Lilian Mitrou, Associate Professor - University of the Aegean/Athens University of Economics and Business
Maria Karyda, Assistant Professor - University of the Aegean

EU´s Data Protection Reform and the right to be forgotten - A legal response to a technological challenge?

Abstract

Technological and social phenomena like cloud computing, behavioural advertising, online social networks as well as globalisation (of data flows) have profoundly transformed the way in which personal data are processed and used. This paper discusses the efficiency of the legislation in force and the impact of PETs and the concept of privacy by design on the enforcement of data protection rules. By recognizing the need to update the data protection regulation as a result of current technological trends that threaten to erode core principles of data protection, the paper addresses the question if the Draft- Regulation presents an adequate and efficient response to the challenges that technological changes pose to regulators. In this context the paper focuses on the right to be forgotten as a comprehensive set of existing and new rules to better cope with privacy risks online in the age of "perfect remembering" and we how persistency and high availability of information limit the right of individuals to be forgotten . The paper deals with both the normative and the technical instruments and requirements so as to ensure that personal information will not be permanently retained.

1. Introduction

Since the adoption of the European Data Protection Directive in 1995 we have experienced dramatic technological changes. We could describe this new situation as a "Data Deluge"[1] strictly related to and combined with accessibility, durability and comprehensiveness of digital information[2]. Advances in search algorithms[3],

[1] See Blanchette p. 25 f.. The European Data Protection Supervisor (EDPS) is also referring to "data deluge" [EDPS 2010].

[2] At the same time the EU Council "Future Group", looked forward to a "digital tsunami" of personal data, with the Council Presidency stating that "every object the individual uses, every transaction they make and almost everywhere they go will create a detailed digital record. This will generate a wealth of information for public security organisations, and create huge opportunities for more effective and productive public security efforts". See Portuguese Presidency, Public Security, Privacy and Technology in Europe: Moving Forward - Concept Paper on the European strategy to transform Public security organizations in a Connected World. - Available at: http://www.statewatch.org/news/2008/jul/eu-futures-dec-sec-privacy-2007.pdf

exponentially increasing storage capacity in combination with decreasing costs, information seeking behaviour, content creation and management practices threaten to erode what we understand as societal forgetting. Personal information may be copied, tagged, reposted and stored virtually forever. Persistency and wide availability of information threaten to infringe core principles of data protection, such as the purpose limitation and proportionality principles, as well as fundamental rights of individuals, like the right to oblivion.

Technological, social and economic phenomena like cloud computing, online social networks, intensive (if not aggressive) behavioural online advertising as well as globalisation (of data flows) have profoundly transformed the way in which personal data are processed and used and maximized problems and risks we have to face and deal with. The European data protection framework required at least "some maintenance", if only because of the fact that it was conceived and adopted before the explosion of the Internet and the impacts of the explosion on economy, society and every-day life.

This paper addresses the question if the Draft-Regulation presents an adequate and efficient response to the challenges that technological changes pose to regulators. We discuss the efficiency of the legislation in force and the impact of PETs and the concept of privacy by design on the enforcement of data protection rules. In this context we focus on the "*right to be forgotten*" as a comprehensive set of existing and new rules to better cope with privacy risks online in the *age of "perfect remembering*". This new right seems to be one of the main pillars of the new European regulatory approach [Castelano 2012, EDPS 2011a] while condemned by some authors as a new instrument of censorship [Rosen 2012].

We discuss the normative as well as the technological perspective of this right. We try to point out the technical prerequisites and/or requirements to achieve the goal of providing individuals with the right to make information about them less accessible after a period of time and enjoy forgetfulness and a right to re-start. We discuss different methods for implementing the right of individuals to delete personal information about them that are held by others: in particular we suggest that a multifaceted approach, including legal regulations and technical controls is essential.

2. Data Protection Law: Need to change?

The EU's Data Protection Directive, adopted 17 years ago, has indeed been a milestone in the history of personal data protection with worldwide impact and influence[4]. The Directive can be credited with creating one of the world's leading

[3] The so called "Semantic Web" (or WEB 3.0), while enabling the sharing of information and personalization of searches improves furthermore the functionality and usability of search engines and increases profiling and monitoring of users (Giannakaki 2011).

[4] Both with the intensification of transborder data flows, the adoption of the Data Protection Directive forced to start an international debate about adequacy of protection and it

paradigms for privacy protection [Robinson et al. 2008]. However, despite the substantially positive track record and general acceptance of the Data Protection Directive, certain aspects have been criticised and its efficiency (has been) contested.

Criticisms from within the EU have often focused on the – "useless" or "burdensome" - formalities imposed by the Directive, on vague definitions and unclear rules, on cumbersome and outmoded rules and tools concerning data transfer to third countries. Even if the Directive has successed in accomplishing a certain degree of regulatory harmonization in member states, its enforcement has been diversified and inconsistent[5]. Moreover, the debate about the legal nature of IP addresses, the notion of data and consent, the applicability of EU law to online social networks and search engines signalized the need to ensure at least more clarity [DPWP 2009 a].

Principles like necessity, proportionality, data minimisation, purpose limitation and transparency have been around for 25 or 30 years and have been confirmed – even not always properly enforced - over and over again [DPWP 2009a]. They have proved their usefulness and adequacy [Mitrou 2010]. However, many argued that the Data Protection Directive required at least "some maintenance", if only because of the fact that it was conceived and adopted before the explosion of the Internet and the impacts of this explosion on economy, society and every-day life" [EDPS 2011a]. The convergence of the network around a single interoperable platform, changes in identification and authentication techniques, identity management and profiling, social networks, cloud computing, behavioural advertising, RFIDs, geo-location devices and applications have profoundly changed the way and the extent in which data are processed and posed crucial challenges for data protection.

Such technological challenges as well challenges resulting from social and political changes and choices[6] threaten to make the application of data protection rules at least more difficult. New technologies interwoven with the globalisation of processing pose

---

accelerated the adoption of respective legislation in other countries and world areas. For an updated overview of the legislative developments and current situation all over the world see Gürtler (2012) p. 126 ff.

[5] Differences in the way that each EU country implements the law have led to an uneven level of protection for personal data, depending on where an individual lives or buys goods and services. The judgment of the European Court of Justice on case C-518/07 (Commission v. Germany) has for example proved that there were and still are different approaches concerning the independence of the Data Protection Authorities.

[6] In the wake of each terrorist attack in Europe during the last decade, earlier legislative proposals, which had no chance to be accepted, were re-introduced, and new policies with similar objectives were drafted to extend state surveillance authority. Ubiquitous data availability, widespread and often excessive information sharing and surveillance often via automated means that are inclined not only to errors but also to discriminatory effects marked this new security environment. After 9/11 many reference criteria changed and the guarantees were reduced everywhere in the world, as shown particularly by the Patriot Act in the USA and the European decisions on transfer of airline passenger data, the so-called PNR data to the US as well as on the retention of electronic communications data.

new risks for personal autonomy[7] and increase the imbalance of power between the data subject and data controllers. The present array of norms fails to shield users from risks and harms not easily remedied on an Internet of infinite memory. In this "brave new data world" a robust, future-proof set of rules is required, in order to ensure that individuals will enjoy (and retain) effective control over their personal information.

