Internet privacy and the right to be forgotten/right to oblivion

De Terwangne , Cécile

Published in:
Revista de Internet, derecho y politica

Publication date:
2012

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

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monograph «VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet»

ARTICLE

Internet Privacy and the Right to Be Forgotten/Right to Oblivion

Cécile de Terwangne

Submitted: December 2011
Accepted: December 2011
Published: February 2012

Abstract
The right to oblivion, equally called right to be forgotten, is the right for natural persons to have information about them deleted after a certain period of time. The Internet has brought with it a need for a new balance between the free dissemination of information and individual self-determination. This balance is precisely what is at stake with the right to oblivion. This right has three facets: the right to oblivion of the judicial past, the right to oblivion established by data protection legislation and a new, and still controversial, digital right to oblivion that amounts to personal data having an expiration date or being applicable in the specific context of social networks. This paper analyses each of these facets within the Internet environment.

Keywords
right to be forgotten, right to oblivion, privacy, data protection, right to object

Topic
IT law, data protection law

Privacidad en Internet y el derecho a ser olvidado/derecho al olvido

Resumen
El derecho al olvido, también llamado derecho a ser olvidado, es el derecho de las personas físicas a hacer que se borre la información sobre ellas después de un período de tiempo determinado. Internet ha traído consigo la necesidad de un nuevo equilibrio entre la libre difusión de la información y la autodeterminación individual. Este equilibrio es precisamente lo que está en juego con el derecho al olvido. Este derecho presenta tres facetas: el derecho al olvido del pasado judicial, el derecho al olvido establecido por la legislación de protección de datos y un nuevo derecho digital y aún polémico al olvido, que equivaldría a la atribución de una fecha de caducidad a los datos personales o que debería ser aplicable en el contexto específico de las redes sociales. Este trabajo analiza cada una de estas facetas en el entorno de Internet.

Palabras clave
derecho a ser olvidado, derecho al olvido, privacidad, protección de datos, derecho a objetar

Tema
Ley sobre tecnologías informáticas, Ley de protección de datos

Introduction

The right to oblivion, equally called the right to be forgotten, is the right for natural persons to have information about them deleted after a certain period of time.

The development of information and communication technologies has been a determining factor as regards extending the scope of that right. Technological progress has had a considerable impact in this field. The Internet – which can be taken as the most representative paradigm of the radical technical and sociological change we are facing – has brought with it a need for a new balance between the free dissemination of information and individual self-determination. This balance is precisely what is at stake with the right to oblivion.

The infallibility of the 'total memory' of the Internet contrasts with the limits of human memory. Now memory can be one of rancour, vengeance or belittlement, thanks to the "eternity effect"[1] of the Internet, which preserves bad memories, past errors, writings, photos and videos we would like to deny at a later stage. "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."[2] The European Commissioner for Justice, Viviane Reding, recently 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."[3]

This paper presents and analyses this right to oblivion, examining each of its three facets, each one linked to a specific context. But before continuing, it is advisable to clarify the meaning of 'Internet privacy' which underlies the question of the right to be forgotten. Effectively, this notion is not always well decrypted, and an inadequate perception of it might bring a biased approach to the question.

1. Internet Privacy

When considering 'Internet privacy', 'privacy' is not to be read as 'intimacy' or 'secrecy'. It rather refers to another dimension of privacy, i.e. individual autonomy, the capacity to make choices, to take informed decisions, in other words to keep control over different aspects of one's life.

In the context of the Internet this dimension of privacy means informational autonomy or informational self-determination. The Internet handles huge quantities of information relating to individuals. Such personal data are frequently processed: it is disclosed, disseminated, shared, selected, downloaded, registered and used in all kinds of ways. In this sense, the individual autonomy is in direct relation to personal information. Information self-determination means the control over one's personal information, the individual's right to decide which information about themselves will be disclosed, to whom and for what purpose.

On the Internet, at least two difficulties arise. Control over who you are disclosing your information to is problematic. What you have agreed to disclose to certain

1. Walz (1997), p. 3.
2. Ettighoffer (2008), p. 2 (our translation).
3. Reding (2010)

recipients because they belong to a determined circle (friends, family, colleagues, persons taking part in a forum, members of an interest group, etc.), you do not necessarily want to be accessible to anyone else. Search engines like Google today bring together information from various contexts, and in doing so, they take data out of the initial circles and make it extremely difficult to control who you disclose information to. The other difficulty concerns the moment when disclosure occurs: what you have disclosed at one stage in your life you do not necessarily want to be permanently available. This raises the very question of whether a right to be forgotten should be recognised.

