Comunicación: el debate en torno a la autorregulación y la cancelación de datos personales en internet

The debate on self-regulation and cancellation of personal data on the Internet

Carmen Sabater Fernández
Universidad de La Rioja
carmen.sabater@unirioja.es

Resumen

La comunicación trata sobre el derecho a la cancelación de datos personales en Internet (conocido popularmente por el "derecho al olvido") y la necesidad de una normativa regulatoria del uso indiscriminado de la información personal en la Red. Se presenta el contenido de este derecho, la problemática asociada al mismo derivada de la exposición pública y permanencia de la información personal, más allá del objetivo para el que fue recabada, y las propuestas legislativas presentadas en la Unión Europea sobre la actualización de la privacidad de los datos personal y en Estados Unidos, como propuesta *Privacy Bill of Rights*. Si bien, en la primera, se enfatiza en la necesidad de un control posterior de los datos de bloqueo o eliminación, en la segunda se proponen limitaciones al uso indiscriminado de determinada información personal (religiosa, financiera, médica) pero ambas coinciden en conceder un mayor control de los datos personales a los propios usuarios. Por último, se propone la defensa de un área proactiva de la propia privacidad que contemple los derechos subjetivos fundamentales, sin menoscabar la libertad de expresión.

Palabras clave Derecho al olvido. Derecho a la cancelación de datos personales. Protección de la información. Privacidad en Internet.

Abstract

Communication is about the right to cancel personal data on the Internet (known popularly as the "right to forget") and the need for legislation regulating the indiscriminate use of personal information on the Web is presented the content of this right , the problems associated with it derived from public exposure and retention of personal information beyond the purpose for which it was collected, and the legislative proposals in the European Union on updating the privacy of personal data in the United States, as proposed Privacy Bill of Rights. While, at first, it emphasizes the need for further control data block or delete, the second proposed limitations to the indiscriminate use of certain personal information (religious, financial, medical) but both agree grant greater control of personal data to the user. Finally, we propose proactive defense of an area's own privacy that includes fundamental individual rights without undermining the freedom of expression.

Key words: Right to oblivion. Right to cancellation of personal data. Protection of information. Internet Privacy

Fecha recepción: Febrero 2010 **Fecha aceptación:** Abril 2010

Introduction

> *José Luis Rodríguez Álvarez, director of the Spanish Agency for Data Protection, declares that technological advances have seriously questioned privacy guarantee systems: "Today, these barriers practically do not exist. Our personal data is easily available to anyone" (Dávila, 2011)*

Digital identity (also called identity 2.0) has gained great prominence in recent years. The data is spread over the network either by our own decision from the creation of profiles on social networks or other 2.0 services, or from the publication of our personal data on institutional websites or in official bulletins and their indexing in the seekers. The reality is

that, more and more, the information of our real identity crosses the border of the private and filters into the public space.

The Internet generates a diffuse environment in constant expansion with great possibilities for information and communication, but with greater difficulties in monitoring and controlling personal information. Paradoxically, the data that was solely owned by the person is extended to commercial files, exceeds the audience and the time for which they were created or is published by official bodies without our explicit authorization.

In this context, the right to cancellation of personal data (popularly known as "the right to be forgotten" or "right to be forgotten") represents the possibility of self-regulation of personal information itself. Marta Sánchez of the Legal Department of Áudea defines it as the *"The right of all people to manage their personal data, in this case on the Internet, establishing all the necessary legal mechanisms so that all published negative information disappears, as well as its indexing in the main search engines, with the aim of recovering and controlling our information. , guaranteeing the right to one's own image, honor and personal and family privacy"* (Sanchez, 2011). Jurists such as Guillermo Borda propose the development of an authentic subjective right on the disposition of digital life, as the faculty of each human being to build their own biography free of interference that could harm them (Borda, 2011).

This right represents, therefore, the possibility of eliminating information that is likely to harm personal life. The Director of the AEPD, Artemí Rallo, raises some of these situations that can harm personal life, related to the workplace (layoffs or selection processes), and the administrative field (publication of sensitive information in official gazettes: pardons, sentences, subsidies to exclusion groups, etc.).

