Chapter 9
Online Social Networks and Young People's Privacy Protection: The Role of the Right to Be Forgotten

Rachele Ciavarella and Cécile De Terwangne

Contents

Rachele Ciavarella is a lawyer with ICT Legal Consulting Law Firm and a Blue Book Trainee at EU Commission DG CNECT Unit H4 Trust and Security. Cécile De Terwangne is a professor at the Law Faculty of the University of Namur (Belgium) and Research Director in the 'Freedoms in the Information Society' Unit of the Research Centre in Information, Law and Society (CRIDS—University of Namur).

R. Ciavarella (✉)
CRIDS—University of Namur, Namur, Belgium
e-mail: rachele.ciavarella@unamur.be

C. De Terwangne
Faculty of Law, CRIDS, University of Namur, Namur, Belgium

S. van der Hof et al. (eds.), *Minding Minors Wandering the Web: Regulating Online Child Safety*, Information Technology and Law Series 24, DOI: 10.1007/978-94-6265-005-3_9,

9.1 Introduction

A number of social studies have shown that children and young people[1] are increasingly interested in new technologies, and especially in new forms of communication and socialisation.[2] According to a recent study[3] conducted by the EU Kids Online network,[4] 38 % of 9–12 year olds and 77 % of 13–16 year olds have a social networking service (SNS) profile. The way they "feed" these profiles and use the SNS is inevitably influenced by their young age. Moreover, the above-mentioned study has demonstrated that younger children are more likely to have a "public" profile.

Young individuals often do not envisage the long-term consequences of the content that they spontaneously make public. They do not fully comprehend the power of search engines to allow access to any piece of information removed out of its initial context. The majority of youths do not consider the possibility that the content they communicate (be it text, photographs or video) may be copied and stored on third-party computers, fundamentally outside their control. Above all, they are largely unaware of the "eternity effect"[5] of electronic memory. Additionally, when surfing the Internet, children are commonly unconscious that they leave traces of their activity, similar to tattoos, which are rather difficult to remove.

Combined with the actual practical difficulty of content removal once published online,[6] this means that as adults such individuals may suffer life-long consequences of an image influenced by their online activities as teenagers.[7] The consequences are thus multiple. In today's society, digital reputation is at least as important as one's "real life" profile.[8] A negative *e-reputation* has the potential to create significant problems for children and young people who do not exercise

---

[1] For the purposes of this document, the term "young people" will refer to legal minors. The meaning of legal minor depends on the jurisdiction in which the service is offered; normally this refers to users under 18 or 16 years of age. However, in the General Data Protection Regulation (see *infra)*, while Article 4(18) states that 'child' means any person below the age of 18 years, Article 8.1 (Processing of personal data of a child) outlines that *the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian*.

[2] Casarosa 2010, available at http://ssrn.com/abstract=1561570.

[3] Livingstone et al. 2011, available at http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/ShortSNS.pdf.

[4] EU Kids Online is a multi-national thematic network, founded by the EC Safer Internet Programme, that aims to stimulate and coordinate investigation into the use of new media by children, www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx.

[5] Walz 1997, p. 3.

[6] For an example of reported cases about people seeking to have their data deleted from a social network and facing practical difficulties, see http://online.wsj.com/article/SB10001424052748703396604576087573944344348.html.

[7] See for example Mayer-Schönberger 2009.

[8] Legrand and Bellamy 2012, www.lesnumeriques.com/divers/touche-pas-a-e-reputation-enquete-a1548.html.

correct control in the use of social networks. Moreover and not insignificantly, the digital traces that they leave behind are easily used for behavioural and contextual advertising.

Due to the expanding possibilities to collect, store and use personal data,[9] we have dismantled the world in which our past is "forgettable" and we have begun to live in a society of permanent memory. The development and diffusion of Information and Communication Technologies has increased simultaneously with the need for an adequate level of privacy on the Internet. Taking such notions into account, in 2009 the Vice President of the European Commission, Viviane Reding, announced her intention to review the 1995 Data Protection Directive[10] and to include a separate "right to be forgotten". She stated, "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 and more private data floating around the Web—especially on social networking sites—people should have the right to have their data completely removed."[11]

Section 9.2 of this chapter will analyse the role of the right to be forgotten, also called the "right to oblivion", in the field of online social networking sites. Section 9.3 outlines the role given to the right to oblivion in the Data Protection Directive of 1995, while Sect. 9.4 focuses on the potential and the limitations of the recent Proposed General Data Protection Regulation that is intended to replace this Directive.[12]

As will be demonstrated, the issue of the right to be forgotten primarily revolves around the conflict between this right and the right to freedom of speech, the duty to remember and marketing purposes.

