The right to be forgotten and informational autonomy in the digital environment

De Terwangne, Cécile

Published in:
The ethics of memory in a digital age

Publication date:
2014

Document Version
Publisher's PDF, also known as Version of record

5

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

Cécile de Terwangne

Introduction

The right to be forgotten, also called the right to oblivion, is today at the heart of intense debate in high-level spheres. European Union legislators have been discussing the relevance of such a right in the digital environment for many years; the Council of Europe authorities have expressed their concern on the subject; national politicians have raised their voices; data protection authorities, entities working in the field of human rights, academics and experts have all 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 from two different angles: regarding a criminal past and as part of data protection legislation. But the development of information and communication technologies (ICT) has made it necessary to re-think the scope of that right. Technological progress has had a considerable impact in this field. The Internet has brought with it a need for new balances between the free dissemination of information and individual self-determination. This balance is precisely what is at stake today with the right to be forgotten.

This chapter develops various possible outcomes deriving from this balancing test between the right to be forgotten and other rights and interests (see the section 'Effects'). There should be much more

nuanced results from exercising the right to be forgotten than the traditional binary 'keep or erase'. These nuanced outcomes should be available for the data subject, the data controller and the conflict resolution authority.

The definition and context of the 'Right to be Forgotten'

What is meant by the 'Right to be Forgotten'?

It is important to understand correctly 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 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, currently, another sense is given to this notion. The notion of the 'right to be forgotten' is used, at least in the framework of the European Union institutions, 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 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' (European Commission, 2010: 8). The right to oblivion in that sense is linked to the purpose of the processing of data, and to the ending of the 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 to replace Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data 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 informational self-determination (see section 'Informational autonomy'). Given that meaning, this right is no longer conditioned by the elapsing of time and does not necessarily concern information (re-)made publicly available. It is rather the right to require someone to forget (delete) what he/she knew because it is not legitimate to keep knowing it. We will see that, in several cases, the right to be forgotten will not imply to 'stop knowing' but rather to stop disseminating data and to de-index it (see section 'Effects').

Specific context of the Internet: the eternity effect

The infallibility of the 'total memory' of the Internet contrasts with the limits of human memory (Székely, 2012). A memory can be one of rancour, vengeance or belittlement. Thanks to its 'eternity effect' (Walz, 1997), the Internet preserves bad memories, past errors, writings, photos or videos which we would like to deny later (Ettighoffer, 2008).

The de-contextualisation

The 'new' digital right to be forgotten, claimed today and sketched in the proposed regulation from the European Commission, is clearly linked to certain Internet specificities. The 'eternity effect' of electronic memory can be combined with the efficiency of search engines to bring to the surface the slightest piece of information, separated from its initial context, and with all the pieces gathered to offer a recomposed though often heterogeneous portrait. Linked to the 'absolute memory' of the Internet, such a portrait may consist of past characteristics that are eternally present. The results can be harmful in different ways. And it is not only information disclosed by third parties that can raise concerns. Troubles can ensue from what we once personally posted on 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...), you do not necessarily want to be accessible to anyone else in a different context. But, thanks to search engines, it does become accessible outside the initial circle and context and you can suffer because of information that you have spontaneously disclosed yourself at an earlier stage.[2]

As a matter of fact, companies specialising in managing the 'e-reputation' of natural or legal persons on the web have appeared. They offer to do 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 our 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 grown exponentially while their costs have diminished. At the same time, 'nowadays forgetting is a costly affair' (Szeleky, 2010). Selection and assessment of data are indispensable processes before deleting it. But these operations are costly and labour-intensive (*ibid.*). Exercising the right to be forgotten therefore goes against the natural economic trend (EDPS, 2011).

In the same way, erasing personal data goes against the Internet's economic model. One of the targets of the right to oblivion is the traces that Internet surfers unconsciously leave behind while browsing the web. Associated with cookies, IP address retention, surf analyses, storage of search requests on search engines, and so on, all these data are highly valuable from an economic perspective. The long-lasting maintenance by most Internet actors of all these unconscious traces is precious to them given the economic model of service offered on the web: most of the informational products or services are apparently for free but are are actually financed by individually targeted advertising and behavioural advertising. This definitely limits the enthusiasm for erasing such information.