The problems derived from the collection of personal data derive fundamentally from the conversion of private information to public without the consent of the interested party and its permanence on the Internet.

Problematic: the "perpetual" transfer from the private to the public

The management of digital identity reaches the very nature of the Internet, whose characteristics of openness, expansion and turbulence are mimicked in the individual data that circulates on personal information. Private life is increasingly projected in the virtual world of the Internet – on many occasions, linked to acts of third parties – and, in turn, technological habits occupy a greater space in our daily lives (Rallo, 2010).

The problem is complex since the digital identity is formed from various temporal processes and different biographical dynamics. Private personal life coexists with professional public life. The web 2.0 environment itself favors the introduction of tools managed by the user himself, who thus becomes responsible for the storage and collection of his information. But the user's consent exceeds the voluntary limits for which it was assigned, since factors such as transmission and sale to commercial companies or indexing favor its location with a simple nominal search.

The right to privacy collides with freedom of expression in an always diffuse limit. The Spanish Agency for Data Protection (AEPD) points out that "Freedom of expression has its limit in respecting other fundamental rights" (Gómez, 2011). In this context, the defense of a proactive area of private choice is generated whose claim mechanisms are difficult to implement a posteriori.

On the other hand, companies such as Google point out that there is a risk of turning this right into a weapon of censorship, especially when a search engine is asked to eliminate a journalistic article in which a reference to a third party is made. Currently, Google and the AEPD are in a litigation process before the Spanish Court due to the refusal of the US firm to remove certain content with more sensitive personal information from its search engine.

For his part, Elliot Schrage, Director of Policy for the United States of Facebook, describes the right to be forgotten as a control of the information itself by users, but considers that specific legislation is contrary to technological development, free flow of information and

global connectivity. "What we want is an orientation, a clear guide, a broad explanation regarding the right to be forgotten, we have to see how to offer better tools to people [...] The idea of a strict rule that says 'right to be forgotten' it is not the evolution of technology" (Sánchez Onofre, 2011)

These companies protect their lucrative interests since the principle that should prevail is the voluntary decision of the Internet user. The current reality is that the leaks of the private into the public sphere of the Internet are not controllable by the user himself, who is subjected to a public exposure that he has not chosen voluntarily. The problem lies mainly in the information that may violate respect for personal dignity. This is the case, for example, of a woman whose name appeared linked to a pardon in search engines. As established by law, the resolution was published in the Official State Gazette (BOE). The digitization of the bulletin multiplied its diffusion to infinity. Google turned that commutation of sentence -a news of little interest except, naturally, for the affected- in a public news. Entering her name in the search engine automatically revealed that she was pardoned in 1995. After unsuccessfully requesting Google to cancel her personal data, the woman, pardoned 13 years earlier, went to the AEPD in 2008, which upheld her rights as it was information that it violated his personal dignity (Gómez, 2010).

The user can find himself in a delicate situation when he finds himself with costly and slow mechanisms to eliminate "confidential" information that he does not want to acquire a permanent public reach. Precisely, the European regulation aims to facilitate the procedures for the deletion of data, whose presence may harm the interested party.

The problems are inserted in the individual biography since the information on the Internet acquires a permanent character, even once the object for which it was collected has been extinguished. Under Spanish law, the information published in official gazettes should not be perpetual, since there are limits both in time (deadlines) and in relation to public interest. However, the possibilities of searching for previous newsletters or the lack of updating of some websites affect the stability of information without an expiration date. The biographical history of the past creates "traces" in the individual life of the present,

which can have consequences in the search for a job or in the personal image. At the 33rd International Conference of Data Protection and Privacy Authorities, organized by the Federal Institute for Access to Information and Data Protection (IFAI), Marie Hélène Boulanger, from the European Commission, pointed out the importance of the time that the information on the network and stated that the information retention period is a controversial issue. Her proposal proposes to analyze the issue to set a period of conservation of the information (Dávila, 2011).

Finally, it should be noted that there are greater difficulties and even the impossibility of withdrawing the information, when it is published with the consent of the user, since they have granted authorization for its publication. Martínez Ferre (2011) points out that, as a general rule, any person should not put up with their personal data being permanently accessible on the Internet as a result of the inclusion of their data in search engines. To do this, two circumstances must be met:

- The purpose for which these data were published. If this was the notification to the interested party of a certain administrative act, once this has been carried out, and after the periods for exercising possible resources have elapsed, the purpose would be fulfilled, and therefore it would not be necessary to maintain these data for their search through through search engines.

