The right to be forgotten under European Law: a Constitutional debate

Pere Simón Castellano[1]

Lex Electronica, vol. 16.1 (Hiver/Winter 2012)

Résumé:

Cet article met en lumière la perspective européenne sur un des plus importants défis que l'Internet et le Web 2.0 présente pour la vie privée et le droit à la protection des données. L'auteur y soulève des problématiques liées à la mémoire numérique et distingue à partir de plusieurs cas où les individus seraient intéressés de réclamer l'oubli tant dans les réseaux sociaux, les journaux officiels des gouvernements et dans les bibliothèques médiatiques numériques. Il trace l'histoire de l'identification du droit à l'oubli dont les fondements ont été définis par les agences françaises, italiennes et espagnoles de protection des données. En conclusion, il pose son regard sur un nouveau cadre européen de la protection des données comprenant le droit individuel à voir leurs données supprimées lorsqu'elles ne sont plus nécessaires à des fins légitimes.

Abstract:

This paper sketches out the European perspective about one of the most important challenges that Internet and web 2.0 involve for privacy and data protection rights. The author describes issues related to digital memory and distinguishes among several cases in which individuals would be interested to call for oblivion: in social networks, in official journals of government and in digital libraries of the media. He then traces the history of the recognition of the right to be forgotten which has been defined basically

[1] Pere Simón Castellano, junior research fellow (BR) at the Department of Public Law, area of Constitutional Law, at University of Girona (UdG), pere.simon@udg.edu. This work is inserted in the research project funded by the Spanish Ministry of Science and Innovation, with reference DER2010-15778, about 'The changes in the model of relationship between the judicial power and the autonomous communities' (University of Girona /Autonomous University of Barcelona).

by French, Italian and Spanish Data Protection Agencies. Finally, he put his eyes on a new European framework of data protection in which will be included the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes.

Table of contents

I. Introduction: Internet and the age of total recall

In the last decades we have observed the unstoppable rise of new Information and Communication Technologies (hereinafter ICT), which have gradually introduced changes in social life, in working times and essentially in interpersonal relationships. Specifically, Internet and Web 2.0 are the new paradigm of public communication process by creating a new scenario where the communications take place horizontally,

Lex Electronica, vol. 16 n°1 (Hiver/Winter 2012)

without hierarchy, globally and in anonymous fashion. The law must control this new environment and should give answers to current issues resulting from the worldwide network architecture.

Furthermore we find many topics on which the law must answer : the legal framework for freedom of speech on Internet[2], the risks of de-contextualization of published information[3], the liability information being disseminated[4], the limits of anonymity on the network[5], the perpetuity of the shared information — which is the subject of this work —, identity theft[6], the citizenship playing an active role on spreading news, *etcetera*. All this themes will be studied in the near future, and most of them will have beheld under a new comprehensive approach on personal data protection in the European Union, which will end with a deep reform of the European Directive 95/46/EC on data protection.

---

[2] The law can serve to encourage people to be more aware of the consequences of their speech and can fix a reasonable balance between privacy and free speech on Internet. A book that proposes legal reforms on this topic is Daniel J. Solove, *The future of reputation: gossip, rumor, and privacy on the Internet*, New Haven and London, Yale University Press, 2007. See also Dragos Cucereanu, *Aspects of Regulating Freedom of Expression on the Internet*, School of Human Rights Research Series vol. 27, Utrecht, Intersentia, 2008.

[3] See on this topic Frank Dumortier, "Facebook and Risks of 'De-contextualization' of Information ", in Serge Gutwirth, Yves Poullet and Paul de Hert (eds.), *Data Protection in a Profiled World*, London, Springer, 2010, pp. 119-138.

[4] See Miquel Peguera, "Internet Service Providers Liability in Spain", *Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 1(3), 2010, <http://www.jipitec.eu/issues/jipitec-1-3-2010/2823/peguera-isp-liablility-spain.pdf>.

[5] Anonymity on the net is sometimes synonymous of immunity owing to a law that currently immunizes people for comments on their blogs, even when they know that such comments are harmful, libelous or invade the privacy of a third party. In addition it is really hard to find who said what on the net. For this reason some authors plead for a system of pseudo-anonymity on the Internet. In this type of anonymity the identity of the message sender may seem truly anonymous because it is not easily uncovered. However, it is possible to discover the real identity of the pseudo-anonymous message sender. Thus allowing citizens to engage and publish their opinions without fear of retaliation; nonetheless it forces them to take ultimate responsibility for their actions and comments. See Milana Homsi and Andy Kaplan-Myrth, "Online Anonymity and John Doe Lawsuits", *University of Ottawa Canadian Internet Policy and Public Interest Clinic*, January 2005, <http://www.cippic.ca/en/online-anonymity-and-john-doe-lawsuits>. See also Ignacio Alamillo Domingo, « Identidad electrónica, robo de identidad y protección de datos personales en la red », in Ignacio Alamillo Domingo *e. al.*, *Robo de identidad y protección de datos*, Cizur Menor, Aranzadi, 2010, at p. 299.

[6] Individual victims of identity theft of course can have their dignity damaged and are inconvenienced and embarrassed. An interesting study of this phenomenon is in Ian C. Ballon, *E-Commerce and Internet Law: A Legal Treatise With Forms*, Second Edition, 4 vol., Part VII, Chapter 46: "Identity thef, Eagan" (Minnesota), Thomson/West Publishing, 2009.

In this wide range of new threats to people, stand out the issue of continuity of the information on Internet, which combine a huge storage capacity with tools like search engines in order to ease the searching and finding of what you are looking for. The web records everything — written documents, photos, images, quantitative data, audio recordings, and so on — and forgets nothing. Indeed, on 2.0 environments all these records are available for transmission, indexation, analysis, storage, retrieval, and visualization in a single media. Every status update, online photo, blog entry and Twitter post by and about us can be stored forever. Much more than this: if someone searched with our names and surnames on search engines, they can easily find a lot of personal and private information about our past life. Our data is recorded on the network as if it were a tattoo that followed us for a lifetime. Consider, for example, many young people who currently share information — videos, photos, status updates, etc. — shameful, obscene and embarrassing. They are influenced by the social trend to share private life on a public space because of the need to socialize and a misconception of the social networking cosmos as a site for relationship among 'friends', when often what is shared is open to the global world because all the netizens[7] have not even bothered to set up and customize their online privacy tools[8].