3. From PETs to Privacy by Design ?

3.1 PETs and their limited efficiency

Information and communication technologies (ICTs) offer a wide range of tools and mechanisms to protect personal data: Privacy Enhancing Technologies (or PETs) have no universally agreed definition, but it is generally accepted that these technologies aim to reduce the risk of contravening privacy principles and legislation, they aim to minimize the amount of personal data being held by other parties, and/or provide individuals with control over their personal information that is being held. The European Commission defines PETs as "*a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system*"[8].

Most PETs are composite technologies that employ security measures such as encryption and access control mechanisms in conjunction with other mechanisms to enhance overall privacy. Their development and application is based on the basic principles for the protection of personal data and they entail various technologies at different levels of maturity and with varying effectiveness. PETs allow individuals control what personal information is processed, how it is processed and by whom (e.g. privacy audits, data minimization tools and log files). They can also provide users with the ability to hide their true identity (e.g. tools that offer anonymous or pseudonymous access to online services). Other PETs include encryption tools, filters and blockers, digital track erasers, consent mechanisms, data minimization tools, the Platform for Privacy Management (P3P[9]), privacy seals, digital identity management tools, privacy policies, access control schemes and technologies for privacy protection for RFID systems. There is a usual misconception between security and privacy technologies. Despite the fact that many information security technologies are also applied for providing privacy (e.g. encryption tools, access control schemes) not all security measures are PETs. Moreover, several security controls (e.g. monitoring tools) have privacy invasive applications.

[7] Increased automated analyses of easily-accessible data, data mining and excessive profiling bear the risk of individuals becoming mere objects, treated (and even discriminated against) on the basis of "profiles", probabilities and predictions.

[8] COM(2007) 228 final.

[9] http://www.w3.org/P3P/

The core principles for the protection of personal data, namely transparency, proportionality and data minimization, as described in the European Union Data Protection Directive of 1995 have, at a large extent, formed the basis for the development and implementation of PETs. Evidence shows[10] that PETs implementing data minimization are more often used than those implementing user consent, whose importance appears to be limited. However, the wide diversity and varying technical characteristics of PETs raise barriers to widespread adoption. Often PETs are application specific, while some are designed to be used in specific applications while others may be applied in different systems. Their deployment depends also on the underlying legal and regulatory framework, on users' privacy awareness and their privacy concerns, as well as on the cost and benefits associated with their use. It should also be noted that often the actual implementation of the PETs is quite simple; However, the complexity of the term makes it difficult for many stakeholders, individuals as well as data controllers to apprehend their usefulness and therefore employ them.

Despite the fact that privacy enhancing technologies have been in use for several years now (D. Shaum's "Mix-networks"[11] is considered the first PET as it enables anonymous communication over a network) it is generally acknowledged that the risks associated with the use of personal data in electronic form are serious and growing, while, at the same time, both overall adoption rates and consumer awareness of PETs are low. PETs' low adoption rate can be attributed to the fact that have not yet reached a maturity level while new PETs are constantly developed[12] . Also, users' privacy awareness remains limited, while usability issues need to be addressed as several PETs require previous experience and/or knowledge with ICTs and many lack a user-friendly interface. Other findings suggest that PETs are still under-developed, that they remain rather weak in terms of implementation and effectiveness and that they are often applied in ineffective ways. It should be noted, finally, that their success in providing for the protection of personal data is constantly limited by technological advances in privacy-invasive technologies, such as more powerful data mining tools and pervasive electronic devices equipped with sensors and biometric identifiers.

[10] European Commission, Directorate-General Justice, Freedom and Security, Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of New Technological Developments, Final Report, Contract No: JLS/2008/C4/011 – 30-CE-0219363/00-28, 20-01-2010.

[11] David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM, 24(2):84–90, 1981.

[12] European Commission, Directorate-General Justice, Freedom and Security, Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of New Technological Developments, Final Report, Contract No: JLS/2008/C4/011 – 30-CE-0219363/00-28, 20-01-2010.

3.2. Privacy by Design – Privacy by Default

As emphasized also in the Digital Agenda 2010, the future of privacy cannot be assured solely by ex-post compliance with regulatory frameworks and ″ticking off″ compliance boxes. In discussions about the new regulatory framework in Europe several new tools, concepts and principles that have been less formally embedded in privacy legislation are now central objectives and tools. Such a critical principle is the so-called "privacy by design".

When initially introduced, in 1995, the term privacy enhancing technology referred mainly to applications that would be 'bolted on' to privacy invasive systems. Recently, however, data protection has been more holistically approached and emphasis is placed on the effort to address privacy concerns in all stages of systems development. The need to offer comprehensive solutions to privacy issues, not just technological add-ons, is emphasized by scholars as well as by regulatory bodies and organisations promoting data privacy. Privacy by Design is a principle for systems engineering which requires that respect for individuals' privacy and protection of their personal data are taken into consideration at all stages of systems lifecycle, namely from early inception and initiation, to development and implementation and finally to operations, maintenance and disposition.

Applying the Privacy by Design principle at all stages of systems development entails including privacy enhancing technologies, devices and tools that can protect data privacy. According to the European Commission, *"the use of PETs can help to design information and communication systems and services in a way that minimises the collection and use of personal data and facilitates compliance with data protection rules. The use of PETs should result in making breaches of certain data protection rules more difficult and / or helping to detect them*"[13].

In order to embed privacy enhancing mechanisms into information processing systems, it is essential to elicit and assess privacy requirements at all stages of information systems' lifecycle. For instance, one should take into consideration the applicable privacy laws and regulations, such as the EU Data Protection Directive or the US Safe Harbour agreement as early as the project initiation stage, when a general idea of what the ICT project will entail and what information assets will be involved. Available technological solutions should also be evaluated to ensure that appropriate privacy controls can be implemented and which will be their cost and effectiveness. As detailed planning proceeds, privacy requirements can be made more concrete and specific privacy enhancing technologies can be selected, such as encryption tools and access control schemes.

During the development phase, it is important that attention is paid to the correct implementation of all privacy protecting mechanisms and it is also essential to

[13] European Union. Press release: Privacy enhancing technologies (PETs). http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/159&format=HTML&aged=0&language=EN&guiLanguage=en.%20Reference:%20MEMO/07/159 (last accessed on June 2012).

examine whether implementation and application context issues raise further privacy requirements that may have not been considered at earlier stages. At the deployment stage one may consider applying audits and change control procedures to ensure that privacy protection meets the requirements. Finally, one should not neglect that even after their use has stopped, ICTs can still raise privacy issues, such as the disposition of storage means containing personal information.