- The condition of public figure of the owner of the data, and that the fact has public relevance. Consequently, any person or fact that does not meet these characteristics should not support the inclusion of their data on the Internet indefinitely. But the facts can have a public interest at a certain moment, ceasing to have this character after a while.

The right to privacy is presented actively and prior to the use of your data, and not only as the possibility of withdrawing consent to subsequent data processing. In this way, we find two differentiated visions of this right in the European and American administration. While the European administration advocates more for the treatment that is done on the Internet of one's own personal image, which would translate into the "right to be forgotten" and the

control of information "a posteriori"; In the American administration, self-regulation by the user himself is advocated in a more permissive attitude to the observation of individual private life due to his historical defense of freedom of expression (Hendel, 2011). However, the need to limit indiscriminate access to personal data has also reached the US.

The legislative proposals made in the European Union and the United States are presented below.

Proposals on privacy for the regulation of personal information

European Union: Legislative proposal on the privacy of personal data

Viviane Reding defends a legislative proposal on the review of current legislation - dating from 1995 - on the privacy of personal data. This proposal arises from the extension of personal information shared over the Internet, which requires the need to create a clear and up-to-date set of rules that guarantees a high level of data protection and privacy for all users. Social networks, specifically Facebook, will be one of the main objectives of these new rules. “Our data is being collected without our consent and often without our knowledge. This is where European laws must intervene… People must have the right to say “no” whenever they want” (Reding in Martínez, February 1, 2010).

The legislative process launched by the European Commission aims to strengthen the protection of citizens' data and adapt the old rules to the virtual environment, where documents not only have a global scope but are also permanent (Gómez, 01/07 /2011).

In this line, the Commissioner will present a legislative proposal to increase the protection of the right to cancellation of personal data in online social networks. The objective of this initiative is for companies like Facebook to effectively and completely erase personal data and photographs when a user unsubscribes from the service, something that they currently do not do despite the existence of legislation in several countries that requires to it, like the LOPD in Spain. “People must have the right to withdraw their consent to data processing”,

defends the Vice President of the European Commission (European Commission, Brussels March 16, 2011).

The reform addresses both the regulation of the storage on the Internet of personal data that is not of public interest and the disappearance of the same in search engines, social networks and 2.0 services if the interested party so requests. Users of social networks such as Facebook or Tuenti will thus be able to have control of their data and demand the complete deletion of their personal information (written, graphic and audiovisual) when they unsubscribe from the service. A task that, at present, is presented as titanic and often frustrating (Gómez, 01/07/2011).

The goal is for the new laws to be stricter. The proposal will require that the configuration of social networks guarantee privacy by default, so that the use of the data for any other purpose that goes beyond what is specified in the contracting of the service, will only be allowed with the explicit consent of the user. . The burden of proof is on the companies, which must show why it is necessary to store certain personal information.

With the modernization of the legislation, we want to expressly ensure that people have and enjoy this right actively and prior to the use of these data, and not only as the future possibility of withdrawing their consent to subsequent data processing.

Another objective of the regulations is that Internet providers, search engines and social networks store as little personal data as possible. Commissioner Reding states that "Any company that operates in the European market or for any online product that has consumers from the European Union as buyers must comply with EU rules" ((European Commission, Brussels March 16, 2011).

The EU will demand greater transparency from the companies that manage these virtual communities, which will be obliged not only to inform users about the data they are going to collect, for what purposes and how it can be used by third parties (as already specified by current legislation) but also to communicate to users what the potential risks are. The vice-

president has remarked that "this is particularly important for younger Internet users" (Europa Press, 03/17/2011). In this way, regulations will be required that make it clear to children what consequences registering on a social network has, explaining in clear and accessible terms where to locate information on the processing of personal data.