But the issue is what happens when these young guys want to be judges, politicians or doctors? Probably they will have difficulty to find work if their past mistakes are perfectly remembered. Additionally, we must remember that the majority of the recruiters and human-resource professionals make online researches about candidates to decide who will be selected[9].

[7] We use the term netizens to talk about citizens that are involved in online communities and are users of Internet. More specifically, the term netizen is a portmanteau of the English words Internet and citizen.
[8] The social networks usually give to the citizens the option to individually change the audience of their posts by customizing with who share personal information.
[9] The web contains information essentially to make decisions about the candidates. For this reason we can observe that seventy percent of United States recruiters report that they have rejected candidates because of information found online, like photos and discussion-board conversations and membership in controversial groups. The data come from a Microsoft survey cited on this article: "Should you check Facebook before hiring?", published in *The Washington Post* on January 22nd, 2011, <http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012203193.html>.

The pursuit of the past, the perfect reminder and whole retention of information can be the end of oblivion as well as poison the present and block the future. It is human nature for the people to commit mistakes and have regrets. People change, evolve, mature and even contradict each other along their life path. Therefore, compared to the enormous potential of ICT and digital memory, the right to be forgotten tries to ensure the privacy and reputation of individuals, avoiding the constant persecution of the past.

This new reality, a world of perfect remembering that nothing can be forgets, contrasts sharply with the fragility of human memory. For this reason it has arisen on the European public, a debate about the need to regulate the 'right to be forgotten' or the 'right to oblivion' that would build on the rights of the personality, encompassing several elements such as rights to a private life, reputation, data protection, intimacy and dignity.

Some ideas that seek to limit the digital memory have been proposed by legal experts who belong to the common law legal tradition: "*Like personal financial bankruptcy, or the way in which a state often seals a juvenile criminal record and gives a child a 'fresh start' as an adult, we ought to consider how to implement the idea of a second or third chance into our digital spaces.*"[10]. The most powerful voice on this topic has been the voice of Viktor Mayer-Schönberger who tells us the following:

> "*I propose that we shift the default when storing personal information back to where it has been for millennia, from remembering forever to forgetting over time. I suggest that we achieve this reversal with a combination of law and software. The primary role of law in my proposal is to mandate that those who create software that collects and stores data build into their code not only the ability to forget with time, but make such forgetting the default. The technical principle is similarly simple: Data is associated with meta-data that defines how long the underlying personal information ought to be stored. Once data has reached its expiry date, it will be deleted automatically by software, by Lessig's West Coast Code. This may sound*

[10] Jonathan L. Zittrain, *The Future of the Internet, And How to Stop It*, Virginia, Yale University Press, 2008, pp. 228-229.

either simplistic or radical (or both), but I believe it is neither, as I hope you agree when you come to understand how I envision it to work, and when I explain its advantages and shortcomings."[11].

On the other hand, the debate in Europe has arisen differently. In particular, some European voices have defended that the right to be forgotten can be considered as being contained on the principles of data protection. The basic principle governing the processing of personal data is the consent[12], such that, on principle, personal data must be collected, processed or communicated to third parties with the data subject's consent. If there isn't consent nobody can publish, collect or process this personal data, unless there is a legal or other overriding legitimate reason to share the information – for example, in case of official state journals or media news –. On the other hand, we must remember that personal information may be kept for no longer than is necessary and must be kept up to date. If some data was collected or communicated for a specific purpose, the data must be deleted or cancelled after the purpose for which it was collected is achieved. Specifically, the data must be kept in a form that 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[13].

Returning to the topic at hand and once already identified the problem, this paper will focus on how European Data Protection Agencies – in France, Italia and Spain – and the European Commission have reacted against troubles that digital memory and search engines cause to individuals rights, especially to data protection and online reputation. We also study the different cases in which it is possible to apply the so-called right to be forgotten. In addition, we will see that the debate about the

[11] Victor Mayer-Schönberger, "Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing", *Working paper RWP07-022,* John F. Kennedy School of Government, Harvard University, April 2007, p. 17, <http://www.vmsweb.net/attachments/pdf/Useful_Void.pdf>.
[12] "The data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.", EU Directive art. 2.h).
[13] EU Directive art. 6.1.e).

recognition of this right is not exactly new; indeed, it is no more than an old matter in a new context.

II. Living in a world that forgets nothing: some case studies and their specifics problems

A) The oblivion of Personal Data in Social Networks

Stacy Snider, a 25-year-old teacher in training at Conestoga Valley High School, shared a photo on her MySpace in which she appears wearing a pirate's hat while drinking from a plastic cup, under the caption "*Drunken Pirate*"[14].

This publication was the source of her problems to get her teaching degree. First, her supervisor discovered the photo and the caption and told her off stating that her conduct was unprofessional. Secondly, the dean of Millersville University School of Education, where Stacey was enrolled, said she had, albeit indirectly, encouraged young people and her under-age students to drink. For all those reasons the university denied her teaching degree and against this decision, Stacy, clearly disagreeing with this decision, sued. Stacy did it arguing that she had been penalized for her legitimate after-hours behavior. She defended that her "*Drunken Pirate*" was protected by the freedom of speech and the First amendment rights[15].

[14] For more information about the facts of the case *Stacy Snyder*, you can see the article titled "Court Rules against Teacher in MySpace 'Drunken Pirate' Case", published in *The Washington Post* on December 3rd, 2008, <http://wapo.st/g3SH>.
[15] This case is also described in Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, New Jersey, Princeton University Press, 2009, pp. 1-3.

However, the *District Court for the Eastern District of Pennsylvania*[16] rejected the arguments pointed out by Stacy in the lawsuit. The First Amendment only protects matters of public concern and does not protect social network posts although these came from a public employee. So, in conclusion, the federal court is not the appropriate *forum* in which to review the wisdom of a personnel decision taken when a public employee speaks upon matters of a personal interest. The case shows perfectly the negative consequences that eventually can cause the shared information in social networks that is public and visible to others. Nevertheless, have citizens the right to cancel the shared personal data on the social networks before they affect their reputation?