9.2 The Role of the Right to Be Forgotten

What is the right to be forgotten? Neither the 95/46/EC Directive nor the Proposed General Data Protection Regulation provide any clear definition or description of what the right to be forgotten clearly consists of. However, in its important communication preceding, the revision process of the general legal text on personal data protection, the European Commission refers to the right to be forgotten as "the right of individuals to have their data no longer processed and deleted

[9] 'Personal data' means 'any information relating to an identified or identifiable natural person ("data subject")' (Article 2, a) of the directive 95/46).

[10] Directive 95/46/CE 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, OJ, 23 November 1995, L281/31.

[11] Reding 2010.

[12] 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).

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."[13]

Could the application of such a 'right to have their data deleted' offer adequate protection to children and young people in the field of SNS?

In this day and age forgetting is difficult, if not impossible. The basic idea of informational self-determination[14] has limits.[15] On the Net it appears that we are indeed prisoners of our past. Control of the fate of the data that has been shared in certain circles and control of what is circulated tends to be an illusion. This is notably due to the frightening efficiency of search engines to examine the Web in its entirety and to bring the slightest piece of information to the surface, often out of its initial context.[16] The content that one agrees to disclose to certain recipients, because they belong to a determined circle (friends, family, members of an interest group, etc.), is expected to be inaccessible to others. However, in order to erase what has been said or shared about us on the Internet, or even what we once shared ourselves, represents a pure challenge. This notably derives from the architecture of information systems that have become increasingly complex, with numerous links rendering any deletion of data both tricky and expensive, similar to a Sisyphean activity.[17] It has been demonstrated that on an SNS a user's loss of control is observed at three levels: the creation of personal data, their accessibility and their deletion.[18]

The situation is even worse when the data subject is a child, wholly ignorant of the mechanisms through which the information he "posts" on the Internet can be spread or further transmitted. It is also often the case that the said child simply does not care about the risks of divulging such information. The risks are, however, very real as is demonstrated by the misadventure of an American student who was denied the possibility to graduate from college due to the discovery, on a social networking site, of a post criticising her supervisor and a photo of herself wearing a pirate hat, holding a cup inscribed with the words "drunken pirate".[19] Additionally, innumerable job candidates are refused positions after simple and rapid Internet searches, all too often revealing compromising pictures posted by the individuals when they were mere teenagers.

---

[13] European Commission Communication, 'A comprehensive approach on personal data protection in the European Union', 4 November 2010, COM (2010) 609 final, p. 8.

[14] Informational self-determination means control over one's personal information, that is to say the individuals' right to decide which information about themselves will be disclosed, to whom and for which purpose. See De Terwangne 2012, p. 112, also available at www.idp.uoc.edu.

[15] See Rouvroy 2008, available at http://works.bepress.com/antoinette_rouvroy/5/.

[16] On the risk of de-contextualisation in SNS, see Dumortier 2009, available at http://works.bepress.com/franck_dumortier/1.

[17] De Terwangne 2012, p. 112 and 117, also available at www.idp.uoc.edu.

[18] Moiny 2012.

[19] Copeland 2012, p. 1.

The 'perfection' of the memory of the Internet is contrasted with the imperfections of the human memory. The eternity effect of the Internet preserves past errors, memories, photos and videos that have been 'posted' on the Web and that we would often, at a later stage, like to cancel.[20] The right to be forgotten may appear to be a solution that 'cleans' our past, our errors, and consequently preserves our digital reputation. It is a legal way to reintroduce oblivion in social life. It raises serious concerns, however, regarding the possibility of individuals to rewrite their own history. It should not be considered nor built, then, as a way of having elements of one's past completely disappear on a whim of desire. We observe, under Sect. 9.4.2, that this right must indeed face serious limits.

As outlined before, Sect. 9.3 will focus on the elements of what the right to be forgotten could be, as found in the Directive 95/46/EC, Sect. 9.4 will deal with the right to be forgotten under the Proposed General Data Protection Regulation.