However, there are still several issues that need to be clarified, as this new concept has started to gain acceptance among researchers, practitioners and decisional bodies: for instance the methodological approach that will enable its seamless integration into technological artifacts, the evaluation of its cost and effectiveness as well as its impacts and implications for individuals, systems and organizations are open to discussion.

4. From Here to Eternity and the Right to be forgotten

Technological developments in general and the tremendous growth of their use in all human activities have shown the necessity to enrich the fundamental data protection principles with specific rights. The consent of the data subject[14] remains a cornerstone of the European data protection structure and architecture, but – apparently - it has to be adapted to the requirements of the online environment, without however being reduced to a "just click submit" automatism. Of crucial importance for preserving the individuals' rights especially in Web seems to be the introduction of an expressis verbis "right to be forgotten" in the information era of "no oblivion".

Over the last years this right[15] has raised increasing attention and concern[16]. The scientific and public discussion reflects that people and decision-makers[17] have

[14] See DPWP Opinion 15/2011 on the definition of consent.

[15] This right seems to have its origin in French law, which provides a "right to oblivion" (le droit à l'oubli) and Italian Law (diritto al'oblio) that conceived mainly and primarily as the right of a convicted criminal who has served her sentence not to be confronted with information concerning her criminal and object to this publication. The right to oblivion is tied to privacy and the ability to escape the past and consequently the possibility of being reintegrate into society "free from having past criminality taint [her] reputation" (See Walker, p. 27).

[16] The term "right to be forgotten" has been created quite recently. However the - similar but not identical - "right to forget," which refers to the already intensively reflected situation that a historical event should no longer be revitalized due to the length of time elapsed since its occurrence (Weber 2011) has a longer history as it was already more than a decade ago an issue of scientific and public discussion. Another definition of the right to forget is the right not to be accountable for one's conduct after a certain amount of time and beyond a given framework of relationships (Pizzetti 2009).

realized the "disappearance of forgetfulness"[18] and the impacts thereof. Under this term we understand "the claim of an individual to have certain data deleted so that third persons can no longer trace them", in other words or more correctly from another perspective, we could define this right as the "right not to see one's past coming back forever" [Pizzetti 2009] or "the right to silence on past events in life that are no longer occurring" [Pino 2000].

Human memory processes allow forgetting "by design" [Eltis 2011, Blanchette 2011]. Technology, however, is changing this paradigm. Persistence, replicability and searchability belong to the built-in features of online digital data and allow its endless persistence and accessibility [Lindsay 2012]. Furthermore, the cost of data storage has been falling rapidly for many years (from less than 10$ per gigabyte in 2000 to less than 10 cents per gigabyte in 2010), the processing speed of digital electronic device has doubled approximately every 18 months (this phenomenon is described as Moore's law) and recent advances in broadband Internet and wireless access allow low-cost access to any wireless enabled device. The ubiquity of data collection practices, advances in search methods, content creation and decreasing costs of technological products allow perpetual storage, dissemination and multiple use of information and threaten to erode what we understand as social forgetting [Ambrose et al. 2011].

Information lasts longer than the context, in which its initial collection and processing was - often but not always- legitimate, and consequently it is available for analysis and use "in totally different interpretative contexts"[19]. Moreover, information stored and accessed on the Web consists of fragments of people's lives that may be out of context, at random, incomplete or wrong [Solove 2007]. Even if information is removed from or corrected on the source websites, Internet archives, cache copies and various abstracts produced by search engines may still provide an inaccurate and distorted status/picture of the person[20]. The role of search engines in remembering and vitiating forgetfulness and forgiveness is crucial. They enable bringing to the surface the slightest piece of information, gathering all the pieces and offering various recomposed or hererogeneous portraits of a person [De Tetwagne 2012]. Through the

---

17 As underlined by V. Reding, EU Commissioner for Justice, Fundamental Rights and Citizenship, "The God forgives and forgets, the Web never does". V Reding, Privacy matters – Why the EU needs new personal data protection rules, Speech held on The European Data Protection and Privacy Conference, Brussels, 30 November 2010. Accessible at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/700 .

[18] Through the "disappearance of forgetfulness" the "disappearance of disappearance" (Levi, M. and Wall D.S, 2004) becomes perpetual.

[19] See Marx (1986), p. 150.

[20] In Greece a person, accused and acquitted of all charges, sued a newspaper claiming to remove the respective information from its website. The newspaper proved that it had no more the technical possibility to remove the inaccurate content, because it was actually saved on a mirror page. In January 2006, the Italian Garante Privacy has called upon Google to find out solutions to remove obsolete or inaccurate personal information after such information has been amended at the source websites. See Liguori and De Santis, The Right to be Forgotten: Privacy and online News (18/3/2011), available at www.portolano.it

– complicate, enigmatic and not transparent search algorithms - a sensational information, widely disseminated and reproduced in the past, appears among the top results of a search, despite the time passed[21].

Weblogs, social networking and social bookmarking that depend on participatory information sharing, result into the creation of records of all digital activity a person may have. These records containing personal information, which are permanent in essence as old records are practically never erased, can have consequences for individuals long after the event they record (a 'tweet' or a 'status update') has been forgotten by their actors. The default of forgetting has changed into a default of remembering. Forgetting seems to go against the "natural economic trend" as it has become less expensive to store data than to destroy or anonymise them [De Tetwagne 2012].

The issue of maintenance and forgetfulness seems to be cast, either implicitly or explicitly, as one referring to the tension (and balance) of informational privacy and other rights and interests, public or private. However, the asymmetry of power of individual on the one side and the institutions/organisations that collect information is manifest. In the expanding and borderless information world and/ or market, individuals develop inevitably into a permanent and inexhaustible source of information. Moreover, this asymmetry refers not only to the storage of information by "big controllers" such as public authorities, search engines, online social network and/or application providers, advertising networks. Users in WEB 2.0 environment are playing, at least potentially, a "central role in the collection, processing and distribution" of personal data [Wong & Savirimuthu 2008]. They generate content on themselves and others[22]. Especially with reference to social networking, individuals are at the same time users and data controllers[23] . The new ICTs and their potential serve not only the so-called institutionall memory of the State but, moreover, extend the persistence of social memory, enabling the creation of a panoptic society [Blanchette and Johnson 2003].

Perfect and precise remembering affects the claim of individuals to live and act without leaving permanent traces or shadows[24] and in this perspective interferes with a crucial element of information privacy. Information storage ad perpetuum affects a right that is at the very centre of the informational privacy: the right to informational self-determination, the right to control the use of her own information[25]. Due to the

[21] As noted by Lindsay (p. 422), the operation of search engine algorithms, such as Google's PageRank, often results in the most embarrassing or humiliating information about a person dominating search returns.

[22] In this capacity as "data controllers" users may become infringers of the rights and freedoms of other persons that are not necessarily users.