Data protection rights have a huge scope in Europe for *Directive 95/46/EC* (hereinafter EU Directive) which give the individual the right to prevent or control another party's use of data that is personally identifiable to the individual, whether or not sensitive or confidential, that was lawfully obtained by the other party. Especially, that means the right of individuals to delete or cancel the personal data when data subjects have not given the consent or withdrawn it. Indeed, in order to be lawful the processing of personal data must be carried out with the consent of the data subject. The EU Directive fixes that "*Member States shall provide that personal data may be processed only if (a) the data subject has unambiguously given his consent*"[17]. Therefore data protection gives individual far greater rights to control uses of personal information by third parties. The European principles for data protection creates and protects an individual's interests relating to collection, processing, or other use of information identifiable with that person. One of the most important principles for our topic – the right to be forgotten – is the "*Collection Limitation Principle*" whereby data collection should be with the knowledge or consent of the subject and by fair means.

Therefore, we can state that individuals have the right to claim cancellation and rectification of information identifiable with them in case other netizens share personal

[16] The United States District Court for the Eastern District of Pennsylvania, December 3rd, 2008, Case 2:07-cv-01660-PD : <http://voices.washingtonpost.com/securityfix/Decision%202008.12.03.pdf>.
[17] EU Directive art. 7.a).

data in a social network without data subject consent. In other words, against the publication of images, videos and comments in social networks that contain personal or intimacy data that may injure the reputation of people, those affected who have not consented could relying on European legislation on data protection exercise their right of cancellation and rectification.

But, what happens when personal data is published in a social network by the data owner? It is generally assumed that individuals have a right to revoke or withdraw their consent to the processing of their personal data by others; nonetheless this may not be straightforward in practice, or addressed adequately by the law. In spite of the right of withdrawal, the consent is not explicitly stated on the EU Directive, this could be based[18] on the right to "*object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data*"[19].

However, the situation is clearer in European countries like Spain, where the data protection law — *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* (hereinafter LOPD) — stated specifically the right to withdraw their consent. With preciseness art. 6.3 of LOPD provides the right to withdraw the consent when there are justified or well-grounded reasons, with no retroactive effects attributed. So in conclusion the individuals have the chance to revoke their consent and ask the person in charge of social network to delete their personal data, even when data is published by the data owner.

Nevertheless, we must clarify that the rights of access, objection, rectification and cancellation of information published in the field of social networks do not provide a real or effective solution to the problem of the continuity of information in the network. Mainly because of the information, which may influence the future of the data

[18] In this same vein see Liam Curren and Jane Kaye, "Revoking consent: A 'blind spot' in data protection law? ", *Computer Law & Security Review*, Vol. 26, Issue 3, May 2010, pp. 273-283.
[19] EU Directive art. 14.a).

owner, was exposed in the public tribune and it is possible that had been copied or downloaded by different global users. In this way that possibility may prevent a full and effective delete of information. However, with the access, objection, rectification and cancellation of personal data that social networks contain at least it could guarantee the right of citizenship to control the dissemination and access to their personal data, and in a negative sense, to expel third party for the knowledge of these by ensuring its future oblivion.

B) The oblivion of Personal Data in Official Journals of Government

In Spain, a deputy headmaster of a school found it difficult to remember that some years ago was fined for urinating in the street, but an official sanction is the first search result when their students place his name into Google[20]. There are many negative consequences of the knowledge of information that was published only in order to pay the fine. Teachers, students and their parents give more importance to the past mistakes of the teacher than for his teaching abilities. The reputation of the deputy headmaster was strongly hurt.

That is just a small case amongst many others. What about all the information and personal data contained in official journals of government? Fines, judgments in which the name is not hidden, received grants and subsidies, governmental pardons, names and surnames of people to grant amnesty, etc. All these kind of information could affect reputation, privacy and dignity and one must insist on the multiplying disclosure effects of the Internet and, to a greater extent on search engines, and their repercussion on personal data protection, especially that of no public transcendence. On Internet every statement has a potentially global audience, nothing is forgotten, and

[20] For more information about the facts of this case you can see the article titled « Los 93 que no quieren aparecer en Google », published in *Público* on January 18th, 2011, <http://bit.ly/gK8uGT>.

everything can spread beyond the private sphere. This makes it much harder for victims of gossip and defamation to be socially rehabilitated.

However, what can individuals do against the enormous extension and dissemination of official government documents posted on the Internet? These documents are public, and people have the right to access public information, nonetheless the easiness which search engines give us to find obscene or embarrassing information on the governmental websites is out of proportion.

Formerly, if we wanted to find that information we would have gone to see the official document and read it fully. Today, by contrast, we need only to know the name and last name of a person and put them in a search engine to find everything the web hosts about this person. That is an easy way to find embarrassing data in public or official documents; for this reason this topic has been studied by Spanish Data Protection Agency – *Agencia Española de Protección de Datos* – (hereinafter AEPD).

AEPD has solved this issue by arguing that citizens must hold real and effective mechanisms to ensure oblivion, meaning that any citizen who is not subject to a newsworthy event of public importance does not have to be resigned to see how their data are disseminated on the Internet without being able to react or correct it[21]. Thus the right to be forgotten would turn public information into private information at a certain time by no longer allowing third parties to access such information.

The legal grounds of this 'new' right to be forgotten could be found in the four principles of data protection[22] : "*Collection Limitation Principle*" which requires consent as we have studied *supra*; "*Purpose Specification Principle*" -

a purpose should be specified at or before collection –; "*Data Quality Principle*[23]" – the data should be relevant to the purpose for which collection occurred and should be kept

[21] AEPD Decision procedure no. TD/00463/2007, <http://bit.ly/pHPPUv>.
[22] All these principles could be found both in EU Directive art. 6.1 and in LOPD arts. 4-12.

accurate, complete, current, and no longer than is necessary for the purposes for which the data was collected –; "*Use Limitation Principle*" – no disclosure or use should occur for purposes other than the specified use without consent of the subject or authorization by law –. Thus AEPD argues that the right to delete data trails in the Internet should be understood as an extension of the data protection principles. More precisely AEPD stated that:

> "*In light of the foregoing* [mainly refers to Collection Limitation and Data Quality Principles]*, it can be proclaimed that a citizen who neither has the status of a public personality nor is the subject of a news event of public relevance needs to accept that his personal data circulate on the Web without being able to react or correct the unlawful inclusion thereof on a universal communication system such as the Internet. If requiring the individual consent of citizens to include their personal data on the Internet or demanding technical mechanisms to prevent or filter the non-consented incorporation of personal data might represent an unbearable barrier to the free exercise of the freedoms of speech and information as a form of prior censorship (which is ruled out by the Constitution), it is equally true that it is blatantly legitimate that a citizen who is not under the obligation of submitting to the discipline of the exercise of the aforesaid freedoms (because his personal data are not of public interest and, in consequence, knowledge thereof does not contribute to shaping a free public opinion as a basic pillar of a democratic State) must enjoy reactive mechanisms protected by Law (such as the right of cancellation of personal data) preventing the secular and universal conservation of his personal information on the Web.*"[24].