Before focusing on this last point, there is still one term to clarify. The concept of personal information or personal data is to be considered in its widest sense, since it should not be linked to the idea of intimacy as in a classical view of privacy, but to *any* information related to a natural person, so covering professional, commercial and published data.

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.[4] The Council of Europe Convention 108[5] has, since 1981, established the right to protection as regards the automated processing of personal data. The European Union Charter of Fundamental Rights[6] is the first general international catalogue of fundamental freedoms and rights that mentions the right to data protection as an autonomous right, and, as such, protected. 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[7] 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.

2. The Right to Oblivion of the Judicial Past

2.1. The Criterion of Newsworthiness or of Historical Interest

The first facet of the right to oblivion, the most classical, is linked to an individual's judicial or criminal past. It was at first mostly related to the creation of criminal records. Today, the right to oblivion of the judicial past has gone widely beyond criminal records. It has been recognized by case law in several countries, based on the right to privacy or as part of personality rights. It is justified by faith in a human being's capacity to change and improve as well as on the conviction that a person should not be reduced to their past. Once you have paid what is due, society must offer you the possibility to rehabilitate and restart without bearing the weight of your past errors for the rest of your life.

This right is in conflict with the right to information, time being the criterion to resolve the conflict. The right to oblivion must give priority to the requirements of the right to information when the facts revealed present a topical interest for disclosure, so interest is linked to the newsworthiness of the facts. This occurs when a decision pronounced by a court or a tribunal is part of judicial news. It is then legitimate to refer to this decision, mentioning parties' names (except if they are minors, in which case different rules of protection apply). But with time, when it is no more a question of news or current events, and as long as there is no longer a justification for re-disclosure of the information as news, the right to oblivion overrides the right to information. There may still be mention of the case, but this should not include parties' names or specific details. So the newsworthiness of a case tips the balance in favour of the right to disseminate instead of the right to oblivion, but as soon as it is no longer newsworthy, the scales tip the other way.

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. Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data (ETS No. 108, 28.1.1981).
6. Charter of Fundamental Rights of the European Union, *Official Journal*, 18 December 2000, C-364/1.
7. 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.

Two exceptions can be admitted, meaning that the right to information will override in spite of time having elapsed:

- 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 general interest are also to be taken into consideration to solve the conflict between the right to oblivion and the right to information.

2.2. Impact of Technical Developments

2.2.1. Gathering Information: the Power of Search Engines

Technical developments have radically changed the balance between the necessity to disclose judicial information and the individual right to be forgotten. As mentioned earlier, the slightest piece of information can be brought to the surface and gathered along with other pieces. This implies a radical change. It is worth citing a change underlined by a US Supreme Court decision,[8] pronounced more than twenty years ago but nevertheless very enlightening today. The case concerned a journalist who asked for access to FBI documents relating to the criminal records of four people. Three had died and, for the fourth the FBI refused to disclose information 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 the 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 clearing house of information."[9] A Californian Appeal Court also stated that it was "the aggregate nature of the information which makes it valuable to respondent; it is the same quality which makes its dissemination constitutionally dangerous."[10]

The power of Internet search engines to access all data concerning a targeted individual at any time, from anywhere, without any administrative procedure, without revealing the identity of the person who requested the search, and for free, raises an even greater danger. We must carefully reconsider the balance needed. On the precise point of data about judicial past, a first answer is the anonymisation of case law databases available on the Net,[11] which is now the rule in the majority of European countries. But another important source of concern, which will be dealt with next, is the question of newspaper archives.

2.2.2. The Eternal Availability of Information: The Case of Internet Newspaper Archives

Internet newspaper archives are a source of all kinds of information that was once news: much concerning individuals, and not limited to judicial data of course. Even if focusing on this latter, what follows is also valid for other personal information.[12]

Judicial data mentioned in a newspaper are then eternally available on the archives website of the newspaper. This raises the problem of a possible conflict between the judged person's right to be forgotten (on the basis of the right to privacy, the rights of personality or the right to free development of one's personality) and the freedom of the press.