[23] See Wong, Social Networking : Anybody is a data controller (2008).

[24] Digital traces or digital footprints is data created by users themselves and data shadows, is data generated about users by others. See Koops (2011), p. 230 ff.

[25] This right consists in the right of the person to determine in principle the collection,

persistency of information and the absence of forgetting individuals are steadily confronted with their past[26]. They cannot escape it or re-create their present and/or future[27]. Andrade emphasizes the relationship of the right to be forgotten and the identity perspective by arguing that the right to oblivion serves not only to be hidden from society but also as an instrument through which individuals correct and re-project their images to society [Andrade 2011].

As everyone depends upon others and their perceptions to engage in social or professional transactions, long-lasting or perpetual information that brands a person, affects – often irrevocably - relationships, social status, current and future employment that person. A lost or damaged reputation may have serious impact on the ability of a person to engage in communicative processes and – in the final analysis - in society. Persons are not only deprived from the opportunity of a new start: Accessibility and durability of information may lead to self-censorship and (digital but not only) abstinence from activities[28]: if every act or opinion expressed can be easily recorded and recalled, persons may hesitate to act and to participate in social and public life, which in turn affects the development of democratic citizens [Blanchette and Jonhson 2003].

5. The Normative Perspective

5.1. The right to be forgotten in the Draft Data Protection Regulation: a new right ?

disclosure and use of her own information. In the current European regulatory framework this right is concretized also through the consent to processing as well as the rights to access and deletion/erasure.

[26] Walker underlines that all personally identifiable information is of equal ontological weight (i.e., all information in a digital system is reducible to a series of 1s and Os) regardless of the data's relative significance to a person's life: past foibles are just as searchable as present success (Walker 2012).

[27] By undermining identity and eroding autonomy, "digital traces therefore have the potential to act as a virtual prison, to keep us tethered to expressions of ourselves that are outdated, incomplete or inaccurate" (Lindsay, p. 422).

[28] Mayer-Schönberger (2009) and Solove (2007) are referring to the assumption that these qualities of digitized information (comprehensiveness, durability, ubiquity, accessibility) may lead individuals to self-censorship. The German Constitutional Court in the famous Census Decision (1983) underlined that "… (w)hoever is unsure if their dissenting behaviour may be recorded at any time and, as information, permanently saved, will try to avoid attracting attention through such behaviour. This would impair not only the personal development chances of individuals, but also the public good, as self-determination is a prerequisite for a free democratic polity based on its citizens' capacities of civic action and collaboration" BVerfGE 65, 1 (Volkszählungsurteil/Population Census Case, para. 44).

As already emphasized, perfect and perpetual reminding and remembering undermine a crucial virtue of informational privacy, i.e. the right of a person to control and determine principally the dissemination and use of information concerning her. A right to be forgotten relates strictly to the autonomy of the person becoming the "rightholder in respect of personal information on a time scale"[29]. It is highly questionable if current law is sufficient to deal with the protection of this right in the digital environment. (Re)ensuring forgetfulness in a context of outstanding digitization, proliferation and "by default" storage of personal information seems to be, primarily, a matter of regulatory and - in the end - political choice[30], i.e. seeking for a normative tool, capable of forcing data controllers to respect and to realize in practice a right to be forgotten.

The right to be forgotten seems to form a key component of the EU regulatory reform process : it is explicitly enshrined in the recently (Januar 2012) proposed Data Protection Regulation (Art. 17)[31]. The features of the proposed right encompass the obligation to erase or abstain from further dissemination of data if: a) they are no longer necessary in relation to the purposes for which they were collected or otherwise processed, b) their processing does not comply with the data protection framework[32], c) the data subject withdraws her consent or objects to the processing. Prima facie these proposals are complementary to the principles already included in the Data Protection Directive [Koops 2011]: Data Controllers are also under current law obliged to delete information as soon as it is no longer necessary for the purpose of the processing and the data subject has the right to object to the further processing of her personal data[33]. It is noteworthy that the Council of Europe does not provide for an explicit inclusion of a "right to oblivion" to the Proposal for Modernisation of

[29] See Weber, who also argues that the longer the origin of the information goes back, the more likely personal interests prevail over public interests (p. 121).

[30] Blanchette and Johnson describe this choice as an issue of social policy, on which society has to choose between the "forgive and- forget" and "preserve but evaluate" theories of recordkeeping in each substantive area (p. 35).

[31] Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final (25.01.2012).

[32] The fundamental principles of data protection (proportionality/data minimization) require that data should be kept 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. (Art. 6 § 1 e of the Directive).

[33] The right of the data subject to object on compelling legitimate grounds relating to his particular situation to the processing (Art. 14 of the Directive). The right of data subject to obtain from the controller the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data (Art. 12 b of the Directive). Xanthoulis (2012) is of the opinion that from the relevant EC Communication "the right [of individuals] to have their data deleted if they withdraw their consent and if there are no other legitimate grounds for retaining the data" results that the right to be forgotten is tautologous with the right to erasure(…).

Convention 108[34]. According to the Consultative Committee it would be difficult to reconcile this right with freedom of expression (Art. 10 of ECHR). Moreover the Consultative Committee considers such a provision as unnecessary, as "It was felt that the existing safeguards (notably article 5.e – length of time of data storage, and article 8.c –right of rectification or erasure of data) coupled with an effective right of opposition would offer adequate protection.

The Draft Regulation creates two separate rights: a right to rectification (Art. 16) and a right to be forgotten (Art. 17): the current draft proposal goes further than the Data Protection Directive in force by requiring data controllers and/or website operators to "carry out erasure without delay," unless the retention of data is "necessary" for exercising "the right of freedom of expression", as defined by the national law[35]. According to the purpose of the proposed provision individuals should give no effort or insistence to have their data deleted, as erasure should take place in an automated way. In this sense the proposed Regulation includes also a reversion of proof concerning the erasure of data[36].

In case that deletion is requested, a website operator must take "all reasonable steps" including technical measures to inform third parties, which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. More specifically, where the controller has authorised a third party publication of personal data, he shall be considered, according to the provision, as responsible for that publication This provision goes obviously beyond the current obligations of data controllers, even if both the meaning of "reasonable technical steps" and "authorising publication" are uncertain and vague. This obligation is, moreover, limited to "what is technically feasible and does not require a disproportionate effort". This provision should be considered in combination with Art 13 of the Proposal according to which "the controller shall communicate any rectification or erasure carried out in accordance with Articles 16 (Rectification) and 17 (Right to be forgotten) to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort".

The European Data Protection Supervisor considers the "obligation of endeavour" upon the controller as more realistic from a practical point of view than an obligation of result"[EDPS 2012]. Failure to comply with the Regulation could result in fines up to one million Euros or two percent of the operator's annual worldwide income. Moreover, the data controller carries the responsibility for third party publications that the controller has authorised. The "right to be forgotten" seems to be basically not

[34] Council of Europe- The Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data [Ets no. 108] (T-PD) Modernisation of Convention 108: New proposals - Strasbourg, 27 April 2012.