The referred decisions were issued following the request of individuals who wanted Google not to associate their names with negative events which had occurred years ago and that were published in the online editions of newspapers and official journals of regional governments.

---

[23] This principle was collected for the first time in Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data by setting. It specifically stated that personal data undergoing automatic processing shall be "preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored" — art. 5.e) —.
[24] AEPD Decision procedure no. TD/00266/2007.

C) The oblivion of Personal Data in the media

Another case study appears with regard to the dissemination of personal data published for the media in the development of its information role. Newspaper and periodicals digital libraries have also search engines that allow the searching and finding of embarrassing news about past mistakes. News on individuals who are not considered public figures, but they did something in the past that had public importance. For example, news about crimes, criminals, defendants and their investigation thereof. The problem being that sometimes the judge ended up giving reason to the person appearing in the past news. Therefore if someone searches in digital libraries of newspapers they can easily find the name and last name and other personal data of a person linked with a crime even though courts acquitted him. But, who repairs reputation damage caused by the knowledge of personal data linked with information that at the time of publication had public interest but later has become outdated, inaccurate and uncertain?

Logically, the right of the public to receive information or reports on judicial proceedings is a core value protected by the constitutional guarantee of freedom of expression[25]. But this freedom is not absolute and could be limited if personal data in reports on judicial proceedings wasn't kept up to date and turned into false, inaccurate or outdated data.

As we have seen so far, the AEPD considered that personal data owners have the right to object data processing performed by search engines, even when it is about public or legitimate information such as official journals of government as long as they do not have current public importance. On the other hand, AEPD has argued that the treatment given in the digital media libraries is framed within the freedom of

[25] "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers". *Charter of Fundamental Rights of the European Union (2010/C 83/02)*, art. 11.

information[26]. This interpretation has been criticized in different ways in the Spanish legal doctrine — *hornbooks* —. Some authors[27] have understood that digital media libraries are not a means of communication strictly speaking as such should not be regarded as publicly available sources in accordance with LOPD – art. 3.j) –, which only recognizes the public character of the media and not of some apps – search engines — of their digital libraries. In this same vein personal data owners should have the right to object to the processing of their personal data by the search services of the digital newspaper libraries.

Other authors, however, maintain that it would be paradoxical that "*information with public interest and obtained with scrupulous regard to the canon of professional diligence may be consulted in the archive of the printed edition of a newspaper and, by contrast, has disappeared from the online edition*"[28].

I agree with the idea that distinguishes between information that had public interest when it was published – public source according to LOPD art. 3.j) – and the treatment that the search engines of digital medias libraries gives information[29]– that multiplies disclosure effects, especially negatives –. So, as it happens with oblivion required to common search engines, information should neither disappear of the Internet, nor stay unavailable at printed edition of newspapers. The right to be forgotten under digital media libraries means that individuals have the right to object to finding

[26] AEPD Decision procedure no. TD/01164/2008 and TD/01540/2008.
[27] Lorenzo Cotino Hueso, « Datos personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público (Art. 3 de la LOPD) », in Antonio Troncoso Reigada (dir.), *Comentario a la Ley Orgánica de Protección de Datos Personales*, Cizur Menor, Civitas, 2010, pp. 289-315.
[28] The original document is in Spanish : « una información de interés público y obtenida con escrupuloso respeto al canon de la diligencia profesional se pueda consultar en la hemeroteca de la edición escrita de un diario y, por el contrario, haya de desaparecer de la edición digital ». See Marc Carrillo, « El derecho al olvido en Internet », article published on *El País* in October 23rd, 2009, <http://bit.ly/2srRjO>.
[29] See for more details my work Pere Simón Castellano, « El régimen constitucional del derecho al olvido en Internet », in Agustí Cerrillo i Martínez, Miguel Peguera, Isabel Peña-López, Mónica Vilasau Solana (coords.), *Net Neutrality and other challenges for the future of the Internet*, Barcelona, Universitat Oberta de Catalunya, UOC-Huygens, 2011, pp. 391-406.

easily personal data, which is outdated or inaccurate, that contains embarrassing information that could affect reputation, dignity and privacy of the data owner.

III. An old matter in a new context: data protection on court recordings

The discussion about the balance between freedom of expression and privacy in the issue of electronic access to court records is an old matter. The so-called "*Open Court Principle*" is a hallmark of a democratic society and applies to all judicial proceedings in order to guarantee the integrity of judicial processes by demonstrating that justice is administered according to the rule of law. Openness of courts records also allows the maintenance of the independency and impartiality of courts and it is especially useful to maintain the public confidence in the justice system.

Nevertheless, the open court principle and its inherent background concept has been a discussion point in Continental Europe, United States, Canada and Australia for many years. The extension of the open court principle in the matter of public access to court records differs greatly depending on the legal tradition to which each country belongs.

In the vast majority of the European countries that belong to a civilian law legal system, the people who were convicted in court have the right to make this personal data disappear after a certain time period had elapsed. Specifically, in Spain, there is a center — *Centro de Documentación Judicial*[30] (hereinafter CENDOJ) — which is in charge of guaranteeing the public electronic access to all judicial sentences after concealing the identity — fictitious names — of the parties. Furthermore, only the sentences of the Constitutional Court — *Tribunal Constitucional* — and the sentences

[30] See website <http://www.poderjudicial.es/search/index.jsp>.

of the *Court of Justice of the European Union* are published entirely with real names, surnames and other personal data of the parties[31].

In the same manner, access to information contained in the criminal records in Spain is subject to restrictions and when legally established time has passed[32], either on application or *ex officio*, the criminal records are then to be stored in a special and separate registry which only can be consulted by the Spanish Courts and police[33]. This makes it impossible to formally recall the names and surnames of the criminals, and encourage proper reintegration and rehabilitation of offenders in society and guarantee their privacy. The regulation of prescription and cancellation of the criminal records in countries which belong to a civilian law legal system to reinforces the arguments for the recognition of the right to be forgotten.

On the other hand, the countries that belong to a common law legal system have defended that the covertness of court proceedings is the exception and openness the rule. For example, in Canada, the right to open courts generally outweighs the right to privacy. The *Supreme Court of Canada* has recently reaffirmed:

> "*Openness is necessary to maintain the independence and impartiality of courts. It is integral to public confidence in the justice system and the public understands of the administration of justice. Moreover, openness is a principal component of the legitimacy of the judicial process and why the parties and the public at large abide by the decisions of courts.*"[34].