Informational autonomy or informational self-determination

The notion of informational autonomy/self-determination

Informational autonomy or self-determination means control over one's personal information, that is, the individual's right to

determine which information about themselves will be disclosed, to whom and for what purpose (de Terwangne, 2012; Rouvroy & Poullet, 2009; Hornung & Schnabel, 2009; Leonard & Poullet, 1992; Schwartz, 1989). 'Control' also signifies, not so much the ability to decide about the use of one's data, but at least the right to be aware of its fate, to be informed about who knows what about you and for what purpose.

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, that is, individual autonomy,[3] the capacity to make choices, to take informed 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 a crucial decision in 1983 (BundesVerfassungsGericht, 1983). 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 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' (Council of Europe Parliamentary Assembly, 1998).

In Europe, this informational self-determination has been recognised and protected as a right: the right to the protection of personal data. The European Court of Human Rights derived this new dimension of privacy from Article 8 ECHR.[4] The Council of Europe Convention 108 has established since 1981 the right to protection as regards the automated processing of personal data. The European Union Charter of Fundamental Rights 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, EU Directive 95/46 offers a very detailed legal regime for the protection of personal data, which is currently under revision.

Personal information or personal data is to be conceptualised very broadly since it should not be linked to the idea of intimacy as in the usual approach to privacy. It rather means *any* information related to a natural person. It thus covers professional data, commercial data and published data.

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's control over the data.

In the digital environment, and especially on the Internet, huge quantities of information relating to individuals are processed. Control over who you are disclosing your information to is pretty delicate (ENISA, 2012). As mentioned above, search engines like Google bring together information from various contexts. In doing so, they take data out of its initial circles and make it very difficult to control who you disclose information to. The other difficulty concerns the moment at which the disclosure occurs. What you have disclosed at one stage of your life you do not necessarily want to be permanently available. This raises the question of the recognition, or not, of the right to be forgotten.

The Right to be Forgotten linked to informational self-determination

As stated above, the right to be forgotten was initially linked to the elapsing of time. It is presented today as a part of the informational autonomy.

The European Commission has had concerns about the problems raised by the interrelation of Internet specificities. Perfect memory and the de-contextualisation of data have proved to be a source of problems for individuals. And users of social network services have complained that they are unable to obtain the complete erasure of their data as it is stored by the service provider. In its proposal for a general regulation on data protection, the Commission tackles these problems by guaranteeing 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 not the length of time that has 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 it remains in its initial context, the data is not

necessarily problematic. People do not necessarily desire the erasure of data 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 under 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 someone had previously disclosed about him/herself, the right to be forgotten could then be partially described as the 'right to change one's mind' and the 'right to repentance'.

All these aspects of a right not to be permanently reminded of one's past, a right to have someone delete what he/she knows because it is no longer legitimate, a right to refuse de-contextualisation of data, and a right to repentance and to change one's mind are derived from the newly sketched right to be forgotten (RtbF).

This right is to be comprehended considering two different situations:

- When the processing of data is based on the data subject's consent (see, 'The right to be forgotten in case of data processing based on the data subject's consent')
- When the processing relies on another issue (see, 'The right to be forgotten in case of data processing based on other grounds').

The Right to be Forgotten in case of data processing based on the data subject's consent

The Right to be Forgotten as a right to repentance and a right to change one's mind

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

But, as in ordinary life, people do come to regret what they have expressed or disclosed thanks to this web interactivity. Or they change their minds.

Such situations are particularly frequent when expression is spontaneous and unhesitating (as 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 but, on the contrary, remains continuously available to the public or to a certain part of the public long after it has been made.

Repentance or change also often arises as regards information or pictures shared while the issuer was young. Adults may want to erase traces of their online activities as teenagers that they now consider to be immature, irresponsible, incorrect or improper.