9.3 The Right to Be Forgotten Under the Directive 95/46/EC on Data Protection

The right to be forgotten is not evoked as such under the Directive 95/46/EC on data protection. As previously stated, no definition of the right to oblivion appears in the text. Can this logically bring one to conclude that such a right has little or nothing to do with the Directive and is a sort of non-legally-binding principle? Shall we then consider the concept of the right to be forgotten as a new principle, or instead as an old principle only phrased differently?

While the concept is not present as such in Directive 95/46/EC, we find elements of what could be considered a right to oblivion in the current European Union data protection framework. The first element ensues from the so-called principle of purpose.[21] The purpose principle states that personal data must be processed for a determined, legitimate and transparent purpose. Moreover—the most interesting point here—this that the principle specifies that personal data must not be kept longer than necessary for the purposes for which it was collected or further processed. A sort of right to oblivion is therefore directly attained by the means of this principle.[22] According to the EU Data Protection Directive, personal data should be anonymised or deleted once the purposes for which it was processed have been achieved. This rule clearly establishes a right to oblivion in the sense that data is not supposed to remain in the hands of the controller eternally.

In addition, Article 12(1)(b) allows the data subject to demand the rectification or the deletion of their data when the processing of it is not in compliance with the Directive. If personal data is kept longer than what is allowed on the basis of the

[20] De Terwangne 2012, p. 110.

[21] Article 6(1)(b), (e) of the 95/46 Directive.

[22] De Terwangne 2012, p. 114.

purpose principle, the data subject may get such data erased. The current European Union framework provides sanctions in the case of infringement of these rules.[23]

These elements may be regarded as illustrative forms of a right to be forgotten in the Directive. They give the data controller[24] the role of verifying whether or not data is necessary for the purposes of the processing and whether the personal data should be deleted or anonymised. The right to be forgotten in this sense is assimilated to a right to deletion (of the data or at least of the identifying elements of it), inherent to the legal system of protection of personal data. The data subject does not have to do anything in order to have his/her data erased or anonymised. The data controller is the main actor in the right to be forgotten while the data subject is simply given a tool to see to it that the rule is respected and to obtain erasure of data in the case that the controller has not erased or anonymised it spontaneously.

There is another way of achieving the right to be forgotten in the Directive: through the right to object to the processing of personal data. This right is stated in Article 14 of Directive 95/46/EC. Data subjects have the right "to object at any time on compelling legitimate grounds relating to [their] particular situation to the processing of data relating to [them]. Where there is a justified objection, the processing instigated by the controller may no longer involve those data."[25] In this case, the active role is deferred to the data subject. The continued processing of personal data is considered legitimate until the data subject intervenes, unlike the case when data is kept after the necessary period to achieve the purposes of processing.

Both ways come to the conclusion that data processing is considered legitimate until a certain and specific moment: either when the purpose of processing is achieved (which includes the legal period of data retention for purposes of proof), or when the data subject objects on a compelling legitimate ground relating to his/her particular situation.

Notwithstanding the importance of the elements of a right to oblivion established by the Data Protection Directive, it shall be observed that the framework created in 1995 is old (adopted just before the societal diffusion of the Internet) and the provisions previously mentioned do not grant the data subject perfect and complete control over their data.[26] Should an individual object, for example, to the processing of his/her data, the individual must present compelling legitimate grounds. The "compelling" nature of the grounds is difficult to assess by someone outside of the processing. This difficulty has been taken into consideration in the Proposal of the General Data Protection Regulation, as will be seen below.

---

[23] Article 24 of the 95/46 Directive.

[24] A "controller" is "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; […]" (Article 2, d) of the Directive.

[25] Article 14(1)(b) of the 95/46 Directive.

[26] Copeland 2012, p. 4.

Rapid technological developments have brought new challenges to the protection of personal data. Consequentially, it has been heavily debated whether or not it is appropriate to envisage an extension of the existing bits of the right to be forgotten in response to certain Internet specificities, particularly those linked to social networking services. As a result of the development of the Internet environment and of the limitation of current legislation, the European Commission, in its communication entitled "A comprehensive approach on personal data protection in the European Union",[27] concludes that the European Union needs a more comprehensive and coherent policy regarding the fundamental right to personal data protection.