Therefore in Canada the principle of open courts entails a common law right to public access to court records which prevails over the right to privacy[35]. Canadian case

---

[31] See Joaquín Silguero Estagnan, « Régimen de la protección de datos en la publicación de las decisiones judiciales », *Revista Española de Protección de Datos* no. 5, 2009, pp. 55-154.

[32] More specifically, the criminal record would be cancelled in six months for low penalties, two years for penalties that not exceeding 12 months imposed for crimes and reckless, three years for the remaining less severe penalties, and five years for severe penalties. See *Spanish Criminal Code*, art. 136.1.b).

[33] See *Real Decreto 95/2009, de 6 de febrero, por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia*, art. 5 and 6.

[34] *Toronto Star Newspapers Ltd v Ontario* [2005] SCC 41.

[35] "Public confidence in the integrity of the court system and understanding of the administration of justice are thereby fostered. As a general rule the sensibilities of the individuals involved are no basis for

law has established well accepted categories in which the right to public access to court records can be displaced in order to respect the nature of others social values, essentially by protecting the innocent and the vulnerable[36], promoting fair and effective administration of justice, allowing access to the courts[37], and preserving trade secrets and other commercial interests[38].

There are other exceptions relating to public access to court records set up in statutory prescriptions in the criminal, civil and family law context. We will illustrate some examples. The *Child Protection Act* provides that "*a person who publishes information that identifies parties to an agreement or proceedings pursuant to this Act, other than information respecting the child of that person*"[39] is committing an offence. In the criminal context, the *Youth Criminal Justice Act* provides generally that court files and documents are not accessible to the public[40], and the *Canadian Criminal Code* provides among others a mandatory publication ban upon application by the victim of sexual assault[41].

Thus we can easily become aware of the huge difference regarding the concept of open court principle and the right of public access to court records among countries that belong to a civilian law or common law legal cultures[42]. The countries that follow the civilian law tradition are more likely to recognize the right to be forgotten. In the same vein, Pierre Trudel said:

---

exclusion of the public from judicial proceedings.". *MacIntyre v Nova Scotia* (Attorney General) [1982] 1 SCR 175 at 185.

[36] See for example *Canadian Broadcasting Corp v New Brunswick* (Attorney General) [1996] 3 SCR 480 at [71].

[37] *Dagenais v Canadian Broadcasting Corp* [1994] 3 SCR 835. In this sentence we observe that publication of pre-trial could undermine the right of an accused to a fair trial, in particular in case of trial by jury.

[38] *Sierra Club of Canada v Canada (Minister of Finance*) [2002] SCC 41.

[39] *Child Protection Act,* R.S.P.E.I. 1988, c. C-5.1, Section 59 (k).

[40] See *Youth Criminal Justice Act,* S.C. 2002, c.1, Part 6 – Publication, records and information – Protection of privacy of young persons.

[41] *Criminal Code*, R.S.C. 1985, c. C-46, Section 486 (3).

[42] An interesting comparison on this topic between Spain and the United States can be found in James B. Jacobs and Elena Larrauri, « ¿Son las sentencias públicas? ¿Son los antecedentes penales privados? Una comparación de la cultura jurídica de Estados Unidos y España », *Indret, Revista para el análisis del Derecho* no. 4, 2010, pp. 1-52, <http://www.indret.com/pdf/769_es_1.pdf>.

> « *Dans les systèmes juridiques d'inspiration civiliste, l'oubli se présente comme un droit indirect. Il découle du droit à la vie privée ou même du droit à la réputation. L'oubli présuppose une information ayant déjà circulé dans un espace collectif. L'oubli a pour objet de l'information qui n'est pas secrète, qui a déjà été portée à la connaissance d'une ou de plusieurs personnes. À l'égard d'une personne, un droit ne se conçoit pas sans l'existence d'une obligation imposée aux autres. La violation de l'obligation d'oubli suppose d'identifier un devoir d'oublier.*»[43].

So, in conclusion the topic of the right to oblivion is not new. There has been for a long time a debate about meaning and extension of the open courts principle and the right to public access to court records. However, at this point, we can understand the difference between the right to oblivion and the right to be forgotten. The first is regarded with the debate about the right to public access to court records and is normally used to refer to the already intensively reflected situation that an historical event or a criminal record that should no longer be remembered due to the length of time elapsed since its occurrence. Thus the right to oblivion means the right for individuals to constrain the access to their personal data contained in criminal and court records in order to reintegrate into society and not have to be pursued by past actions. On the other hand, the new concept of the right to be forgotten is more than this and also tries to turn public information into private information at a certain time by no longer allowing third parties to access such information. The right to be forgotten is a guarantee for the individuals against prejudice that the data owner could face in case of diffusion through the Internet, without duration limits, of his personal data.

[43] Pierre Trudel, « L'oubli en tant que droit et obligation dans les systèmes juridiques civilistes », p. 1, <http://www.chairelrwilson.ca/cours/drt6913/Notes%20oubli3808.pdf>.

IV. European Data Protection Agencies and its role by recognizing the right to oblivion: a comparative view.

A) French Data Protection Agency

The role of the *Commission nationale de l'informatique et des libertés* (hereinafter CNIL) is especially interesting because it was pioneer in recognizing the right to be forgotten – *le droit à l'oubli* – in accordance with data protection principles, to be precise with data quality principle. At the end of the twentieth century, the CNIL noticed that:

> « *Jamais sans doute les principes établis par la loi du 6 janvier 1978 n'ont eu une telle actualité. A l'heure des réseaux et du 'tout numérique', ces principes sont autant de sauvegardes: principe de finalité, contrôle de la pertinence des données collectées, confidentialité des informations nominatives, droit d'accès et de rectification, droit d'opposition, droit à l'oubli enfin.* »[44].

Later, the CNIL doctrine smoothly moved into website context, understanding data protection principles are more relevant than ever with the advent of digital networks. In 2009, CNIL even reached a favorable statement in the recognition of the fundamental nature of the right to be forgotten:

> « *Il est inacceptable et dangereux que l'information mise en ligne sur une personne ait vocation à demeurer fixe et intangible, alors que la nature humaine implique, précisément, que les individus changent, se contredisent, bref, évoluent tout naturellement. Il en va, pour tous, de la protection de la liberté d'expression et de la liberté de pensée, mais aussi du droit de changer d'avis, de religion, d'opinions politiques, la possibilité de commettre des erreurs de jeunesse, puis de changer de vie.*

[44] CNIL, *20ème rapport d'activité,* Paris, La Documentation Française, 1999, p. 6.