But it appears to be difficult to correct past stupidities. We have even discovered that it is impossible to entirely erase data once posted on Facebook (European Commission, 2010; Van Alsenoy, *et al.*, 2009).[5]

The right to withdraw consent leading to the erasure of data

In view of these difficulties, the European Commission clarified, in 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. Article 7, § 3, of the Regulation proposal already expressly provides for the right to withdraw consent at any time. Article 17 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 the deletion of data will occur after withdrawal of consent only if there is no other legal ground for the processing of the data.

This right to erasure in cases where information has been disclosed at the data subject's initiative seems quite logical and obvious, even to Peter Fleisher (Google's Global Privacy Counsel) who is a fervent opponent of 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' (Fleisher, 2011).

The Right to be Forgotten in case of data processing based on other grounds

When processing personal data based on other grounds than the data subject's consent, the interests of the data subject, as they are protected by the right to be forgotten, conflict with other interests, rights and freedoms: those of the person processing the data; or the persons interested in such a processing; or certain public interests. In particular, they conflict with freedom of expression and the freedom of the press. They undermine the conservation of full archives. For the same reason, they can be in conflict with the duty to safeguard memory. They are a hindrance to historical research. They also have an impact on business continuity, the management of employee files, the duty to keep evidence, and so on (de Terwangne & Moiny, 2011). 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 of balancing the competing values and interests. 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 an another one. The answer to a conflict always arises through a balancing test. Conflicting rights are put onto scales so as to reach a balanced result. The infringement incurred by the sacrificed value should not be disproportionate with regard to the benefit obtained from the conflicting value.

Conflict of interests and balancing test: criteria of newsworthiness, historical interest and public interest

The right to oblivion with respect to 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 noticeable facet of this right. The right to oblivion of the judicial past has been recognised by case law in several countries, based on the right to privacy or as a part of personality rights. As mentioned in the first section of this paper, it is justified by faith in humanity's capacity for change and improvement, as well as the conviction that man should not be reduced to his past. Once you have paid what is due, society must offer you the opportunity to rehabilitate and restart

without bearing the weight of your past errors for the rest of your life.

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

The right to be forgotten must cede 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. As soon as time has passed and it is no more a question of news or current events, that is, as soon as news necessity no longer justifies re-disclosure of the information, the right to oblivion overrides the right to information. Mention of the case may still occur 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 longer newsworthy, the scales tilt the other way.

The right to information will nevertheless override in spite of time elapsing for facts pertaining to history or concerning a matter of historical interest, or for facts linked to the exercise of a public activity by a public figure.

Technical developments have a great impact on the balancing test: they have radically changed the previously agreed balance. 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 the searcher's own identity, and for free, raises serious concern. We must carefully reconsider the right balance. Concerning data about the judicial past, a first answer is the anonymisation of case law databases available on the Web (de Terwangne, 2005). Such anonymisation is now the rule in the majority of European countries. But another important source of concern is the question of newspaper archives.

Internet newspaper archives

Internet newspaper archives contain all kinds of information that were once news. Many of them concern individuals. They are not limited to judicial data.

The fate of personal data, as soon as it is mentioned in a newspaper and then eternally available in its archive website, 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 newspaper archives, consideration must be given to the above-mentioned criteria of:

- newsworthiness;
- historical interest;
- public interest.[6]

By definition, newspaper archives are not supposed to contain any newsworthy materials any longer. When considering the historical value of the facts, one should take into account whether other sources of information exist.

In the *Times Newspaper* case, the European Court of Human Rights cast some very interesting light on the way the balancing test should be implemented. Even if the right to be forgotten was not at stake in this case, 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 the 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 than if the main function, that of watchdog, were at stake. The Court said it agrees that Internet archives 'constitute an important source for education and historical research, particularly as they are readily accessible to the public and are generally free... 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'.[7]

Contrary to Article 17 of the European Regulation proposal, which only provides for the erasure of data and abstention from further dissemination of it, or blocking of it, one can envisage different outcomes from a balancing test concerning the right to be forgotten (see the section, Effects). Here, the outcome could, for example, be the obligation to erase identifying data from an article in publicly available Internet newspaper archives. A non-expurgated version would be maintained with restricted access (for research purposes). Or the outcome could be the requirement that additional information be linked to the data (the data subject's opinion, for example,

or, in the case of judicial data, a notice specifying that the decision is under revision if an appeal has been made against it). Conclusions 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 of controversial information through the web. The balance reached on the web does not necessarily correspond to what would be done in classical formats. Certain solutions are likely to give 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 web. The harm deriving from the eternal and universal availability of data via the Internet is more likely to be considered disproportionate than the harm resulting from local publicity subject to procedures.