[35] The Draft General Data Protection Regulation provides an exemption for, "the processing of data solely for journalistic purposes, or for the purposes of artistic or literary expression" (Art 17 § 3).

[36] EDPS, Opinion of 14 January 2011 on the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union, para. 89.

only a re-affirmation but also a strengthening of already existing obligations and rights[37].

However, unclear remains how and the "extent to which the right to be forgotten may be enforceable in practice" [EDPS 2012 para. 141]. Furthermore a major issue concerns the scope of this right: Against whom can this right be exercised. Difficulties arise not only in relation to user generated content and in general in Web 2.0 situations where the user may invoke the so-called "household exception"[38]. If this exception does not apply, we are facing the problem of defining the responsible data controller as both the user (uploader) and the SNS are regarded as data controllers [DPWP 2009b] Another major issue relates to the implementation of the right to third parties responsible for copies in caches or mirror websites. Indeed, in some cases it may be a huge effort to inform all third parties who may be processing such data, as there will not always be clear understanding of where the data may have been disseminated [EDPS 2012 para 147]. In general it is not at all obvious how should the right to be forgotten deal with ubiquitous and opaque cross-platform data transfers [Ausloos 2012].

5. 2. A new right: a new clash?

The discussion about the substance, the justification and boundaries of a right to be forgotten inevitably reflects and involves the tension between individual privacy, public interest or other individual rights and interests[39]. In the final analysis privacy is a social attribute of a person: privacy is defined in relation to the interaction between the person and the others, the person and the society. Without underestimating the "chilling effect" of perfect remembering on individual behaviour and consequently on democracy some authors underline that remembering is a way to ensure the accountability of persons for the consequences of their actions, which nourishes "the

[37] The EDPS in his recent Opinion on the Data Protection Reform Package (07.03.2012) is referring to "the reinforcement of the scope of current rights (such as the right to erasure, which has been strengthened into a right to be forgotten)" (para. 140).

[38] The Data Protection Directive does not impose the duties of a data controller on an individual who processes personal data "in the course of a purely personal or household activity" (the so-called "household exemption" established in Art 3 § 2). However, the activities of a user of an SNS may not be covered by the household exemption. In any case, even if the household exemption applies, a user might be liable according to general provisions of national civil or criminal laws in question (e.g. defamation, liability in tort for violation of personality, penal liability). Andrade (2011) expresses the opinion that the right to be forgotten should override the "household exemption". Lindsay (p. 438) underlines the considerable uncertainties about the application of the household exemption to Web 2.0 applications, as well as the extent to which individuals should be regulated as data controllers and proposes reverting to the earlier draft proposal, which would ensure that it is not available where an individual makes personal data "accessible to an indefinite number of individuals".

[39] Social goods such as law enforcement, government efficiency, national security or constitutionally protected rights such as legitimate economic activities like advertising. Andrade (2011) notes that in fact, the right to be forgotten lives in permanent tension and conflict with other rights, interest, values and objectives.

sense of responsibility that is just as necessary to a democratic society" [Blanchette and Johnson 2003].

On the other side in the WEB 2.0 environment every user re-products and disseminates any "newsworthy" information (such as information about crime and evasions). In WEB 2.0 personalization and contextualization as well as de-contextualization of information is the primary product and goal. Through this potentially endless dissemination and the - complicate, enigmatic and not transparent - search algorithms a sensational information, widely disseminated in the past, appears among the top results of a search, despite the time passed. This reveals the crucial importance and the role of search engines in remembering and vitiating forgetfulness and forgiveness.

Recently, there are several cases of persons suing Wikipedia[40] or Search Engines like Google or Yahoo asking to remove stigmatizing information that affect informational privacy and more specifically the reputation of the claimants. Of major importance are the cases of the Spanish citizens, like the plastic surgeon Russo[41] or the Entrepreneur Masiá[42], who sued Google for removing stigmatizing information[43]. Search engines algorithms and – consequently - results ranking take little consideration of time or

[40] Some years ago (2009), Wikipedia has been sued by two Germans who claimed that the online encyclopaedia's description of their involvement in the murder of a German actor back in 1990 violates their right to privacy. Following a German court's judgment, which reflects the German jurisprudential tradition after the Lebach Urteil of the German Constitutional Court, the claimants had already successfully pressured German publications to remove their names from their online coverage. German editors of Wikipedia had removed their names from the German-language version of the article about the victim, the murdered actor Walter Sedlmayr. By supporting their right to privacy after having "paid their debt to society", their lawyer underlined that "they should be able to go on and be resocialized, and lead a life without being publicly stigmatized" (Report in NY Times on 12/11/09). The U. S. (San Francisco) based company refused to comply with this request for the reason that the First Amendment protects freedom of speech and dissemination of such information.

[41] Hugo Guidotti Russo, a Spanish plastic surgeon, had, over twenty years ago, a widely covered dispute with one of his patients over an allegedly botched breast surgery. Although since then Russo has practiced his profession without any incident, the mere mention of his name on a search engine produces a huge number of results all linked to the supposedly bungled and very gruesome procedure and the respective reports, which overwhelm any and all other relevant and recent information about him. For more information and references see Eltis, p. 85 ff.

[42] Mario Gianni Masiá, the owner of Los Alfaques campground in Spain, had sued Google's Spanish subsidiary in a Spanish local court over search results for the campground that lead to information, photos and a Wikipedia page presenting details on a more than 30-year old disaster in the campground, in which more that 200 people were burned to death. For more information see McNealy (2012), The Emerging Conflict between Newsworthiness and the Right to be Forgotten.

[43] Also outside Europe there are such suits: Lindsay (with reference to Levy) reports the example of Jessica Ewing, a Google search engineer, reportedly once requested the Google search team to alter the first search result for her name, which returned an "embarrassing photograph of her as a 13-year-old mathlete" (p. 421).

other pertinent factors. The deletion of an article from the search engine's results would diminish the capacity of users to find it. Therefore, if an article has been deleted from search engines following a request of an affected person, it would not matter that this article is still in existence in its primary source of publication for the reason that it would be rendered invisible at least to new users.

Google reacted to the order of the Spanish Authority to delete links to any website containing outdated or inaccurate information by claiming in the Audiencia Nacional (Spain's Highest Court) that only publishers, and not search engines, may be deemed responsible for contents published through their websites and on the Internet. The Audiencia requested recently[44] the European Court of Justice to clarify some jurisdictional and however very substantial issues. The Spanish Court also addresses the following issues: if the functions of a search engine fall under the definition "processing of personal data", if the company running the search engine is a "data controller" and if it is the case does the search engine bear the obligation to apply the right to be forgotten upon a data subject's request and remove data from their index without previously or simultaneously requiring this removal from the original source of publication? Is Google (and any other search engine or social network site) obliged to guarantee the rights to delete and to object (as laid down in the Data Protection Directive) and delete or block the information, even if its preservation at the site of origin can be deemed as lawful? The preliminary ruling of the European Court could be a milestone concerning the protection of online personal data and the right to be forgotten in the digital world.