> *C'est pourquoi notre Commission se félicite du débat qui s'ouvre actuellement en France sur ce sujet, qui souligne avec force le caractère fondamental du "droit à l'oubli".* »[45].

Moreover, in France, a bill that has already been approved by the Senate but (yet) has not been approved by the National Assembly explicitly recognizes the existence of the right to be forgotten. More precisely, it states that:

> « *Au total, il convient de noter que plusieurs mesures de la présente proposition de loi permettent de donner une plus grande effectivité au droit à l'oubli numérique* [...]*: l'information spécifique, claire et accessible donnée aux personnes, avant tout traitement, mais également de manière permanente, sur le site Internet du responsable du traitement, de la durée de conservation des données; la possibilité de demander à la CNIL, pour les traitements déclarés auprès d'elle* [...]*; l'exercice plus facile du droit d'opposition, renommé, pour plus de clarté, droit à la suppression des données* [...]*; la possibilité de saisir plus facilement et plus efficacement qu'aujourd'hui les juridictions civiles en cas d'impossibilité pour les personnes d'exercer leur droit à la suppression des données* »[46].

B) Italian Data Protection Agency

The *Garante per la Protezione dei Dati Personali* (hereinafter *Garante*), which is the highest governing body for the protection of the right to data protection in Italy, resolved a case in November 2004 about the right to be forgotten – *diritto all'oblio* – where it recognized its existence based on art. 11[47] of the *Codice in materia di*

[45] CNIL, *30ème rapport d'activité,* Paris, La Documentation Française, 2009, p. 29.
[46] *Proposition de Loi visant à mieux garantir le droit à la vie privée à l'heure du numérique*, submitted by Yves Détraigne and Anne-Marie Escoffier, senators, recorded by the Senate Presidency, p. 8, <www.senat.fr/leg/ppl09-093.html>.
[47] « Art. 11. Modalità del trattamento e requisiti dei dati (…) b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi *[...]* ». *Codice in materia di protezione dei dati personali*, art. 11.b). In English words the personal data may only be collected and recorded for specific, explicit and legitimate purpose. Obviously, when that disappears the treatment is no longer justified.

protezione dei dati personali (Italian data protection law), which contains the data quality principle. To be precise the *Garante* states that:

> « *Peraltro, le modalità di funzionamento della rete Internet consentono, in particolar modo attraverso l'utilizzo di motori di ricerca, di rinvenire un consistente numero di informazioni, riferite a soggetti individuati, più o meno aggiornate e di natura differente. La questione sollevata dai ricorrenti è di particolare interesse e delicatezza coinvolgendo il dovere di informazione da parte di organi pubblici sulla propria attività, i diritti di utenti e consumatori, ma anche quelli dei soggetti cui si riferiscono i dati diffusi, in particolare del diritto all'oblio una volta che siano state perseguite le finalità alla base del trattamento dei dati (art. 11 del Codice)* [as previously mentioned, its wording is equivalent to data quality principle]. *Decorsi determinati periodi, la diffusione istantanea e cumulativa su siti web di un gran numero di dati personali relativi ad una pluralità di situazioni riferite ad un medesimo interessato può comportare un sacrificio sproporzionato dei suoi diritti e legittimi interessi quando si tratta di provvedimenti risalenti nel tempo e che hanno raggiunto le finalità perseguite* »[48].

Thus the *Garante* has recognized that the data quality principle included in art. 11 of Italian data protection code also means a statement of the right to be forgotten that involve the right to delete personal data when no longer useful to the purpose for which it was processed. The right to be forgotten acts as an instrument to pursue effective enforcement of the data quality principle, which requires data being used only for the

[48] A possible translation of the text in English is the following: "Moreover, the manner in which Internet works allows, in particular through the use of search engines, to find a substantial amount of information referred to people identity, more or less up to date and of a different nature. The question raised by the applicants have particular interest and sensitivity because it involves the duty of information by public bodies on its activities, the rights of users and consumers, and also those of individuals whose data disclosed, including the right to be forgotten once they have been pursued the underlying intentions of the data processing (Article 11 of the Code). At any time after certain periods, the instantaneous and cumulative spread of a large number of personal data that websites contain relating to a variety of situations, with regard to the same subject, may involve a disproportionate sacrifice of his rights and legitimate interests if it is not necessary to going back in time, especially when personal data have already achieved the pursued objectives". Garante Decision *Reti telematiche e Internet – Motori di ricerca e provvedimenti di Autorità indipendenti: le misure necessarie a garantire il c.d. diritto all'oblio',* November 10th, 2004, <http://www.garanteprivacy.it/garante/doc.jsp?ID=1116068>.

purpose for which collection occurred and it should be kept accurate, complete, current, and no longer than is necessary for the purposes.

C) Spanish Data Protection Agency

Although later than the French and Italian counterparts, the AEPD has recognized the right to be forgotten build on data protection principles, basically on data quality, collection limitation and purpose specification principles. However, the Spanish Data Protection Agency has been a pioneer by extending and defining the 'new' right to be forgotten. As we have seen up to now, the AEPD has provided that a citizen who neither has the status of a public personality nor is the subject of a news event of public relevance has the right to react and correct the unlawful inclusion of his personal data on Internet[49], which multiplies disclosure negative effects due to the fact that search engines provides a greater extent of the information.

So in conclusion the AEPD has ordered Google to delete links on its search engine to any website containing out of date or inaccurate personal data about individuals and, thus, breaching their right to be forgotten. The Spanish Data Protection Agency considered that individuals have both the right to cancel personal data published without data owner consent and the right to object data processing performed by search engines, even when it is about public or legitimate information as official journals of government if that information has not a current public relevance.

Google states that information made available by third parties is public and its removal should be considered as a matter of someone else. In particular, Google believes that Spanish and European law rightly hold the publisher of material

[49] See AEPD Decision procedure no. TD/01335/2008 and TD/00627/2009.

responsible for its content[50]. For this reason Google faced off against AEPD decisions by claiming in the Spanish National Court – *Audiencia Nacional* – that only publishers, and not search engines, may be deemed responsible for contents published through their websites and on the Internet. With this legal battle, an important debate started in Europe about the balance between the right to be forgotten, on one hand, and the freedom of speech and information on the other.