The elements of the Right to be Forgotten in data protection legislation

The right to object to the processing of data

Commentators have noted that the recently hyped digital right to be forgotten is perhaps simply the 'lyric' translation of the already existing right to object (Cyberlex, 2010: 10).

The right to object is indeed already guaranteed today by Article 14, § 1, b, 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 conditional on any justification.

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.

Obligation to delete personal data deriving from the purpose principle

The right to object is left to the data subject's initiative. On the contrary, to benefit from the right to be forgotten deriving from the

purpose principle requires no effort from the data subject. It is up to the data controller to see to it that personal data is erased when the purpose of processing is achieved.

One of the basic principles of the data protection regime is the purpose principle. This 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 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 (Article 6(1)(e) of Directive 95/46). This means that personal data may be kept if it is justifiable to achieve the purpose of processing. It should be either anonymised or deleted once that purpose has been achieved, or as soon as keeping the link with the identifiable person is no longer necessary to achieve that purpose.

The right to erasure

The right to erasure is part of Article 12(b) of Directive 95/46, which 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 of data is a way for the data subject to act against non-compliance with the protection rules.

The ability to withdraw consent and to object is given to the data subjects with regard to the lawful processing of their data. Unlike those rights to change one's mind and to object, the right to erasure is a tool for achieving compliance. It can be considered an element of the right to be forgotten.

Effects

Erasure or...

The right to be forgotten in principle entitles the data subject to demand that his/her personal data be deleted. In fact, other cases may occur where the data subject does not intend for his/her data to be erased. Different actions could also be envisaged in addition to data erasure. They would better respect the proportionality principle.

- Not to be associated with the data could suffice. *Anonymisation* of the data would then be an adequate answer to such a wish.
- The problem could ensue from the public disclosure of personal data, not from an internal processing of it. The data could then remain stored and be used by the controller; the right to be forgotten would mean *abstention from further dissemination* of the data. *Restricted access to the data* could lead to the same result. External access would be blocked.
- The data subject could *opt for another form of publicity* that respects the proportionality principle in place of a form where harm would be too serious in comparison with the benefits of competing values. For example, a person may consent to be filmed, and accepts that the film will be shown on TV on an agreed day and time, but refuses to allow the film to be permanently available on the web thereafter.
- The data subject wants to act against de-contextualisation and would be happy just with his/her *data being de-referenced or de-indexed,* with links to it being suppressed. *The suppression of any link* to the data would be the right tool against the de-contextualisation of data without depriving members of the initial circle of access to this data provided that they remain inside the circle.
- *Additional information* could also be linked to the data: a warning or the data subject's opinion, for example.

These nuanced results of exercising the right to be forgotten should be available to the data subject, the controller and the authority potentially invited to find a balanced result in case of disagreement between parties.

Information to third parties

To strengthen the right to be forgotten in the online environment, Article 17, § 2 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' (Recital 54 of the Regulation proposal).

This has been presented by some commentators as the real innovation of the Regulation proposal regarding the right to be forgotten. But one must note that this provision is not so different from Article 12 (c) of Directive 95/46, which guarantees 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, notably the fact that 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.

Right of automatic deletion of data in the electronic environment

In response to the new developments in Internet services, and to the problematic situation deriving from the specificities of the Internet pointed out earlier in this chapter, the same proposition has been made in different political, institutional and experts circles (V. Reding, 2010; Council of Europe Deputy Secretary General, 2010; European Data Protection Supervisor, 2011, § 85), that is, to grant data subjects an automatic right to be forgotten after the expiry of a certain period of time even if the data subject does not take action or is not even aware that personal data was ever stored.