These cases reveal, however, another area of conflict, this of the tension between forgetfulness and free speech. American scholars argue that "enshrining a so-called right to be forgotten …. clashes head-on with cherished legal values in America—foremost, the freedom of expression"[45]. Moreover, some authors regard the new right not as a "modest expansion" of existing data privacy rights but as "the biggest threat to free speech on the Internet in the coming decade" [Rosen 2012]. Free Speech Activists have declared the death of "open Internet". Indeed more than a revival of the (only prima facie!) conflict between informational privacy and freedom of information it seems that we have to face a new "transatlantic clash" between European and American conceptions of the proper balance between privacy and free speech.

In this context a balance should be also struck between the right not to be confronted with the past and the (social and scientific) requirements for preserving collective

[44] The Spanish Data Protection Authority had already ordered Google to delete links to any website containing outdated or inaccurate information. The Spanish Authority regards that the right to be forgotten may lead also to the deletion of public or legitimate information if that information has not a current public relevance.

.

[45] The right to be forgotten is not protected in the US, being clearly overshadowed by the right to inform and the right to free speech. It seems to be a clear preference for the free speech over the privacy interests of individuals. For more details on the clash between Europe and the US concerning the tension between the right to inform and the right to be forgotten, see F. Werro (2009).

memory. The right to be forgotten risks to clash with the (historical) interest of archiving every available information. In this perspective we have to take into account the changes in the perceptions and methods of historical research and collective memory. It seems to be an interdisciplinary interest on recording every-day life[46]. Availability and storage capacity have contributed to the trend to archive every available information for possible future use.

Apparently, the right to be forgotten cannot be synonymous with a right of a total erasure of history. However, on the other side the interests of social and historical inquiry does not legitimize keeping every piece of personal information regardless the rights and interests of the persons affected. Appealing constitutionally embedded freedom of speech should not, however, serve as a pretence or excuse for extensive data collection, retention and use through Online Network Sites and Search Engines producing a "panopticon beyond anything Bentham ever imagined"[47].

6. The technological perspective

Legal instruments are essential, but they are not self implementing and – apparently - they are not sufficient. The enforcement of data protection principles and rules remains a critical point. A further structural problem is the fact that every specific regulatory framework reflects a political and legal compromise under particular circumstances and within a given socio-economical and technological context. Changes in technology, economy and society demand, at least, a review of regulatory policy. Technological measures are needed to reinforce or supplement legal measures, for example through a kind of Privacy "digital privacy rights" that could enforce policies and individual control over the use of data[48]. The conception of the right to be forgotten in the Proposal for a Data Protection Regulation tries to respond to major technological and societal challenges posed in relation to information society services. The usefulness of this right depends however upon its construction and enforcement as a privacy by design /privacy by default[49] requirement for the lawful processing of personal data.

[46] A paradigmatic example of the preservation of a collective memory is cited by Andrade (2012) and refers to an announcement made by the US Library of Congress. The world's largest library has announced that it will digitally archive every public tweet since Twitter's inception, in March 2006.

[47] See Ausloos (2012) with reference to L. Lessig, Code: Version 2.0 (Perseus Books 2006) p. 208.

[48] Blanchette (2011) proposes also the or through providing the "perfect contextualization" that would situate each piece of information within its full historical context (p. 163).

[49] The European Data Protection Supervisor in his Opinion (2011b) notes that the right to be forgotten can be translated in a "privacy by design" obligation. In discussions about the future of privacy and the respective legislation in Europe privacy by design and privacy by default are now presenting as central objectives and tools.

Theory has presented original suggestions to ensure legally and technically the right to oblivion. Zittrain has proposed an art of "reputation bankruptcy" to be declared every ten years, allowing individuals to clean "their reputation slates (through the deletion of certain categories of ratings or sensitive information) and restart[50]. Mayer-Schönberger proposes shifting the default when storing personal data "back to where it has been for millennia, from remembering forever to forgetting over time". This should be achieved "with a combination of law and software" [Mayer – Schönberger 2009] and concretely through the establishment of expiration dates on information. Mayer-Schönberger focuses on users' empowerment: The main idea is that users would be forced to specify a retention period, when saving a file in the same manner they specify the file's name **[**Blanchette 2011**].**

Controlling, however, the life-time of personal information is a difficult task, due not only to the nature of digital information (it is shareable and not consumed in its use) but also because of today's vast data retention and search capabilities. Thus, we need some automated mechanism to delete records that have escaped our control. One type of automated control which implements the right to be forgotten entails building a technological "self-destruct" or "expiration date" mechanism into data records. For instance, some systems allow copies of certain archived data (such as copies of emails maintained by email providers) to become unreadable after a user-specified time, without any specific action on the part of the user, through the use of cryptographic techniques and distributed hash tables. This solution, however, has the following limitations: The automated destruction mechanism can potentially render unusable valuable information if it applies for all data. To counter this problem, the creator of the data records should configure the timer of the destruction mechanism, but it is questionable whether data collectors or data aggregators would have the incentives to do so. Another challenge that needs to be addressed is that to control data records containing personal information in an automated way we need a mechanism to track and delete all instances of a record or document. This is particularly difficult to be implemented, due to the nature of information, as data records are easily integrated into other records, copied and shared with other parties.

Manual control, on the other hand, allows users to control their personal information, by choosing what data is to be retained and what is to be deleted. 'Deletion managers' are tools that can automate the process of deleting records by identifying and interacting with the parties keeping personal information. They can also track the flow of information from one party to another, and they provide users with an interface that supports them decide when or whether to delete records containing their personal information. Google's Dashboard[51], for instance, provides its users with the ability to delete selected records from products and services that Google offers, while tools such as the "Web 2.0 Suicide Machine"[52] allow users to erase their records and profiles from multiple social networking sites. Delete mechanisms, however, could be abused

[50] Zittrain (2008), p. 229.

[51] https://www.google.com/dashboard/

[52] http://suicidemachine.org/

by malicious parties seeking to cause harm or disrupt a person's digital presence in her social networks.

7. Conclusion

Without any doubt, one cannot deny the value of having (at least a portion of) the past forgotten, the value of "starting over", the value of deleting both digital footprints and especially digital shadows. Actually, as already discussed, the right to be forgotten reflects a social value[53] and – just as the umbrella right of informational privacy - constitutes a democratic prerequisite for participation to societal life and public discourse, free from social disgust, disgrace, public or private surveillance.