The Commission will also influence the obligation of companies that process data of EU citizens but have their legal headquarters in a country that is not a member, to comply with these rules. To this end, the data protection agencies of each country of the Union will be empowered to cooperate more effectively with each other and to legally prosecute foreign companies so that they adapt their activity to this new legislation. This issue is basic for the guarantee of users, since the social networks with the greatest penetration in our country – with the exception of Tuenti- are based in the United States, so they are not obliged to comply with European regulations.

The European Union aspires to bring transparency to the foggy digital world. Its objective is that Internet service providers or search engines collect the minimum data from users and that they carry out this collection process clearly, communicating who stores them, how, for what purpose and for how long. In addition, it is proposed to simplify and improve the exercise of the rights of access, rectification and deletion of content related to the user. The intention of the Community Executive is to curb the absolute power of search engines and service providers.

The defense of these rights has come about as a reaction to citizen pressure -especially due to the increase in complaints and claims- and due to the legal problems that have arisen in recent years, especially linked to US companies such as Google (especially with its controversial Google Maps Street View service) and Facebook.

The multinational Google takes refuge in the current legal loopholes, alleging that the data and its possible use are not the responsibility of the company, since the service is provided from the USA. In this way, the European data protection directive and the Spanish law that applies it, do not affect them. In addition, they allege that the webmaster himself must be

the one to install certain tags to prevent the Web from being tracked by the googlebot, since his technology does not allow the modification of the content (Gómez, 01/07/2011). For this reason, cooperation is vital, as Artemí Rallo, President of the AEPD, points out: "The Internet is a global framework and needs a global standard, with international privacy protection treaties. That is the only logic that can satisfy the demand to protect privacy. Strength is in unity" (Gómez, 01/07/2011).

This problem has also reached Spain, especially since 2009, the date on which the networks increased their penetration. Thus, the former director of the AEPD, Artemí Rallo, indicated in March 2010 that social networks are "obliged to carry out an urgent update" of their digital platforms to respect the right to privacy of their users (Editor DJ, 15 of April 2010). The Agency itself encourages citizens to request the cancellation of their private references in forums, blogs, social networks or search engines if they consider that respect for their personal dignity is violated: "No citizen who does not enjoy the status of a public figure or is object of an event of public relevance has to resign himself to his personal data circulating on the Internet" (Gómez, 01/07/2011).

In Spain, the problems of information on the Internet derive:

1.- Of its permanence and its global expansion. As Artemí Rallo explains, "the problem is not the avalanche of information about a person that can be found on the Internet, but that information is imperishable... The right to be forgotten refers to the multiplying effect of Google and search engines. It can be deleted the personal information of a digital medium or data that appears in the BOE, such as fines, sanctions or pardons. That information, unlike what happens on paper, acquires a global and temporally eternal expansion. It is quite reasonable that something that happened 30 years ago it was not in the indices of a search engine" (Gómez, 01/07/2011).

For Artemi Rallo, the right to be forgotten recognizes the cancellation of personal data that has been legitimately collected so that it can be withdrawn when the purpose for which it was obtained is exhausted. It is equivalent to realizing the power of any citizen to have all

the information of which he is the owner and to ensure that digital memory does not become something perpetual (Gómez, 01/07/2011).

2.- **of the problem of consent**, in the event that the information has been provided voluntarily. Marc Carrillo, Professor of Constitutional Law at the Pompeu Fabra University, explains that the intention of an individual to erase the data that refers to his person on the Internet "is legitimate in cases in which his appearance on the Internet has not been of their own free will, but as a consequence of appearing in an archive, public or private, and the reason for this is of no public interest" (Gómez, 01/07/2011).

But this claim is not sustained if the individual, for example, is the author of a crime convicted by a final judgment as it is an act of public interest, and in the case of the information published on social networks since it has been done of his own free will. The only way could be that the administrations of the webs equip themselves with the adequate computer measures that allow avoiding the indexing of the news.

The AEPD also acts to cancel data published in Internet forums provided by a third party without the consent of the affected party. In this case, the agency specifies that the comments posted on the Internet fall within freedom of expression, but it clarifies: "Freedom of expression has its limit in respect for other fundamental rights." It states that, even if the information published in that forum was truthful, "since it does not refer to public matters of general interest, the fundamental right to data protection prevails" (Rallo, 2010).