9.4 The Right to Be Forgotten Under the Proposal for a General Data Protection Regulation

Due to the compelling developments in ICT since 1995 including the digitalisation of content and the proliferation of information, the need to revise the current legislative framework has become obvious. Concerns regarding the necessity to develop a genuine "right to be forgotten" have notably ensued from the multiplication of misadventures linked to SNS with the realisation that individuals may suffer grave consequences after the spontaneous disclosure of information at earlier stages. This is particularly evidenced upon understanding that it is impossible to entirely erase data once it is posted on Facebook.[28] The modification of the existing legislation revolves around the question of granting Internet users the possibility to take initiative regarding their personal data, and the possibility of deleting their data from websites, blogs and social networking sites.[29] The idea to attach a sort of expiration date to the data so that they are no longer usable after a certain time is also at issue.

9.4.1 An Article Specially Devoted to the Right to Be Forgotten and to Erasure

Article 17 of the Proposal for a General Data Protection Regulation[30] grants data subjects the right to have their personal data erased[31] when the data are no longer

---

[27] COM(2010)609 final.

[28] Van Alsenoy et al. 2009, pp. 65–79.

[29] Gomes de Andrade 2012, p. 124.

[30] Article 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*

necessary for the purposes for which the data were collected or otherwise processed, where the data subject has withdrawn this/her consent for processing, when the data subject has objected to the processing of personal data concerning them or when the processing of their personal data otherwise does not comply with the rules set forth in the Regulation.

The situation does not differ considerably from that discussed above given that the purpose principle and the right to object are already present in Directive 95/46/EC. The right to object, however, will be more easily executed by the data subject as the grounds that he/she must present when objecting must no longer be "compelling and legitimate". Instead they must only relate to the particular situation of the data subject.[32] Recital 56 clearly states that "The burden of proof should be on the controller to demonstrate that their legitimate interests may override the interests or the fundamental rights and freedoms of the data subject".

On the other hand, what is openly welcomed is the clarification of the possibility to withdraw previously given consent. This is a key tool related to social networks as data processing in such a context partly relies on the consent of the data subject. The authors of the proposed Regulation 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."[33] That being said, one does not see the legal implication of saying that data subjects have the right to obtain the erasure of personal data on the part of the data controller, "especially in relation to personal data which are made available by the data subject while he or she was a child," as included in Article 17 of the Draft Regulation. Should it then be more difficult for the controller to demonstrate that its legitimate interest

(Footnote 30 continued)
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. (emphasis added).

[31] Article 17 is entitled "Right to be forgotten and to erasure". One could wonder whether Article 17 establishes two separate rights. This is not the case as these two rights are merged in the view of the authors of the Regulation Proposal (see recital 54: "To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended […]." Also Opinion of the European Data Protection Supervisor on the data protection reform package (7 March 2012, 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".

[32] 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".

[33] Recital 53 (emphasis added).

overrides the data subject's interests when the data were made available when the latter was a child? The draft report of the Parliament on the Regulation Proposal has, in the same sense, stressed that there appears to be little specific value to demand 'particular' attention for children.[34] The Parliament is, in fact, concerned that this portion of text could implicitly lessen protection for adults.

To strengthen the 'right to be forgotten' on the Internet, Article 17.2 provides that, in case the data controller has made the personal data public or has authorised a third party to publish the personal data, he will be obliged to take all reasonable steps, including technical measures, to inform third parties who are processing such data, of the request from the data subject to erase any links to, or copies/replications of such personal data. Many commentators, among which is the European Data Protection Supervisor,[35] have noted that it may, in some cases, be an extensive effort to inform all third parties that may be processing such data, and that there will not always be clear understanding of where the data may have been disseminated. This is clearly the case with Internet pages open to the public. It should not, however, be applicable to the responsible operators of a social network having to warn application developers who process the data available in the network. Nevertheless, the "obligation of *endeavour* upon the controller is surely more realistic from a practical point of view than an obligation of *result*".[36]

A rapid analysis might lead us to believe that our children will now freely return to making mistakes and that as parents we can stop fearing that what they say may be used against them in the future.[37] But the right to be forgotten as outlined in the Proposal of Regulation indeed has limits.

9.4.2 Limits

1. The personal and household exemption

First of all, data protection principles, including the right to be forgotten, do not apply to individuals who process personal data exclusively for their own personal and domestic purposes. The application of this exemption to social networking sites has led to a fervent discussion.[38] What is the definition of personal or household activity? In the *Lindqvist* case, the European Union Court of Justice

[34] 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.

[35] Opinion of the European Data Protection Supervisor of the data protection reform package, 7 March 2012, p. 148.