There is no a priori hierarchy among human rights: conflicts of rights cannot be solved by giving systematic priority to one right over another. Resolving a conflict always passes a balancing test. Conflicting rights are

8. *Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989).
9. 489 U.S., 764.
10. *Westbrook v. Los Angeles County*, 32 Cal. Rptr. 2d 382 (Cal. App. 1994)
11. On this question that cannot be developed more deeply in the present paper see De Terwangne (2005), pp. 40-48.
12. Another paper in the present issue of this Journal deals with the question of the right to oblivion and the press and goes further into the problems linked to newspaper archives.

weighed to reach a balanced result. The infringement incurred by the sacrificed value should not be disproportionate with regard to the benefit obtained by the conflicting value.

As regards the conflict raised by Internet newspaper archives, consideration must be given to the above-mentioned criteria of newsworthiness, historical interest and public interest. By definition, information in newspaper archives is assumed to be no longer newsworthy. When considering the historical value of the facts, one should specifically take into account whether other sources of information exist. As regards judicial data, special attention must also be paid to whether an appeal has been lodged against judicial decisions stored in newspaper archives. If this is the case, the first judgement could be kept in the archives but should be accompanied by a notice specifying that the decision is under revision.

In the recent *Times Newspapers* case, the European Court of Human Rights shed some very interesting light on how the balancing test should be implemented. Even though the right to oblivion was not at stake in this case,[13] the statement of the Court could be usefully applied to hypotheses implying a conflict between the freedom of the press and the right to oblivion in presence of publicly available newspapers archives. The Court stated 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 has less weight when striking the balance than if its main function, that of the famous watchdog, were at stake. The Court stated that 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.* [...]"[14]

One can consequently envisage the outcome of a balancing test being that identifying data should be erased from an article in Internet newspaper archives. However, this conclusion should always be reached on a case-by-case basis. And we should keep 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 should be done in the case of non-digital formats. Certain solutions concerning Internet archives will very likely consist in giving priority to the right to oblivion, 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 on the Internet will much more often be considered disproportionate than the harm ensuing from local publicity subject to procedures.

3. The Right to Oblivion Established by Data Protection Legislation

As previously noted, technological developments have lead to the multiplication of use of data and of places where data are stored and processed. Electronic tools have become more and more powerful, with growing storage capacities and extraordinary efficiency in selecting and retrieving information. Data protection laws have appeared, not to inhibit technical progress but to offer a framework for the new developments to re-balance the situation.

The second facet of the right to oblivion derives from this data protection regulation. Through different principles, this legislation guarantees what can be considered as a right to be forgotten. But in this context, the right is extended. It is no more exclusively linked to judicial past but applies to processing of any personal data.

13. 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.
14. 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).

Before detailing the principles shaping this right, it is worth stating that there exist no global, legally-binding instruments relating to data protection.[15] National and regional laws address the subject.[16] Among these, the EU directive 95/46[17] is of undoubted interest since it is the most detailed protection regime in place, and, for that reason, references are made to this legal instrument in the following paragraphs. But while it is of interest as a legal shaping of a right to be forgotten, one has to bear in mind that this European regime is not a global answer to the concerns raised in the Internet universe.

3.1. Obligation to Delete or to Anonymise Personal Data Derived from the Purpose Principle

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 this principle since, according to one of its applications, 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 data were collected or for which they are further processed".[18] This means that personal data may be kept as such if it is justified to achieve the purpose of processing. It should be either anonymised or deleted once the purpose has been achieved or as soon as it is no longer necessary to keep the link with identifiable persons to achieve that purpose.

This rule clearly establishes a right to oblivion. To say the least, data protection legislation establishes the obligation for anyone who processes personal data to foresee and to respect an expiry date for these data. Data subjects are entitled to check this rule is respected.[19] They are granted the right to have the controller erase or block the data when processing does not comply with the limitation ensuing from the purpose principle. Moreover, sanctions can be imposed in case of infringement of the rule.[20]

3.2. Attenuation of the Right to be Forgotten

The authors of the Data Protection Directive were conscious that, in many cases, people who do historical, scientific or statistical research have to use data not initially collected for that purpose. Since they were convinced that this research is important for society, they opted for a system where historical, scientific or statistical use of data is systematically admitted, on condition that states lay down appropriate safeguards for such uses.[21]

This means that personal data may be kept after the expiry date if it is justified by these specific purposes. National safeguards vary from one state to the other. Certain states have foreseen the obligation to anonymise or at least to code the data. There must be some justification to keep data in their original form. Other national safeguards are however more minimalist.