Experts agree that citizens must have mechanisms within their reach to cancel personal data and prevent their universal maintenance on the Internet.

Proposals in the United States: Privacy Bill of Rights

In the United States, in December 2010, the Federation Trade Commission (FCT) proposed the creation of a tool so that consumers could prevent their online monitoring (likes, visits, searches, etc.), based on the idea presented by the person in charge of Commission, Jon

Leibowitz that "privacy self-regulation has not worked well so far and is not working well for American consumers" (Angwin & Valentino-Devries, 12/02/2010). On this same date, the Democratic Party defended the elaboration of a law that would regulate the monitoring of the navigation of children under 13 years of age on the Internet, so that it would be necessary to obtain parental permission before collecting personal data, such as the names or email addresses of the children (Stecklow, 12/23/2010).

In March 2011, the need to expand the defense of privacy began to spread through the development of a “Privacy Bill of Rights”1 (Johnson, 02/03/2011). This Charter would regulate the commercial collection of user data online, what can and cannot be recorded, and what use would be acceptable for the data collected. The FTC would be in charge of ensuring that these codes of conduct were respected, fulfilling a mission analogous to that already carried out in Spain by the Data Protection Agency.

According to the US Secretary of Commerce, Gary Locke, “industry self-regulation is not enough”. (Johnson, 02/03/2011) since the use of personal data has increased so much that specific legislation is needed that, through mandatory measures, allows consumers' trust to be recovered online, while establishing a framework for companies to continue doing business online.

In April 2011, Senators John Kerry and John McCain proposed legislation to create the "Privacy Bill of Rights" to protect individuals from increasingly invasive commercial data collection practices. This bill, called the Commercial Privacy Bill of Rights Act of 2011, imposes new rules for companies that collect personal data, such as prior consultation on access to data or the ability to block the information from being used or distributed. In this way, companies would have to ask for permission before collecting and sharing sensitive data (religious, medical and financial information) with external entities (Angwin, 2011).

The bipartisan proposal represents the first comprehensive privacy law and largely adopts recommendations made by the Obama administration in 2010. Current US laws only cover the use of certain types of personal data, such as personal information. financial and

medical. This legislation responds to the need for users to have control over data access to third parties and to the limitation of the commercial use of personal data.

In this debate, social networks represent the first front of the battle, because they have been the technological applications that have most influenced the change in privacy, because of their great penetration among Internet users and because of the personal identification of users/ as (which, in most cases, share real data). In particular, Facebook, which has always been at the center of the controversy.

In the US, there are websites that encourage Internet users to leave the Facebook network, such as http://www.quitfacebookday.com/, while some US organizations such as MoveOn.org or the Electronic Frontier Foundation have published information on the regression of Facebook in its practices to protect the privacy of its members. The European group of data protection agencies sent a letter on May 12, 2010 to Facebook denouncing the changes in the privacy management options that, by default, open content to third parties. A complex option management because the Internet user had to evaluate 170 alternatives. Some US senators joined the protests (El País, 05/26/2010).

The reform is aimed at regulating the storage on the Internet of personal data that is not of public interest, limiting its indiscriminate collection, providing greater transparency in its management, information to the user about its use and the possibility of making Google's personal data disappear, Yahoo, YouTube or social networks, if the interested party so requests. The proposal will require that the configuration of social networks guarantee privacy by default, so that the use of the data for any other purpose that goes beyond what is specified in the contracting of the service, will only be allowed with the explicit consent of the user. .

The defense of these rights has come about as a reaction to citizen pressure – especially due to the increase in complaints and claims – and due to the legal problems that have arisen in recent years, especially linked to US companies such as Google. In this debate, social networks represent the first front of the battle, because they have been the

technological applications that have most influenced the change in privacy, because of their great penetration among Internet users and because of the personal identification of users/ as (which, in most cases, share real data).

Conclusions

The right to be forgotten represents a subjective right that defends fundamental prerogatives (right to image, honor, personal dignity...) that conflict with other basic rights, such as freedom of expression. The Internet generates a new technological environment that affects the personal interests of the subject, creating situations of defenselessness derived from the perpetuity and publicity of the information.