It is likely that *Audiencia Nacional* take times to response because it has requested a preliminary ruling from the Court of Justice of the European Union basically on two matters[51]. First, whether Google must guarantee the rights to have data deleted and the right to object referred to in Articles 12.b) and 14.a) of the European Data Protection Directive. Second, whether AEPD may require Google to delete or block the information, even if its preservation at the site of origin is lawful, but the applicant considers that its appearance in search results threatens their privacy, dignity or right to oblivion.

The upcoming decision of the Court of Justice of the European Union will have a great significance, binding not only the Spanish courts but also all of the national courts of the European Member States. In the near future we will see how the European Court of Justice defines, interprets and understands the right to be forgotten and its limits. It is really likely that the final result will be influenced by the new framework in data protection — modification of EU Data Protection Directive — in which the European Commission is going to address this matter.

---

[50] To be precise Google consider that requiring intermediaries like search engines to censor material published by others would have a profound chilling effect on freedom of expression. See Peter Fleischer, "'The Right to be Forgotten', seen from Spain", blog entry published on September 5th, 2011, <http://bit.ly/qBMJmL>. Peter Fleischer is *Google's Global Privacy Counsel*.

[51] See *Providencia Audiencia Nacional (Sala de lo Contencioso-Administrativo)*, first section, no. procedure 211/2009.

V. The incorporation of the right to be forgotten in the European political schedule in the context of reform of Directive 95/46/CE

Although the vast majority of the principles and rights enshrined in the EU Directive remain in full force and validity until today, the truth is that ICT's, Internet and Web 2.0 have changed completely the process of public communication, the context or environment where the data is disseminated. The challenges to privacy and the right to data protection have been markedly increased in a society that treats in the public space the private life matters, with a citizenship that plays an active role both briefing and, mainly, sharing personal information in real time and globally. Social networks are the best example of how people share private information, usually to socialize. In this context, there are many voices from Europe calling for a new directive on data protection, based on a comprehensive approach capable to face up the enormous threats connected with technological advancement.

Peter Hustinx, one of the most powerful voices in Europe, who is the European Data Protection Supervisor, tells us that "*an interesting example* [of the need to provide more effective protection of personal data] *is the right to require that personal data are deleted or transferred to another provider – often referred to as the 'right to be forgotten' or the 'right to data portability' – which might be particularly useful in the context of social networks or other online services*."[52]. So the data portability and the right to be forgotten would be a corner pillar of the new European approach. Peter Hustinx believes that the right to be forgotten would ensure that the information automatically disappears after a certain period of time, even if the data subject does not take action or is not even aware the data was ever stored. In other words, the data would be attributed some sort of expiration date[53]. The subject of the right to be forgotten

[52] Peter Hustinx, "Towards more effective Data Protection in the Information Society", *datospersonales.org, Digital review published by the Data Protection Authority of Madrid*, 50th issue, April 2011, <http://bit.ly/fmUzzW>.

[53] By contrast, other authors are really skeptics about this possibility: "The new concept of introducing expiration dates for digital information is a challenging approach. Nevertheless, certain weaknesses cannot be overlooked: The ubiquity of social networking nowadays is so extensive that the introduction of

appears as one of the most important challenges for data protection in twenty-first century.

For this reason, the European Commission has recently put its eyes also on the subject of the right to be forgotten. More specifically, in a Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions titled "A comprehensive approach on personal data protection in the European Union", it is said that:

> "*Underlines, furthermore, the importance of improving means of exercising the rights of access, rectification, erasure and blocking of data, and of clarifying the 'right to be forgotten'* [which in the same text is defined 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.*"[54].

Thus arises the need to clarify the so-called right to be forgotten, proposing a definition that bases its existence both on data quality and limitation collection principles, and emphasizing the right to cancel, withdraw or delete personal information when it has been released or processed without consent. The Council of the European Union praised the effort to revise the rules on data protection, specifically encouraging the European Commission to define and explore the introduction of the right to be forgotten as a pioneer legal instrument. To be precise the Council of the European Union "*encourages the Commission to explore the introduction of a right to be*

'expiration dates' requiring somebody (who?) to delete the information is difficult to apply in practice. Furthermore, the proposal of 'expiration dates' also seems to be inadequate and deficient in and of itself since the approach focuses on self-censorship or a lack thereof, contradicting the human desire to chronicle life (to the smallest and most trivial detail) and to immortalize previously fleeting memories". Rolf H. Weber, "The Right to Be Forgotten: More Than a Pandora's Box?", *Journal of Intellectual Property, Information Technology and E-Commerce Law* vol. 2, 2011, at p. 127, <http://www.jipitec.eu/issues/jipitec-2-2-2011/3084>.

[54] European Commission COM (2010) 609 final, "A comprehensive approach on personal data protection in the European Union", Brussels, 2010, <http://bit.ly/bXUXvi>.

forgotten, as an innovative legal instrument, insofar as the exercise of such a right is enabled by new technologies"[55].

The European Commission started a public consultation to obtain different points of view on the Commission's ideas — as highlighted in the Communication a comprehensive approach on personal data protection in the European Union — on how to address the new challenges for personal data protection (e.g. clarify the right to be forgotten) in order to ensure an effective and comprehensive protection to individual's personal data within the EU. The period of consultation was from 4th November, 2010, to 15th January, 2011.

It is particularly interesting to note some of these contributions. The AEPD in its contribution[56] to the European Commission's consultation defended the existence of the right to be forgotten in some provisions of Directive 95/64/EC, to be precise on data quality and collection limitation principles — arts. 7.a) and 6.1.c) —, and was in favor of recognizing both the right of deletion, blocking or correcting inaccurate data that Internet contains and the right to object against unauthorized search engines treatment of personal data.

In a less ambitious vein, we find the contribution of the German Federal Government, which proposes that it distinguishes clearly between the terms 'Right to be forgotten' and 'Right of deletion' by suggesting that the first has a wider content than the second. For this reason, the German Federal Government propose that the new European Directive should specify clearly the relevant requirements to exercise the right to be forgotten, and it would have to be lay down against whom the right may be enforced. Thus, in his opinion the exceptions to the right to be forgotten should have to be defined in the new framework to European data protection policies. Moreover, the

[55] Council conclusions on the Communication from the Commission to the European Parliament and the Council – A comprehensive approach on personal data protection in the European Union, adopted on 3071st Justice and Home Affairs Council meeting, Brussels, 24th and 25th February, 2011, <http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf>.

