The right to respect for private life: an effective tool in the right to be forgotten?

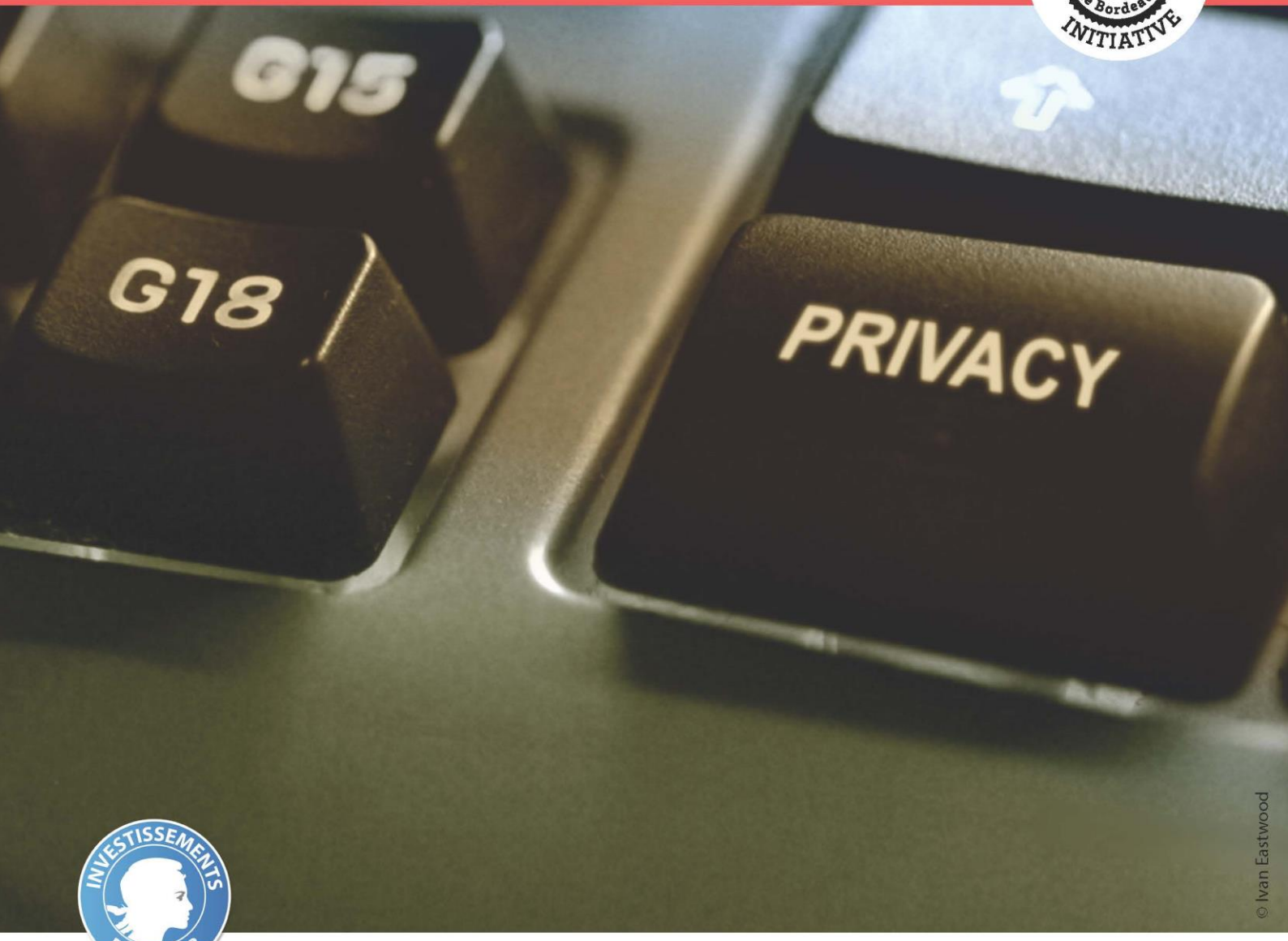
Maryline Boizard

Issue | July 2015
No.2 | Special Issue: Privacy

Montesquieu Law Review

The right to respect for private life: an effective tool in the right to be forgotten?

Maryline Boizard, Associate Professor, IODE UMR CNRS, Faculty of Law and Political Science, University of Rennes 1



© Ivan Eastwood

Program supported by the ANR
n°ANR-10-IDEX-03-02

Forum Montesquieu
Faculté de droit et science politique

université de BORDEAUX

The right to respect for private life: an effective tool in the right to be forgotten?

Maryline Boizard, Associate Professor, IODE UMR CNRS, Faculty of Law and Political Science, University of Rennes 1

Suggested citation: Maryline Boizard, The right to respect for private life: an effective tool in the right to be forgotten?, 1 Montesquieu Law Review (2015), issue 2, available at
http://www.montesquieulawreview.eu/review.htm

The right to be forgotten is not explicitly enshrined in positive law. Nevertheless, some legal provisions lead to it. Article 9 of the French Code Civil, Article 7 of the Charter of Fundamental Rights of the European Union, and Article 8 of the European Convention on Human Rights, which all enshrine the right to respect for private life; but also Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1) transposed into French law by an amendment to the *Informatique & Libertés* Law of 6 January 1978 – without making explicit provision for a right to be forgotten, all contain prerogatives that lead to such a right. French and European case law has been able to adapt and respond to critical cases. Since its inception, the *Commission Nationale Informatique et Liberté* (CNIL) has discussed the issue of the right to be forgotten in most of its annual reports.