Another specificity of data protection legislation marks a fall as regards the right to oblivion. Article 9 of the Directive 95/46 puts into place an exemption regime for data processing

15. The 'Madrid Resolution' adopted by a collective of national data protection authorities is but a proposition at this stage and is not legally-binding. See Agencia Española de Protección de Datos (2009).
16. Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data (ETS No. 108, 28.1.1981); OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, published on www.oecd.org; APEC Privacy Framework, November 2004, http://www.apec.org/content/apec/apec_groups/som_special_task_groups/electronic_commerce.html
17. 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, *O.J.*, nº L 281 23 November 1995, p. 31.
18. Art. 6, § 1, e) of the Directive 95/46.
19. Art. 12 of the Directive 95/46.
20. Art. 24 of the Directive 95/46.
21. The same is accepted for statistical and scientific purposes, see art. 6, § 1, b), *in fine*, of the Directive 95/46 : "Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards."

for journalistic purposes[22] or for the purpose of artistic or literary expression. Member states are invited to themselves define the appropriate exemptions they consider necessary to "reconcile the right to privacy with the rules governing freedom of expression".[23] According to which derogations have been granted by a state, persons processing personal data for these specific purposes in that state can be freed from the obligation to delete data once the purpose is achieved.

3.3. Right to Object to the Processing of Personal Data

To benefit from the right to be forgotten deriving from the purpose principle, the data subject does not have to do anything: it is the data controller who has to see to it that personal data are erased when the purpose of processing is achieved. Another way of achieving the right to be forgotten is established by the Directive, then left to the data subject's initiative.

According to article 14 of the Directive 95/46, data subjects are granted 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." 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.[24]

Faced with the media fuss created around the recent claim to guarantee everyone a digital right to be forgotten, it was said that the clamour was perhaps simply about the 'lyric' translation of the already existing right to oppose.[25] It is worth noting that this right to object is not totally equivalent to a right to delete one's personal data. It amounts to a right to demand that processing of the data ceases. In many cases this will imply erasing the data since the processing includes data storage. 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').

Non-respect of objection justified by legitimate grounds is punishable.

4. New Digital Right to Oblivion Claimed

Recently, the right to be forgotten has been at the heart of intense debates, related in the press, in official reports, political statements, and in blogs, etc. The concern expressed is about the appropriateness of extending the existing right to be forgotten in response to the situations born from the development of the Internet environment. According to the French CNIL president, what is at stake with the rethinking of the right to oblivion is to bring back a natural function, forgetting, that renders life bearable.[26]

4.1. Context of the Claim: Internet Specificities

The 'new' digital right to oblivion is clearly linked to certain Internet specificities. Some of these have already been mentioned: the 'eternity effect' of the electronic memory as well as the efficiency of search engines to bring to the surface the slightest piece of information, out of its initial context, and to gather all the pieces together to offer a recomposed, often heterogeneous, portrait. Linked to the 'absolute memory' of the Internet, this portrait may consist of past characteristics eternally present and sometimes harmful in one way or another. As a matter of fact, certain companies specialised in the managing of the 'e-reputation' of individuals and legal entities on the Web have been set up. They offer to do one-shot or long-

22. To understand what a journalistic purpose means today, see the important decision of the European Court of Justice in the case *Satamedia*: E.C.J., 16 December 2008, *Satakunnan Markkinapörssi Oy et Satamedia Oy*, Case C-73/07. See also C. de Terwangne (2010). "Les dérogations à la protection des données en faveur des activités de journalisme enfin élucidées", note under E.C.J., 16 December 2008, *Satakunnan Markkinapörssi Oy et Satamedia Oy*, Case C-73/07, *R.D.T.I.*, nº 38, pp. 132-146
23. Art. 9, *in fine*, of the Directive 95/46.
24. Art. 14, § 1, b) of the Directive 95/46.
25. Cyberlex (2010), p. 10.
26. Turk (2009).

term cleaning operations to protect, maintain or restore one's reputation and image.