[36] Opinion of the European Data Protection Supervisor of the data protection reform package, 7 March 2012, p. 147.

[37] Koops 2011, available at www.ssrn.com.

[38] Moiny 2010, pp. 250–253; Van Alsenoy et al. 2009, pp. 65–79.

stated that the exception must be interpreted as relating only to activities which are carried out in the course of the private or family life of individuals, which is clearly not the case with the processing of personal data published online as those data are made accessible to an indefinite number of people.[39] Applied to the SNS context, this reasoning leads one to say that SNS users will not benefit from the exemption for personal use when their profile is 'public'. It is, however, debatable whether situations where access to data posted by a user is limited to self-selected contacts (e.g. friends) may benefit from this exception. In some cases users have an extensive number of contacts/friends, some of whom they may not actually know. "A high number of contacts could be an indication that the household exception does not apply."[40] Yet is there a minimum number of 'friends' one must have on a social network in order to be covered by data protection rules when the access is restricted by the use of privacy settings? Of course no such numerical threshold exists. The quality of the link with the recipients must also be taken into account. A sufficiently personal connection should thus be established in order to be exempted from data protection rules. In fact, it may also be argued that the publishing of information on sites such as Facebook, even if for purely personal reasons and even when restricted to a confined circle of persons, involves the disclosure of information and the storing of it by the *host*, in this case Facebook, an aspect that affects the application of the exemption. Finally, it should be clarified that what the social networking site does on its own initiative (copies of data, processing of data for marketing purposes, etc.) is not covered by the exemption.

To summarise, the right to withdraw one's consent or to object to the storage and publication of data cannot be invoked in situations where the personal exemption applies, i.e. in SNS cases where individuals disclose data and pictures inside a confined circle of *real* friends, family or relatives. Other legal tools from both civil and criminal law are then at the possible disposal of data subjects. An exemption for journalistic and artistic purposes as well as for literary expression also exists.

If the exemption for personal use does not apply, one must consider that the exception for journalistic purposes, artistic or literary expression may instead apply.

In the *Satamedia case*, the European Court of Justice provides a very broad understanding of what is to be covered by 'journalistic purposes'. For the Court this notion encompasses all activities whose objective is to disclose information, opinions or ideas to the public, irrespective of who carries out such activities (not necessarily a media undertaking), and of the medium used to transmit the processed data (it may be an electronic medium such as the Internet) and irrespective of the nature of those activities (profit-making or not).[41]

---

[39] ECJ, 6 November 2003 (*Lindqvist*), C-101-01, *Rec*. p. I-12971, § 47.

[40] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, WP 163, p. 6.

[41] ECJ, 16 December 2008, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, C-73/07. See comment of this case by De Terwange 2008, *Satakunnan Markkinapörssi Oy et Satamedia Oy,* Affaire C-73/07, *R.D.T.I*., 2010, n° 38, pp. 132–146.

The second part of the exception concerns the processing of personal data carried out solely 'for the purpose of artistic or literary expression'. The outline of this exception is still to be enlightened by the case law.

In the case that the first or second part of the exception is considered to apply to SNS activities, a balance between the freedom of expression and the rights of the data subject needs to be struck.[42]

2. Conflicts with other rights and interests

The right to be forgotten is not an absolute right. In fact, it is in major conflict and permanent tension with other rights and interests including the right to free speech, the right to information[43] and the duty to remember.[44] The question remains: "[s]*hould we have the right to remove … things from the Web or allow them to let be for the whole world to see until eternity…?*"[45]

Resolving such a conflict demands that the proportionality principle be respected. There should be no a priori and systematic pre-eminence given to one right over the others. A balancing test must be made in every case. It is true that where information regarding the life of a young person is at stake, most of the time priority will be given to the data subject's interest to erase it. There is indeed little chance that such information be linked to questions of public interest.

The proposed Regulation allows the further retention of personal data notably where it is necessary to exercise the right of freedom of expression, or for historical, statistical and scientific research purposes.

The text also provides that there may be cases where one could prefer restricting the processing of the data instead of erasing them. The text is not clear on what is meant by 'restricting the processing'. One should in any case understand that data remains stored but that access to it and use of it is restricted. This way of achieving the right to be forgotten is therefore a perfect illustration of the application of the proportionality principle.