A right to be forgotten should ensure that the information which relates to an individual "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"[54]. Time seems to be a decisive parameter as far as it concerns balancing remembering and forgiveness, the right to be forgotten and the social interests and individual rights on preserving, sharing and accessing information. Time is, indeed, an important element of each of the existing legal forgiveness measures[55]. Forgiveness and balancing of interests are "too complex and important to be left to the private sector" [Lindsay 2012]. It appears suitable, if not necessary, to require clear and standardised sets of retention periods and respective decision- making and oversight procedures and mechanisms in order to weight competing rights and interests, if conflicts arise.

The conception of the right to be forgotten in the Proposal for a Data Protection Regulation tries to respond to major technological and societal challenges. This right offers data subjects at least the opportunity to re-evaluation of the secondary use of their data in changing contexts[56]. In this perspective it could, without doubt, contribute to shift the balance in favour of the data subject and re-establish at least some of the control that individuals have lost over their data [Bernal 2011]. With regard to implementing an individual's right to be forgotten there is the need to balance this right with competing rights and interests, such as freedom of expression, freedom of contract, preservation of socially valuable information, and mutual parties with interests in the same data record.

[53] About the discussion if forgetfulness is a social value, a right or a legitimate interest see Koops (2011) and Rouvroy (2008).

[54] See EDPS, Opinion of 14 January 2011 on the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union", p. 18.

[55] Our legal system acknowledges that punishment should not necessarily be eternal. The person's right to avoid disclosure of facts and information about her status of being accused or convicted is laid down in central European law either as confidentiality/secrecy of the pre-trial stage or as restricted and exceptional access to criminal records (Mitrou, 2012).

[56] See Ausloos (2012), p. 145 f.

However, the affirmation of this right could not be regarded as panacea or serve as a regulatory alibi for pervasive and intrusive processing. A right to be forgotten could not replace the legal requirements concerning the predominance of informed and explicit consent[57], the lawful processing and compliance with core data protection principles like the principle of proportionality and data minimization. S*ome authors point out that "*introducing a 'right to be forgotten' only postpones this illusion of choice" (Koops 2012). Indeed, as proposed the right to be forgotten would usefully put pressure especially on advertisers, search engines and social networks sites to respect the users' wishes about the control over their data but it could also "(offer) a wild card for more privacy-intrusive uses" [Koops 2012].

The affirmation of such a right[58] could (and should) function along with new rules referring to explicit obligations and accountability for data controllers[59], data portability, and data breach notification in order to ensure more effective protection for data subjects. The usefulness of this right depends largely upon its construction and enforcement in practice and on the adoption of this right as "privacy by design /privacy by default requirement"[60] for the processing of personal information. If additional and detailed legal provisions are needed to effect a right to be forgotten, these legal measures have to be supported, supplemented and reinforced by technical measures.

A kind of "Privacy Digital Rights Management (DRM)" could enforce policies and individual control over the use of data. However, if the burden is placed on users to set preferences or expiry dates, this may be regarded as too onerous and it will be largely ignored [Lindsay 2012]. Over-reliance on the technological aspect can be problematic since there are often inherent limitations in many technological artifacts and they are seldom user friendly.

Moreover, technical solutions focusing or relying on empowering users to have their data deleted are therefore unlikely to find a support by data controllers and they are

[57] That means that it doesn't simply consist in a "just-click submit" consent fallacy but it is confirming the choice of an individual while exercising her right to informational self-determination.

[58] It is noteworthy that both France and Italy had even before the Proposal of the Data Protection Regulation presented legislative proposals in this matter. France has also adopted the Code of Good Practice on the Right to be Forgotten on Social Networks and Search Engines (Charte du Droit à l'oubli numérique dans les sites collaboratifs et moteurs de recherché) which however is not compulsory. However, the French Data Protection Authority has not signed this Code.

[59] According to Ausloos, controllers might also become more lenient in their privacy policies, as the subject has the right to demand retroactive removal of all his/her data (p. 146). Bernal notes that the right to be forgotten is simply putting the 'rights' side of an existing principle: allowing individuals to demand that those holding data fulfil their existing obligations (p. 9).

[60] That means shifting the default when storing personal data "back to where it has been for millennia, from remembering forever to forgetting over time" (Mayer- Schönberger 2007, p. 17). Bernal notes that this (right) can form part of a bigger paradigm shift - a shift to a position where privacy is the norm rather than the exception (p. 1).

susceptible to circumvention by them. Technical measures need strong support from the law in order to be - mandatorily - deployed. The advent of ICTs tend to shift the balance of power away from the individual user of technology to those who accumulate, store and manage users' personal data. PETs and technological trends such as Privacy by Design can offer a certain level of privacy protection, but their effectiveness can be hindered by several factors, including improper application and use, limited user awareness and counter technologies. It's worth remembering that the promising – and voluntarily proposed - PETs are still not widely adopted on a large scale.

Built-in solutions that provide forgetting in the Internet architecture are still in an embryonic phase. Automated mechanisms that apply the right to be forgotten suffer in general from problems similar to that DRM solutions provide for copyrighted materials: they may hinder the distribution and use of valuable material and there is always the possibility that counter technologies that circumvent the self-destruct mechanism are applied. Furthermore, power relations, advocacy coalitions and lobbies in privacy field are apparently different from those related to copyright protection interests[61].

The introduction of technological constraints and barriers on persistence, accessibility and replicability of information is a necessary but not sufficient condition for guaranteeing privacy rights in the digital world. Technological solutions are able to support individuals by controlling the use of their data but they cannot replace the legislator in defining and designing the scope and the limits of remembering and forgetfulness. Technological defaults are the symptom [Lindsay 2012] or the result of social and economical processes and choices. Every specific regulatory framework reflects a political a political and legal compromise under particular circumstances and within a given socio-economical and technological context. Since these problems are common to all technological solutions to content control, it is evident that the technological approach alone is insufficient and should be combined with legal and procedural measures to ensure that personal information will not be permanently retained and become potentially a widespread and ever lasting digital stigma.

REFERENCES-BIBLIOGRAPHY

Ambrose, M., Friess N., Van Matre J. (2012). Seeking Digital Redemption: The Future of Forgiveness in the Internet Age. Pages 1-55. Available at work.bepress.com

Andrade, Norberto Nuno Gomes de (2012). "Oblivion: The right to be different … from oneself. Reproposing the right to be forgotten". In: "VII International Conference on Internet, Law & Politics. Net Neutrality and other Challenges for the Future of the Internet". I*dp. Revista de internet, derecho y política*. No. 13 (2012), p. 122ff

Ausloos, J. (2012). The right to be forgotten – Worth remembering? Computer Law & Security Review 2012. Available at ssrn:http://ssrn.com/abstract=1970392

[61] Koops (p. 249) underlines that this fact "lowers the odds that policy-makers will adopt a strong law/technology-combo approach to effect the right to be forgotten".

Blanchette, J.-F. (2011). The Noise in the Archive: Oblivion in the Age of Total Recall, in Gutwirth S. et al.(ed.), Computers, Privacy and Data Protection: an Element of Choice, Dordrecht Heidelberg London New York 2011, p. 25 ff.