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

Moreover, it has become less expensive to store data than to destroy or anonymise them. Storage capacities have grown exponentially while their costs have diminished. "The exercise of the rights of the individual therefore goes against the natural economic trend."[27]

4.2. Right of Automatic Deletion of 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, the same proposition has been made in political, institutional and 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, that the existing right to be forgotten should be extended to ensure that 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 them were ever stored.[28] 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."[29] The Vice-President of the European Commission, V. Reding, said in 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*."[30]

These similar propositions are to attribute some kind of expiration date to 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 equipment such as mobile devices or computers: data would be automatically deleted or blocked after the fixed period of time if the equipment is no longer in the possession of the initial owner.

This system already applies in some states for certain files and registers, such as criminal files and police registers. This involves what the European Court of Human Rights 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.[31]

The automaticity of the deletion or of the prohibition of further use would need to be translated into a 'privacy by default' setting for the processing of personal data, so the right to oblivion could in turn become a 'privacy by design' obligation. Such a technical answer would contribute to shift the balance in favour of the data subject, since they would benefit from the protection without having to take any initiative. This is particularly important in a context as opaque as the Internet where much of the data processing occurs totally outside the data subjects' awareness. It is illusory, therefore, to guarantee individuals a right they would never consciously think of using.

27. European Data Protection Supervisor (2011).
28. European Data Protection Supervisor (2011), § 85.
29. Council of Europe, Deputy Secretary General (2010) (our italics).
30. Reding (2010) (our italics).
31. 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.

'Oblivion' could mean an obligation to delete data, but could equally refer to a prohibition to further use the data, at least in the personalised format. This would perhaps be more realistic taking into consideration the economic cost of deletion mentioned earlier. If the specific problems of Internet media and social networks are focussed on, 'oblivion' could also amount to the prohibition to further disseminate the data.

4.3. Right to Have Information Deleted and Not Only Rendered Inaccessible

A specific problem has appeared in the environment of social networks. Several have shown reluctance to delete data once the person who uploaded them on a page of the social network wanted to stop using the network. The service generally accedes to the expressed wish to no longer publish the data but refuses to destroy them. In answer to this difficulty, certain voices have explored the possibility of establishing a right to have one's information deleted and not only rendered inaccessible.

This would especially apply to cases where information has been disclosed on the concerned person's own initiative. This seems quite logical and evident to Peter Fleisher, who, in spite of this, 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."[32]

4.4. Difficult Practical Implementation

One must be conscious of the technical limits of the implementation of the right to be forgotten: having one's data deleted from the Web is not as simple as that.[33] You have first to ask the editor of the concerned website to erase the problematic data. Once he has complied with your demand, the information will still be available for a while in the results presented by the search engines in the cache memory.[34] It can take some days or weeks till the next indexation of the site will bring an updated version to the cache memory. During the time that the data are publicly available, interested people may download and share the information without you being aware of it. If you discover that, for example, other Internet users have downloaded and re-published the information on their website, you will have to do the cleaning job again. And at some point in this Sisyphean activity, you will probably face great difficulty in convincing the website editor or the inertia of your interlocutor. Moreover, the architecture of information systems has become much more complex, with the numerous links rendering any deletion of data tricky and expensive.[35]

A recent Spanish case, where the data protection authority set up a strategy to circumvent the difficulty, illustrates the problems linked to deletion operations. In January 2011, the Agencia Española de Protección de Datos ordered Google to remove certain links to web pages hosting personal data relating to Spanish citizens from its results. A number of these links connected to newspaper articles containing information which could damage the reputation of those concerned. In particular, a plastic surgeon who was involved in a case of medical malpractice, in 1991, wanted Google to remove the related articles from search results connected with his name. The Spanish authority argued that bringing an injunction against search engines such as Google is the only way to block access to sensitive material online, as newspapers can legally refuse to comply with more informal requests.[36] However, Google refused to obey the order since it amounted, in their view, to censorship of their results. The case was taken to a Madrid Court which deferred it to the European Court of Justice. The Court has been invited to

32. Fleisher (2011).
33. See also Cyberlex (2010), *op. cit.*, p. 41; Fleisher (2011), *op. cit.*; Privacy International (2011).
34. Google presents its cached links as the following: "Google takes a snapshot of each page examined as it crawls the web and caches these as a back-up in case the original page is unavailable. If you click on the 'Cached' link, you will see the web page as it looked when we indexed it. The cached content is the content Google uses to judge whether this page is a relevant match for your query. When the cached page is displayed, it will have a header at the top which serves as a reminder that this is not necessarily the most recent version of the page." Available at http://www.google.com/intl/en/help/features_list.html#cached
35. Cyberlex (2010), p. 33.
36. Halliday (2011); "Spain demands the right to oblivion for its citizens", *Law and the Internet,* The Finocchiaro Law Firm's blog. 31 March 2011; R. G. Gómez (2011).

clarify whether a national data protection authority is entitled to demand removal of links from the results presented by a search engine.