[56] Contribution of the AEPD to the European Commission's consultation on the comprehensive approach to personal data protection in the European Union, Madrid, 2011, <http://bit.ly/dXeR4m>.

German Federal Government has been "*very interested in the idea of an 'expiry date for data' but again technical implementation seems to be a great challenge*"[57].

In a similar vein, the Belgian Data Protection Authority consider that the new data protection framework must seek a balance between the limitation of storage terms, the right to be forgotten and the need for storage of essential historical and cultural information. More specifically, historical and cultural data are protected under freedom of information and for this reason must be transferred to archives dedicated to historical research and "*should be encouraged and treated as a valid way to retain data beyond their operational utility date*"[58].

On the other hand, as we could expect, skepticism about recognition of the right to be forgotten comes mainly from contributions made in United Kingdom. It is not surprising considering that United Kingdom is a country which follows the common law legal system. As we have seen up to now, in these countries there are few reasons to recognize the right to be forgotten, especially if we consider the extend of open court principle which also means public and full access to court records and criminal databases. The regulation of these matters is so far from countries such as Spain, which respond to civilian law legal system. In the United Kingdom the Information Commissioner's Office (hereinafter ICO) gives independent advice and guidance about data protection and freedom of information. In particular, as regards the right to be forgotten the ICO stated that:

> "*Consent is of particular relevance when we consider the 'right to be forgotten'. It is important that the Commission is clear about the extent to which this right can be effective in practice, as it could have a very limited application* [...] *The ICUK can see some situations where the 'right to be forgotten' could work*

[57] Contribution of the German Federal Government to the European Commission's consultation on the comprehensive approach to personal data protection in the European Union, Berlin, 5th January, 2011, <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/bundesregierung_en.pdf>.

[58] Contribution of the Belgian Data Protection Authority to the European Commission's consultation on the comprehensive approach to personal data protection in the European Union, Brussels, 2011, <http://bit.ly/pINtNI>.

> *well in practice, such as where an individual wishes to delete their record from a social network, but these situations are limited* [...] *It could also be technologically difficult for this right to be delivered in practice in some circumstances, such as when the information has been made publicly available on the Internet. The ICUK therefore welcomes the Commission's proposal to clarify the 'right to be forgotten'.*"[59].

In conclusion, as we have seen throughout this section, it seems that finally the European Commission will include the so-called right to be forgotten in the reforms of the framework of the European Directive on data protection. The contributions of vast majority of data protection agencies shows that they are in favor of recognizing and clarifying the right to be forgotten, nonetheless, they notice that European Law should specify clearly the relevant requirements and the limits to exercise this 'new' right as well as clarify against whom it may be enforced.

VI. Conclusions

A) One of the most important challenges that Internet and 2.0 web involves in regard to reputation, privacy and data protection is the unlimited digital memory. Internet records everything and forgets nothing[60], this is the paradigm of the 'new' age of total recall. The huge storage capacity mixed with the fact that it is very easy to find information through search engines sets out unresolved issues for private life. Especially, because on Internet every statement has a potentially global audience and this makes it much harder for victims of gossip, defamation or unauthorized disclosure of personal data to be socially rehabilitated. This new problem forces us to reconsider

[59] Contribution of the Belgian Data Protection Authority to the European Commission's consultation on the comprehensive approach to personal data protection in the European Union, Brussels, 2011, <http://bit.ly/pINtNI>.

[60] See also on this topic Jeffrey Rosen, "The web means the end of forgetting", published in *The New York Times* on July 21st, 2010, <http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html>. Jeffrey Rosen is a law professor at George Washington University.

how the law can implement and guarantee the idea of a second or third chance into our digital spaces as well as in our real life.

B) We have distinguished different fields where the right to be forgotten could be applied. In the field of the social networks the individuals have the right to delete their personal data if it was published without their consent. Moreover, in Europe, the individuals have the right to revoke their consent and thus having the opportunity to demand the person in charge of social networks to delete their personal data, even when his data was published by the data owner. In the fields of government official journals or media digital libraries this topic arises in a manner much different. The personal data contained in these documents is public; nonetheless the right to be forgotten also could mean the right to object the treatment that search engines give of this information.

C) The topic of the right to be forgotten is not new. There has been for a long time a discussion about the differences in meaning and extension of the open courts principle in Continental Europe, United States, Canada and Australia, especially regarding the right to public access to court records. In this context, in Europe they started many years ago using the terms 'the right to oblivion' with regard to the opportunity of the individuals to block the negative effects of the disclosure of a court or criminal records which should no longer be remembered due to the length of time elapsed since its occurrence. By contrast, we used the terms 'the right to be forgotten' with reference to the rights to cancel and object personal data against unauthorized processing's of personal data, even when this data is contained in public documents like government official journals or media digital libraries.

D) So far the recognition of the right to be forgotten has been a role played chiefly by the European data protection Agencies. The CNIL was a pioneer in recognizing in France the right to be forgotten in accordance with data protection principles. In a same vein, the Italian Garante has recognized the right to be forgotten involving the right to cancel personal data when no longer useful to the purpose for which it was processed. On the other hand, last but not least, the AEPD has extended

and defined a wide right to be forgotten which means the right to cancel, react and correct unlawful inclusion of personal data on the Internet. This new right also includes the right of individuals, who neither has the status of a public personality nor is the subject of a news event of public relevance, to object search engines which linked personal data that belong to the public sphere as government official journals. Google faced off against AEPD decisions by claiming the Spanish National Court that only publishers, and not search engines, may be deemed responsible for contents published through their websites. Currently, the *Audiencia Nacional* is studying the case.

E) Plans to reform the current European Directive on data protection rules to include the right to be forgotten into a new framework, as we have seen up to now in the European Commission's Communication on the comprehensive approach to personal data protection in the European Union. Peter Hustinx, European Data Protection Supervisor, considers this new right an example of the need to provide individuals more effective protection of their personal data. The contributions of the vast majority of European data protection agencies to the European Comission's consultation show that they are in favor of recognizing and clarifying the right to be forgotten. Nevertheless, they observe this issue as a great challenge because of the difficulties attached to the technical implementation of an expiry date for data and the inherent characteristics of digital memory. Furthermore, they want that the new European Directive specifies clearly the relevant requirements and the limits to exercise this 'new' right as well as clarify against whom it may be enforced.