3. Conflict with the economic model of SNS

The use of SNS appears to be free. The very efficient economic model of these services in fact relies on contextual advertising, i.e. the commercial exploitation of the information and digital traces left by users when using the service. SNS operators have an economic interest for not erasing personal data from their services since it represents a considerable economic asset.

---

[42] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, WP 163, p. 6.

[43] In Google's legal advisor's view, there should be no expectation of privacy on the Internet and the right to oblivion represents the biggest threat to Internet free speech in our time, http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html; see also Mayes 2011.

[44] Gomes de Andrade 2012, p. 130.

[45] Daly 2011, available at http://emergingbusinessadvocate.wordpress.com/2011/03/15/le-doit-a-loubli-can-we-achieve-oblivion-on-the-internet/.

The General Data Protection Regulation proposal offers a strict answer to this economic activity when it regards children. Article 20 states that every natural person shall have the right not to be subject to measures based on profiling by means of automated processing. According to recital 58, such measures should be allowed in certain circumstances but never when a child is concerned.

4. Technical limits

In addition to these limitations one must be aware that there are serious technical limits to the implementation of the right to be forgotten: the deletion of data from the web is not as easy as it may appear. In fact, once data is removed by the controller, the information could be still available in cache memory. Moreover, during the time that data are available online, other individuals may download and re-publish the information without the data subject's consent, even without them being aware of such an action. At this point effective removal of the data could present intensive difficulties.[46] 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 to know who may be processing such data.[47] Entering in contact with these persons could therefore prove to be rather difficult or even impossible. In the same sense, the European Data Protection Supervisor and the Article 29 Working Party have welcomed the introduction of the right to oblivion but they have emphasised the necessity and challenge of its correct implementation.[48]

9.4.3 The Right to Be Forgotten by Default

Aside the right to have one's data erased upon request, the right to be forgotten could rely on the 'data protection by default' rule. Article 23.2. 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".[49] Article 17.7 more specifically asks 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.

---

[46] De Terwangne 2012, p. 117.

[47] See ENISA 2012, available at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/.

[48] Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012, p. 24 and Article 29 Working Party Opinion 01/2012 on the data protection reform proposals, 23 March 2012, WP 191, p. 13.

[49] 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."

Technical mechanisms should thus foresee that data storage automatically comes to an end as soon as the time necessary to achieve the purposes announced has been reached. It is important that social networking sites very carefully identify the different purposes linked to the processing of data as the time of retention will be determined accordingly. For example, certain sites keep all the data of individuals who choose to no longer utilize the given network, "sparing them the trouble of re-uploading everything if they want to come back". Even if one happens to consider this to be legitimate, it is clear that the retention time in such a case must be rather short. In cases where someone erases his/her messages exchanged via the SNS, there should be no justification to store these messages any longer given that the purpose of communication has expired and so has the time of storage.

In fact, the market already offers such possibilities to implement an automatic system of destruction of data with the data subject's consent.[50] 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 such as Facebook.

9.5 Conclusion

In a society where we are never truly forgotten, the right to oblivion represents a possible solution to problems raised by the "perfect" memory of the Internet combined with the power of search engines that lead to a de-contextualisation of data, notably data disclosed and processed within the framework of SNS.

Elements of a right to be forgotten are present in the current Data Protection Directive 95/46/EC. Rapid changes in the digital environment, and notably the impressive development of SNS, have highlighted the need to reconsider such an answer and to build a specific and augmented right to be forgotten. This new concept has appeared in the Proposal for a General Data Protection Regulation, but we have seen that the content of this concept is not so new. The right to be forgotten means that in different circumstances the data subject is given the possibility to obtain the deletion of his/her personal data. Due to the large number of children and young people active online, in particular on social networking sites, the need for a reinforced concept of right to oblivion gains even more importance.

There are, however, multiple difficulties of different nature for correct implementation of the right to be forgotten in the field of online social networks. First of all, the personal and household exception must be taken into consideration and it must be clarified whether and in which conditions a post on a social network is to be considered as a personal activity and consequently be exempted from data protection rules. Secondly, the implementation of the right to be forgotten faces serious technical limits for the practical deletion of data. Moreover, the erasure of

[50] www.x-pire.de/index.php?id=6&L=2.

personal data endues a potentially significant economic cost and loss, observing the fact that the economic model of the Internet relies heavily on behavioural and contextual advertising. While such difficulties are not insuperable, they strictly impose a realistic approach to the question at hand.