As a final point concerning the specific difficulties for implementing the right to oblivion on the Internet, the data which would be the subject of such a right of erasure should be clarified. Does it concern only data obtained from the data subjects or does it also cover analytical data or metadata created by the data controller?[37]

4.5. A Difficulty Ensuing from the Internet Economic Model

One of the targets of the right to oblivion is the traces Internet users unconsciously leave behind while browsing the Web. Associated with cookies, IP address retention, surf analyses, storage of search requests on search engines, etc., all these data are highly valuable from an economic perspective. The length of time most Internet actors keep all these unconscious traces is important to them, given the economic model of service offered on the Net: most products or services are apparently free, but they are financed by individually targeted and behavioural advertising. This definitely limits the possibility of erasing this information.

4.6. Conflicting Interests

As already commented concerning the right to forget the judicial past, the right to oblivion enters into conflict with important other rights, freedoms and legitimate interests, in particular, with freedom of expression and freedom of the press. It impinges on the conservation of full archives, as developed in point 2.2.2 relating to Internet newspaper archives. For the same reason, it hurts the duty of memory. It is a hindrance to historical research. It also has an impact on business continuity, management of employee files, the obligation to keep evidence, etc.[38] And one inevitably has to take into account the obligation to retain data for public security purposes.

The Asociación Profesional Española de Privacidad puts it a slightly different way, presenting it as a dilemma. In the opinion of this association, unlike the right to object, the right to be forgotten has a retroactive effect. Consequently, the question is whether individuals must be responsible *sine die* for their past actions or whether it is desirable for them to have the right to rewrite their past, and consequently that of others.[39]

The answer to such conflicts or dilemmas lies again in applying balancing tests respecting the proportionality principle (see above, point 2.2.2).

Conclusion

The right to be forgotten as regards one's criminal and judicial past has been recognized by case law on the basis of the right to privacy and personality rights. In the Internet environment, this right could be an appropriate answer to problems raised by the eternal electronic memory (creating the 'eternity effect') combined with the retrieval and gathering power of search engines. Here, these problems are approached through the examples of the criminal case law freely available on the Web and of the Internet newspaper archives equally publicly available. The right to oblivion is not absolute and must give priority to freedom of expression, freedom of the press, the public right to information and public interest in historical research whenever the balance of the conflicting values requires it.

An extended right to oblivion, not reduced to judicial information, is recognized and legally protected by data protection laws. It is valid for any personal data, which is not restricted to private or confidential data. Data protection legislation has set up a quite balanced regime as concerns the right to oblivion. This right is shaped through two main principles: the obligation to erase or anonymise personal data once the purpose of processing is achieved and the right granted to the data subject to object on a justified basis to the processing of personal data.

37. De Terwangne and Moiny (2011), pp. 22-23.
38. *Ibidem*.
39. Asociación Profesional Española de Privacidad (2011).

Beyond this well-established right to be forgotten, an even more extended right to oblivion is claimed. It is intended to be specifically applicable in the networked digital environment. It would mean the automatic deletion of the data, without the data subject having to take any steps to obtain that result. It would thus apply an expiration date to the data without need for a prior analysis on a case-by-case basis. This means the right to oblivion could in turn become a 'privacy by design' obligation. The right to have data completely erased is also claimed for data disclosed by individuals themselves. This specifically aims the sphere of social networks.

However, there are practical difficulties in the implementation of the right to oblivion, and the right inevitably conflicts with other rights, freedoms and legitimate interests. Here again, a balancing test respecting the proportionality principle will hopefully bring the answer as to which value should prevail.

The question of extending the right to be forgotten is still controversial. Either propositions are quite delimited and present the risk, if implemented in data protection legislation, of including very specific answers to specific technological issues, which is no guarantee of long-term applicability of the regulation. Extending the right to be forgotten also raises concern about the restriction it creates on freedom of expression, the public's right to information, and historical and pedagogical interests.