The proposal defends the defense of a proactive area of the privacy of the subject. It is considered that this right should prevail in circumstances that entail serious harm to the individual, especially if the information extends its disclosure beyond the period for which it was created and in the event that it has no public relevance or has been exhausted. However, it is considered that it would have to adopt a flexible form that does not imply censorship and interferes as little as possible with freedom of information. The regulations would have to analyze the possible situations (especially if the subject has given their consent to the publication or it depends on third parties), limit the indiscriminate use of the most sensitive information (medical, academic, financial, ideological, location data) and verify the damages for the interested party.

Faced with the dilemmas of the right to be forgotten, we join the opinion of Marie Hélène Boulanger, representative of the European Commission, who considers that the right to be forgotten must be exclusive to the control of individuals. “Data protection authorities have to be strengthened to provide a response. It is not the right to hide, it is a balance between freedom of expression and the right to data protection” (Sánchez Onofre, 2011).

But, without a doubt, the most suitable option in a turbulent environment is for the Internet user himself to adopt an attitude of prudence and think, before publishing his

private information, about the possible current and future consequences of using it. Likewise, it is considered essential that both legal entities (commercial companies, public bodies) and individual subjects have an attitude of greater caution in the processing of personal data, especially with those of a private nature.

Bibliography

ANGWIN, J. (2011). "Senators Offer Privacy Bill to Protect Personal Data". *The Wall Street Journal*. Recuperado de http://online.wsj.com/article/SB10001424052748703385404576258942268540486.html

ANGWIN, Julia & VALENTINO-DEVRIES, Jennifer (2010) "FTC Backs Do-Not-Track System for Web". *The Wall Street Journal*. Available in http://online.wsj.com/article/SB10001424052748704594804575648670826747094.html

DÁVILA, René (2011). El derecho al olvido debe estar garantizado en el mundo digital, piden autoridades internacionales de protección de datos. *Journalmex*. Recuperado de http://journalmex.wordpress.com/2011/11/04/el-derecho-al-olvido-debe-estar-garantizado-en-el-mundo-digital-piden-autoridades-internacionales-de-proteccion-de-datos/

EUROPA PRESS (2011). Bruselas garantizará por ley el 'derecho al olvido' en redes sociales como Facebook. *Portaltic.es sector*. Recuperado de http://ciberderechos.wordpress.com/

FANJUL, MARTÍNEZ, Diego (2010). Criterios de ámbito de aplicación normativa a buscadores. Recuperado de http://www.abogadoprotecciondatos.com/p/es/blog/derecho-al-olvido-i.php

HENDEL, John (2011). Europe, a Right to Be Forgotten Trumps the Memory of the Internet

in The Atlantic. Recuperado de http://www.theatlantic.com/technology/archive/2011/02/in-europe-a-right-to-be-forgotten-trumps-the-memory-of-the-internet/70643/

JOHNSON, Rich (2011, Febrero 3). A Privacy Bill of Rights?. in Site Jabber Blog.. Recuperado de http://www.sitejabber.com/blog/2011/02/03/a-privacy-bill-of-rights/?display=wide

PLAZA, ALBA, Esther (2011). El mundo interconectado requiere nuevas respuestas. *Profesiones,* 130, 38-39. Recuperado de http://www.profesiones.org/var/plain/storage/original/application/9ad0c95661d7b82853fa0414f186ea51.pdf

RALLO, LOMBARTE, Artemí (2010). El derecho al olvido y su protección: a partir de la protección de datos, *Telos: Cuadernos de comunicación e innovación,* 85, 104-108. Recuperado de http://sociedadinformacion.fundacion.telefonica.com/seccion=1268&idioma=es_ES&id=2010110416500001&activo=6.do#

SÁNCHEZ, ONOFRE, Julio (2011, Noviembre 2). El derecho al olvido: ¿Oportunidad o censura?. *El economista*. Recuperado de http://eleconomista.com.mx/tecnociencia/2011/11/02/derecho-olvido-oportunidad-o-censura

STECKLOW, Steve (2010, Diciembre 23). Proposed Law Would Prohibit Web Collection of Data on Kids. *The Wall Street Journal*. Recuperado de http://online.wsj.com/article/SB10001424052748703865004575649140574658582.html