These similar propositions amount to ascribing some kind of expiry date to the data without any prior analysis on a case-by-case basis. A certain period of time could be fixed, for example, for data stored on terminal equipment such as mobile devices or computers: data would be automatically deleted or blocked after the fixed period of time if the equipment were no longer in the possession of its initial owner.

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 from the right to have one's data erased on request, the right to be forgotten could become a 'data protection by default' rule.

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

Such possibilities to implement an automatic system of data destruction with the data subject's consent already exists. As an illustration of such a system, the software X-Pire (http://www.x-pire.de/index.php?id=6&L=2) 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 means of achieving the right to be forgotten cannot offer an adequate answer in all the circumstances in which the data subject would like to benefit from the right to be forgotten. First, because cases like a withdrawal of consent to the processing of data cannot be foreseen and turned into a systematic expiry date. Second, because the data subject does not necessarily want to see his/her data erased. He may prefer to ask for there to be no further dissemination of it, for example (see *supra*).

Conclusion

The right to be forgotten today presents different facets. It covers:

- the right to repentance and to change one's mind regarding the data previously disclosed or for which consent for processing had been given;
- the right not to be permanently reminded of one's past, not to see the past clutter the present and jeopardise the future;
- the right to have data deleted because it is no longer legitimate to keep it, the purpose principle not justifying it anymore;
- the right to refuse de-contextualisation of data mainly by fighting against the power of Internet search engines while possibly accepting that the data remain in its initial context.

These different facets of the right to be forgotten are legally protected, based on the right to privacy and singularly on the informational autonomy linked to this right.

The right to the protection of personal data embodies that informational autonomy. It contains the ingredients that can realise the different facets of the right to be forgotten:

- the right to withdraw previously given consent to process data;
- the right to object to the data processing;
- the duty to delete or anonymise data once the purpose of processing has been achieved and no longer justifies the retention of personalised data;
- the right to erase data when its processing is non-compliant with the protection requirements.

These elements are already present in the data protection legislation but would nevertheless need more clarification as to their effects. A provision devoted to the right to be forgotten, such as Article 17 of the Regulation Proposal, would be a good opportunity to envisage the necessary wide range of effects that should be provided. Indeed, the results of exercising the right to be forgotten should be much more nuanced than simply having the contested data deleted or imposing restricted processing/use. We have seen above that to reach a fair balance between the competing values and respecting the proportionality principle, this right to be forgotten could become a right to erase data, but also a right to anonymisation (to erase only the identifying data[8]), or a right to erase the electronic links to personal data (in order to efficiently fight against the 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 approach to achieving the right to be forgotten could mean either the controller's refraining from further dissemination, or the data subject's choice of certain forms of publicity instead of others.

The duty to inform third parties of the exercising of facets of the right to be forgotten is logical and desirable, even if it raises serious questions of practicality when data is disseminated on the Internet. This duty is already partially present in the Directive 95/46. It is certainly an opportune tool in the online context characterised by its radical opacity. Where it is reasonably feasible, the controller would have to warn further users of the contested data. He is better able to know these persons or to get in contact with them than the data subject, especially if he has a contractual link with them.

Finally, the development of a 'right to be forgotten by default' through technical automatic deletion or data blocking would contribute to a shift in the balance in favour of the data subject, since the latter would benefit from the protection without having to take the initiative. Even if this does not offer an appropriate answer in all situations, it could be particularly important in a context as opaque as the Internet. Much data processing that occurs in that sphere is 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.