Blanchette, J.-F. and Johnson, D.G. (2002). Data Retention and the Panoptic Society: The Social benefits of Forgetfulness, *The Information Society* 18 (2002), p. 33ff.

Castelano, P. S. (2012). The right to be forgotten under European Law: a Constitutional debate, *Lex Electronica*, vol. 16.1 (Hiver/Winter 2012)

DPWP -Data Protection Working Party (2011). Opinion 15/2011 on the definition of consent.

DPWP - Data Protection Working Party and Working Party on Police and Justice (2009a). The Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, Brussels 2009

DPWP -Data Protection Working Party (2009b). Opinion 5/2009 on online social networking.

De Terwangne, C. (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". *IDP. Revista de Internet, Derecho y Política*. No. 13, pp. 109-121. Available at http://idp.uoc.edu/ojs/index.php/idp/article/view/n13-terwangne_esp/n13-terwangne_eng

EDPS - European Data Protection Supervisor (2012).Opinion of the EDPS on the Data Protection Reform Package (07.03.2012).

EDPS - European Data Protection Supervisor (2011 a). Towards more effective Data Protection in the Information Society. Appeared in the 50th Issue (April 2011) of *datospersonales.org* - Digital review published by the Data Protection Authority of Madrid, Madrid 2011.

EDPS - European Data Protection Supervisor (2011b). Opinion of 14 January 2011 on the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union.

EDPS - European Data Protection Supervisor (2010). Making data protection more effective: challenges and opportunities", British Chamber of Commerce in Belgium ICT Committee - Breakfast Roundtable: "Data Loss Prevention – Is sensitive information leaving your organisation?" Brussels, 9 March 2010

Eltis, K. (2011). Breaking Through the ―Tower of Babel‖: A ―Right to be Forgotten‖1 and How Trans-Systemic2 Thinking Can Help Re-Conceptualize Privacy Harm in the Age of Analytics, FORDHAM INTELL. PROP. MEDIA & ENT. L.J. Vol. 22 (2011), p. 69 ff.

Giannakaki, M. (2011). The right to be forgotten in the era of social media and cloud computing, in Akrivopoulou C. and Garipidis N. (ed.), Human Rights and Risks in the Digital Era: Globalization and the Effects of Information Technologies, 2012, p. 11 ff.

Gürtler, P. (2012). Baustelle Datenschutz –Internationale Entwicklungen, RDV 3/2012, p. 126 ff.

Koops, B.-J. (2011). Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right to be forgotten"in Big Data Practice, (2011) 8:3 *SCRIPTed Volume 8, Issue 3, December 2011, p. 229ff.* Available at: http://ssrn.com/abstract=1986719

Levi, M. and Wall, D. S. (2004). Technologies, Security, and Privacy in the Post-9/11 European Information Society. Journal of Law and Society 31 (2004), p. 194 ff.

Lindsay, D. (2012). The emerging right to be forgotten in data protection law: some conceptual and legal problems, Proceedings of the 8th International Conference on Internet, Law & Politics Challenges and Opportunities of Online Entertainment, Barcelona 2012, p. 419 ff..

McNealy, J. (2012). The Emerging Conflict between Newsworthiness and the Right to Be Forgotten. Northern Kentucky Law Review, 2012. Available at SSRN: http://ssrn.com/abstract=2027018

Marx, G. (1986). The iron fist and the velvet glove: Totalitarian potential within democratic structures. In Short *J. (ed.),* The social fabric: Dimensions and issues, Beverly Hills 2006, p. 135 ff.

Mayer-Schönberger V. (2009). DELETE: The Virtue of Forgetting in the Digital Age. Princeton: Princeton, University Press.

Mayer-Schönberger, V. (2007). 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. Available at http://www.vmsweb.net/attachments/pdf/Useful_Void.pdf.

Mitrou, L. (2010). Privacy challenges and perspectives in Europe. In M. Bottis (ed.), An Information Law for the 21st Century, Athens 2010, p. 220 ff..

Mitrou, L. (2012). Naming and Shaming in Greece: Social control, law enforcement and the collateral damages of privacy and dignity. Proceedings of the 8th International Conference on Internet, Law & Politics Challenges and Opportunities of Online Entertainment, Barcelona 2012, p. 453 ff.

Pino, G. (2000). "The right to personal identity in Italian private law: Constitutional interpretation and judge-made rights". In Van Hoecke M. and Ost F. (eds.). The harmonization of private law in Europe. Oxford: Hart Publishing (2000), p. 225 ff.

Pizzetti F. (2009),Is there a "fundamental right to forget?" -Speech held on Data Protection Conference – Brussels 2009. Available at ec.europa.eu/justice/news/events/...dp_**2009**/.../**PIZZETTI**_Francesco.ppt

Robinson, N., Graux, H. and Botterman, M. (2008). Review of EU Data Protection Directive

Inception Report prepared for the Information Commissioner's Office by RAND Europe, time.lex and GNKS-Consult, August 2008

Rosen J. (2012). The Right to Be Forgotten, (2012), 64 Stanford Law Review ONLINE (2012), p. 88 ff.

Rouvroy, A. (2009). Réinventer l'art d'oublier et de se faire oublier dans la société de l'information (Version augmentée du texte paru dans l'ouvrage collectif édité par Stéphanie Lacour, La sécurité de l'individu numérisé – Réflexions prospectives et internationales, L'Harmattan, 2009). Available at http://works.bepress.com/antoinette_rouvroy/5/

Solove D. (2007). The Future of Reputation – Gossip, Rumor and Privacy on the Internet. New Haven and London: Yale University Press 2007

Walker, R. (2012). Forcing Forgetfulness: Data Privacy, Free Speech, and the "Right to Be Forgotten" (March 18, 2012). Available at SSRN: http://ssrn.com/abstract=2017967

Weber, R. (2011). The Right to Be Forgotten: More Than a Pandora's Box?, 2 (2011) JIPITEC 120

Werro, F. (2009). The right to inform v. the right to be forgotten: A transatlantic clash. In: A. Colombi et al. (eds.), Liability in the third millennium, Georgetown Public Law Research Paper. No. 2, p. 285-f.

Wong R. and Savirimuthu J. (2008?), All or nothing: The application of Art. 3.2 of the Data Protection Directive 95/46/EC to the Internet, John Marshall Journal of Computer & Information Law, Vol. 25, No. 2. Available at http://ssrn.com/abstract=1003025

Wong, R. (2008). Social Networking: Anybody is a Data Controller. Available at SSRN: http://ssrn.com/abstract=1271668

Xanthoulis, N. (2012). Conceptualising a Right to Oblivion in the Digital World- A human rights-based approach. Available at http://ssrn.com/abstract=2064503

ZITTRAIN, J. (2008). The future of the Internet and how to stop it. New Haven: Yale University Press 2008