Bibliographical references

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2009). *Estándares internacionales sobre protección de datos personales y privacidad. Resolución de Madrid*. <http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf>

ASOCIACIÓN PROFESIONAL ESPAÑOLA DE PRIVACIDAD (2011). "Response to the Council of Europe consultation on the modernisation of Convention No. 108". In: *Compilation of comments received on the consultation on the modernisation of Convention 108*. <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_01mosRev6.pdf>

ASSEMBLEE NATIONALE (France) (2011). *Révolution numérique et droits de l'individu: pour un citoyen libre et informé*. Rapport d'information par la mission d'information commune sur les droits de l'individus dans la révolution numérique.

COUNCIL OF EUROPE, DEPUTY SECRETARY GENERAL (2010). "Speaking points for the opening of 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>

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?" <http://www.cyberlex.org/images/stories/pdf/contribution_cyberlex_dao.pdf>

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*. No. 194, pp. 40-48.

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. T-PD-BUR(2011)10en, pp. 22-23. <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_10_en.pdf>

DUASO-CALÈS, R. (2002). *La protection des données personnelles contenues dans les documents publics accessibles sur Internet: le cas des données judiciaires*. Mémoire. Montréal: Faculté de Droit, Université de Montréal.

ESCOFFIER, A. M.; DETRAIGNE, Y. (2009). *Rapport d'information sur la vie privée à l'heure des mémoires numériques*.
<http://www.senat.fr/noticerap/2008/r08-441-notice.html>

ETTIGHOFFER, D. (2008). "Les droits de l'homme numérique: le droit à l'oubli".
<http://www.ettighoffer.com/fr/idees/idees8.html>

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.

FLEISHER, P. (2011). "Foggy thinking about the right to oblivion". Peter Fleisher's Blog. 9. March 2011.

GÓMEZ, R. G. (2011). "Google niega a Protección de Datos legitimidad para ordenar la cancelación de contenidos". *El País*, 19 January 2011.
<http://www.elpais.com/articulo/sociedad/Google/niega/Proteccion/Datos/legitimidad/ordenar/cancelacion/contenidos/elpeputec/20110119elpepusoc_5/Tes>

HALLIDAY, J. (2011). "Europe's highest court to rule on Google privacy battle in Spain". *The Guardian*, 1 March 2011.
<http://www.guardian.co.uk/>

PRIVACY INTERNATIONAL (2011). "Response to the Council of Europe consultation on the modernisation of Convention No. 108". In: *Compilation of comments received on the consultation on the modernisation of Convention 108*. June 2011.
<http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_01mosRev6.pdf>

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.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700>

"Spain demands the right to oblivion for its citizens". *Law and the Internet*, The Finocchiaro Law Firm's blog. 31 March 2011.
<http://www.blogstudiolegalefinocchiaro.com/wordpress/?tag=the-agencia-espanola-de-proteccion-de-datos-aepd>

TURK, A. (2009). "La délicate question du droit à l'oubli sur Internet". Interview in *Le Monde*, 12 November 2009.

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: 17-19 September 1997.

WERRO, F. (2009). "The right to inform v. the right to be forgotten: A transatlantic clash". In: A. COLOMBI CIACCHI; Ch. GODT; P. ROTT; L. J. SMITH (eds.). *Liability in the Third Millennium*. Georgetown Public Law Research Paper No. 2. Baden-Baden: F.R.G.
<http://ssrn.com/abstract=1401357>

Recommended citation

DE TERWANGNE, Cécile (2012). "Internet Privacy and the Right to Be Forgotten/Right to Oblivion". In: "VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet" [monograph online]. *IDP. Revista de Internet, Derecho y Política*. No. 13, pp. 109-121. UOC. [Consulted: dd/mm/yy].

<http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-terwangne_esp/n13-terwangne_eng>

ISSN 1699-8154

About the author

Cécile de Terwangne
cecile.deterwangne@fundp.ac.be

Professor Cécile de Terwangne has an MD (University of Louvain) and PhD (University of Namur) in Law, and an LLM in European and International Law (European University Institute of Florence). She is professor at the Law Faculty of the University of Namur (Belgium), where she gives courses in Computer and Human Rights, and Data Protection. She is Research Director at CRIDS (Research Centre on Information, Law and Society).

University of Namur - Faculty of Law
Rempart de la Vierge 5
B-5000 Namur, Belgium