The last difficulty is that the right to be forgotten inevitably conflicts with other rights, such as the right to freedom of expression, to information and the duty to remember. Solving such conflicts implies the utilisation of a balancing test among all rights and interests at stake as well as respect of the principle of proportionality. The fact that the data subject disclosed data concerning him/her when he/she was a child should influence the balancing test in favour of the cancellation of such data as requested by the repentant adult.

Expressly instating such a right in a legal instrument will certainly not be enough to ensure that oblivion is part of digital relationships in the same way that it characterises natural relationships. Enforcement of the right to be forgotten requires different approaches and is not a one-way solution. The Recommendation of the Committee of Ministers of the Council of Europe to Member States on the protection of human rights with regard to social networking services[51] encourages, *inter alia*, self- and co-regulatory mechanisms. "Member States should co-operate with the private sector and civil society with a view to upholding users' right to freedom of expression. … The social networking service should enable users to control their information". Concerning the right to be forgotten, this Recommendation states that users should be informed of how to completely delete their profiles and all data stored about them in a social networking service.

Besides self- and co-regulation, privacy by design could certainly also help give life to the right to be forgotten, by giving an expiry date to any piece of information disclosed in SNS. Automatic deletion of the data could be an easy solution to the *eternity effect*, but it cannot be the general and systematic answer as there are cases where the deletion of data enters into conflict with overriding rights and interests.

When facing the question of the desire or necessity to delete data published at an earlier date in SNS, one should not forget the most fundamental piece of the puzzle: education that instils long-term and safe behaviour on social networks.

References

Casarosa F (2010) Child privacy protection online: how to improve it through code and self-regulatory tools. http://ssrn.com/abstract=1561570

Copeland N (2012) Online privacy: the right to be forgotten. Library of the European parliament

Daly S (2011) Le doit a l'oubli—can we achieve 'oblivion' on the internet? http://emergingbusinessadvocate.wordpress.com/2011/03/15/le-doit-a-loubli-can-we-achieve-oblivion-on-the-internet/

[51] Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services.

De Terwangne C (2012) Internet privacy and the right to be forgotten/right to oblivion. Revista de internet, derecho y politica, pp 109–121. www.idp.uoc.edu

Dumortier F (2009) Facebook and risks of 'de-contextualization' of information. http://works.bepress.com/franck_dumortier/1

ENISA (2012) The right to be forgotten—between expectations and practice. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/

European Commission (2010) A comprehensive approach on personal data protection in the European Union. COM (2010) 609 final

Gomes de Andrade NN (2012) Oblivion: the right to be different…from oneself reproposing the right to be forgotten. Revista de internet, derecho y politica

Koops B-J (2011) Forgetting footprints, shunning shadows. A critical analysis of the 'right to be forgotten' in big data practice. www.ssrn.com

Legrand F, Bellamy A (2012) Touche pas à ma e-réputation! Enquête. www.lesnumeriques.com/divers/touche-pas-a-e-reputation-enquete-a1548.html

Livingstone S, Haddon L, Görzig A, Ólafsson K (2011) Risks and safety on the internet: the perspective of European children. Full findings. LSE, EU kids online, London

Mayer-Schönberger V (2009) Delete—the virtue of forgetting in the digital age. Princeton University Press, Princeton

Mayes T (2011) We have no right to be forgotten online. The Guardian. www.theguardian.com/commentisfree/libertycentral/2011/mar/18/forgotten-online-european-union-law-internet

Moiny JP (2010) Facebook au regard des règles européennes concernant la protection des données. Eur J Consumer Law, 2: 235–271

Moiny JP (2012), Cloud based social network sites: under whose control? In: Dudley A, Braman J, Vincenti G (eds). Investigating cyber law and cyber ethics: issues, impacts and practices. Hershey, Information Science Reference, pp 147–219

Reding V (2010) Why the EU needs new personal data protection rules? In: the European Data Protection and Privacy Conference, Brussels, 30 November 2010, http://europa.edu/rapid/pressReleasesAction.do?reference=Speech/10/700, accessed 18 February 2014

Rouvroy A (2008) Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?. http://works.bepress.com/antoinette_rouvroy/5/

Van Alsenoy B et a1 (2009) Social networks and web 2.0: are users also bound by data protection regulations? Springer, Heidelberg

Walz S (1997) Relationship between the freedom of the press and the right to informational privacy in the emerging information society. In: 19th International Data Protection Commissars Conference, Brussels