Notes

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, 2012).
2. On the risk of de-contextualisation in SNS, see F. Dumortier, 2009. 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 (Moiny, 2012).
3. For the explicit recognition of a right to self-determination or to personal autonomy as enshrined in the right to respect private life in Article 8 ECHR, see ECtHR, *Evans v. United-Kingdom*, 7 March 2006, req. No 6339/05 (confirmed by the judgement of the Grand Chamber on 10 April 2007); *Tysiac v. Poland*, 20 March 2007, req. No 5410/03; *Daroczy v. Hongary*, 1 July 2008, req. No 44378/05.
4. See among others, E.Ct.H.R., *Rotaru v. Romania*, 4 May 2000, appl. no 28341/95, § 43; *Amann v. Switzerland*, 16 February 2000.
5. 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.
6. On these criteria, see European Court Human Rights, *Osterreichischer Rundfunk*, 7 March 2007.
7. E.Ct. H.R., *Times Newspapers Limited (Nos. 1 and 2) v. the United Kingdom*, 10 March 2009, Appl. Nos. 3002/03 and 23676/03, § 45.

8. 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 this paper.

References

BundesVerfassungsGericht. (1983). *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1 ff. 15 December.

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

Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data, ETS No 108, 28 January 1981.

Council of Europe Parliamentary Assembly. (1998). Resolution 1165 (1998) on the right to privacy. 26 June.

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

Cyberlex, L'Association du Droit et des Nouvelles Technologies (2010). *L'oubli numérique est-il de droit face à une mémoire numérique illimitée?* 25 May ; retrieved from http://www.cyberlex.org/images/stories/pdf/contribution_cyberlex_dao.pdf, 1–145.

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, 40–.48

de Terwangne, C. (2012). Internet Privacy and the Right to Be Forgotten/ Right to Oblivion. *Revista de Internet, Derecho y Politica*, 2012, n°13, p. 109-121, also available at HYPERLINK "http://www.idp.uoc.edu" www.idp.uoc.edu.

de Terwangne, C. & Moiny, J-Ph. (2011). Report on the Consultation on the Modernisation of Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Strasbourg, Council of Europe. Retrieved from http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD BUR_2011_10_en.pdf.

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, 31–50.

ENISA (2012). The Right to be Forgotten – Between Expectations and Practice. 20 November. Retrieved from https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/, p. 10.

Ettighoffer, D. (n.d.). Les droits de l'homme numérique : le droit à l'oubli. Retrieved from http://www.eurotechnopolis.org/fr/oubli.html.

European Commission (2010). Communication: 'A Comprehensive Approach on Personal Data Protection in the European Union'. 4 November, COM(2010) 609 final.

European Commission (2012). 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).

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.

European Data Protection Supervisor. (2012). Opinion on the data protection reform package. 7 March.

Fleisher, P. (2011). Foggy Thinking about the Right to Oblivion. 9 March. Retrieved from Peter Fleisher's Blog: http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html.

Hornung, G. & Schnabel, C. (2009). Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-determination. *Computer Law & Security Review*, 84–88.

Leonard, Th. & Poullet, Y. (1992). Les libertés comme fondement de la protection des données nominatives. In F. Rigaux (ed.), *La vie privée : une liberté parmi les autres ?* Travaux de la faculté de Droit de Namur, n° 17, Bruxelles, Larcier, 231–260.

Moiny, J.-P. (2012). Cloud based Social Network Sites: Under whose Control ? *Investigating Cyber Law and Cyber Ethics*, 147–219.

Reding, V. (2012). The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age. *Retrieved from* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF.

Reding, V. (2010). Why the EU Needs New Personal Data Protection Rules? The European Data Protection and Privacy Conference, Brussels, 30 November. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700.

Rouvroy, A. & Poullet, Y. (2009). 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 and Y. Poullet (eds), *Reinventing Data Protection*. Dordrecht: Springer. Available at: http://works.bepress.com/antoinette_rouvroy/7.

Schwartz, P. (1989). The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-determination. *The American Journal of Comparative Law*, 37(4), 675–701, available at: http://scholarship.law.berkeley.edu/facpubs/866.

Székely, I. (2012). 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, 347–363.

Van Alsenoy, B., Ballet, J., Kuczerawy, A., & Dumortier, J. (2009). Social Networks and Web 2.0: Are Users Also Bound by Data Protection Regulations? *Identity in the Information Society Journal*, 2, 65–79.

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.