefer to ask for the abstention of further dissemination, for example (see *supra*).

Nevertheless, such a technical answer would contribute to shift the balance in favour of the data subject since the latter would beneficiate from the protection without having any initiative to take. This is particularly important in a context as opaque as the Internet. Many of data processing occurring in that sphere are totally out of the data subjects' consciousness. It is illusory in that case to guarantee to the individuals a right they would never think of using.

Conclusive remarks: right to be forgotten and right to erasure, one or two rights?

Article 17 is entitled "Right to be forgotten and to erasure". One inevitably wonders whether article 17 establishes two separate rights. This seems not to be the case. These two rights seem merged in the view of the authors of the Regulation proposal[79].

But this way of presenting things raises problems. According to certain Parliamentary members, "The title proposed by the Commission is misleading"[80]. They would like to abandon the words "right to be forgotten" and keep only the "right to erasure" in the title as well as in the text of article 17.[81] On the contrary, other members of Parliament, in the LIBE Committee, prefer referring to two rights.[82]

It ensues from the analysis made hereunder that maintaining two different rights would be preferable. The right to be forgotten should not be reduced to a right to erasure. Things are more nuanced.

The right to obtain erasure of data is to be understood as a tool to react against non-compliance with the regulation requirements. It covers two of the four grounds listed in article 17 of the Regulation proposal: when the processing of the data does not comply with the Regulation (art. 17.1.d) and when the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed (art. 17.1.a). This second hypothesis is also a problem of non-compliance since normally data should not be retained in a form which permits identification of data subjects beyond the period necessary to achieve the purpose of the processing. Data subjects should not need to act to obtain that. Exercising his/her right to

[78] (http://www.x-pire.de/index.php?id=6&L=2)
[79] See recital 54: "To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended […]". See also Opinion of the European Data Protection Supervisor on the data protection reform package (*op. cit.*, point 146): "The right to erasure has been strengthened into a right to be forgotten to allow for a more effective enforcement of this right in the digital environment."
[80] Comi Report, *op. cit.*, amendment 118.
[81] Kelly Report, *op. cit.*, amendment 479 from Amelia Andersdotter; amendment 480 from Adina-Ioana Vălean, Jürgen Creutzmann, Jens Rohde; Comi Report, *op. cit.*, amendment 118.
[82] Albrecht Report, *op. cit.*, amendment 34.

erasure would only be necessary if the controller does not spontaneously comply with this requirement.

This right to erasure is indispensable. It is presently provided in article 12, b) of directive 95/46, together with the right to rectification. It must certainly be kept in the new text. It is a means of action for the data subject towards unlawful operations performed upon personal data concerning him/her.

But the right to erasure does not completely fulfil the right to be forgotten. As we have seen, the latter can cover situations of data processing which are in principle totally lawful where it rests on the two other grounds of article 17: the withdrawal of consent (art. 17.1.b) and the objection to processing of data (art. 17.1.c).

Furthermore, results of exercising the right to be forgotten should be much more nuanced than just obtaining the deletion of the contested data or imposing a restricted processing of it. We have seen *supra* that in view notably to reach a fair balance between the competing values, this right to be forgotten could turn to be a right to erase data, but also a right to anonymisation (to erase only the identifying data[83]), or a right to erase the electronic links towards personal data (in order to efficiently fight against de-contextualisation of data while maintaining the data available inside the original circle and context), or a right to restrict dissemination (on social network sites, for example). This last way of achieving the right to be forgotten could mean either the controller abstention of further dissemination or the data subject choice of certain forms of publicity instead of others.

The right to be forgotten, unlike the right to erasure, rests on grounds guaranteed somewhere else in the Regulation: the withdrawal of consent and the right to object. It could also be based on the right to erasure if this one were to be guaranteed autonomously (especially where data is retained beyond the authorised period). This observation raises the question of the added-value of the recognition of a specific right to be forgotten. What does article 17 bring in terms of specificities as regards the right to be forgotten?

This provision clarifies, and could do it even better, the effects of mobilising the various grounds. The fact that a provision is devoted to the right to be forgotten should offer the context for envisaging the necessary wide range of effects that should be provided[84].

The duty to inform persons processing data downstream from the making public of that data by the controller is another element that justifies a separate article to guarantee the right to be forgotten. The reflections made here-above about the necessity to widen this duty to cases where *disclosure* of data occurred instead of *public availability* of it are to be recalled. Anyway, it is certainly an opportune tool in the online context characterised by its radical opacity. Where it is reasonably feasible, the controller will have to warn further users of the contested data. He has better chance to know these persons or to get in contact with them than the data subject, especially if he has a contractual link with them.

[83] One must be conscious of the limits of the process of anonymisation and of the existing risk of de-anonymisation. These limits and problems cannot be further developed in the present paper.

[84] One must admit that this legislative work could be done when considering the articles concerning each of the different grounds.

The text was written as result of JRC appointment letter no. 257972 -14 January 2013 to Prof. dr. Cécile de Terwangne University of Namur, Belgium.

European Commission
EUR 26434 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: The Right to be Forgotten and the Informational Autonomy in the Digital Environment

Author: Cécile de Terwangne

2013 – 28 pp. – 21.0 x 29.7 cm

EUR – Scientific and Technical Research series – ISSN 1831-9424

ISBN 978-92-79-35086-3

doi: 10.2788/54562

Abstract

The right to be forgotten, equally called right to oblivion, is today at the heart of intense debate in high level spheres. The European Union legislators have been discussing the relevance of such a right in the digital environment since months, the Council of Europe authorities have expressed their concern on the subject, national politicians raised their voices, data protection authorities, entities working in the field of human rights, academics and experts have joined the procession coming from different geographical horizons.
It is important to rightly understand what is really meant by the right to be forgotten. The idea is not to allow someone to re-write the past and to erase (unpleasant) traces of his/her time on earth. The idea is to see to it that someone's present is not cluttered up by his/her past.

LB-NA-26434-EN-N

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle. Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

ISBN 978-92-79-35086-3