Forgetfulness is the capacity to forget that an individual develops because it is necessary. In that perspective, the act of forgetting fulfils a constructive, even restorative, function. Forgetting modulates the memory in order to *"close the doors and windows of consciousness from time to time*" (2). Nevertheless, the advent of digital technology no longer allows forgetting to come into play under similar conditions and profoundly changes the situation under the combined influence of three factors (3). Firstly, the emergence of digital technologies which serve to store data with little or no risk of alteration. Next, the expansion of the internet, which offers potential access to a large proportion of stored data. Lastly, the use of search engines, which guarantees genuine access to a large proportion of stored data. As the act of forgetting no longer happens naturally, claims as to a right to be forgotten have emerged, which would be an individual's prerogative to require that certain events or certain data concerning him no longer be accessible as they are no longer current (4).

In practice, the initial decisions that had to rule on the existence of a right to be forgotten related to objections raised by persons involved in legal cases to the reporting of the facts several years after these had taken place. The argument typically invoked was the right to respect for private life, of which the right to be forgotten is often seen as a counterpart. More recent applications have, however, encompassed a variety of situations that go beyond the framework of the right to respect for private life. They may relate to the publication of a person's criminal conviction several years before; disseminating pictures that are distasteful or disadvantageous when viewed now; even the storage of medical data in data banks. It is therefore a matter of securing the obliteration of – now mostly digital – traces of a past that a person wishes to forget or have others forget.

In this context, the right to respect for private life would appear to be increasingly irrelevant in addressing the issue of the right to be forgotten. This is why case law now turns more readily to the legal rules for the protection of personal data, which offer more flexibility to the courts. The limits of the right to respect for private life as a basis of the right to be forgotten (section I) result in it being set aside in favour of measures for the protection of personal data (section II).

I – The limits of the right to respect for private life

In order to be protected by the right to respect for private life, acts or data ought to fall within the remit of private life. However, the most recent case law on the subject – both European and French – shows that the right to be forgotten is not confined to the private lives of individuals. Two major differences between the right to respect for private life and the right to be forgotten mark the limits of the former as the basis of the latter. The first difference lies the time criterion (A); the second in the very concept of private life (B).

A – The time criterion

The definition given to the concept of forgetting shows that time is a necessary component. By that single finding, it becomes a characteristic of the right to be forgotten. Time is not, however, a criterion for classifying private life. However, the time factor explains how a public act may be protected by the right to be forgotten when it cannot be by the right to respect for private life. Conversely, it also means that the same act can sometimes be protected by the right to be forgotten and sometimes not.

In the matter of *Diana Z. v Google* of 15 February 2012, the *tribunal de grande instance* (regional court) at Paris condemned the famous search engine for invading the privacy of a woman who, twenty years earlier, had taken part in a pornographic video under a false name and whose real name had been associated with pornographic websites. The court characterized the "*manifestly unlawful disturbance*" by including a direct reference to the right to be forgotten "*if, when she made this film, Ms. Z. necessarily accepted necessarily a certain distribution even then she did not consent a priori to its digitization and distribution on the internet; and, while this video does not itself reveal scenes of private life, the fact remains that this film reflects a particular time in the life of the young woman, who wishes to exercise her right to be forgotten*". The court differentiated between the time criterion and private life, the former becoming essential in the enshrinement of the victim's right.

In the matter of *Google Spain v AEPD* of 13 May 2014 (5), a Spanish citizen had asked a newspaper in 2009 to remove a publication concerning a seizure of property resulting from the non-payment of debts incurred but eventually paid back to Social Security several years previously. Following a request for a preliminary ruling on the interpretation of measures for the protection personal data, the European Court of Justice established the principle of a right to be forgotten for people whose surname links to information concerning them. This right is not absolute. Beyond identifying the specificity of search-engine activity, the decision establishes the time criterion as a determining criterion for being forgotten. Here again, no reference is made to an invasion of privacy.

The ECJ decision was echoed in the French courts: the regional court at Paris handed down a decision on 19 December 2014, ordering the search engine to remove a link from its search results (6). Google was condemned for ignoring a request made by the interested party to be forgotten on the basis of the right to be forgotten, which request concerned an article about his

conviction in 2006 for fraud. In order to recognize that right, the court relied heavily on the age of the case as almost eight years had elapsed between the publication of the article and the filing of the complaint.

B - The concept of privacy

For the European Court of Human Rights, privacy is a broad, shifting concept (7). In 1992, the Court stated that: "*it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings*" (8). Nevertheless, restricting the right to be forgotten to an individual's personal data atrophies the scope of that right because it makes identifying the public or private nature of the information disclosed a key element in the protection afforded to the person. The qualification is not always obvious. We must in particular consider whether the initial dissemination of information exhausts the right to privacy. Case law is divided (9).

Media coverage of an event at the material time may have an impact on the legal treatment of the exploitation of the facts which gave rise to the event. Whenever a news story has had a great deal of media coverage, freedom of expression allows the story to be discussed without any objections raised on grounds of the right to be forgotten. In this area, the Court of Cassation appears to make the following distinction: either the facts have been sufficiently disclosed to be considered public, in which case replaying them does not affect privacy and blocks the right to be forgotten (10); or the facts were revealed by the person himself and, having formerly held the opposite view, that fact should not come into play: the re-disclosure by a third party therefore crystallizes a new invasion of privacy (11). This distinction is however not always followed. Disclosure by the applicant may also be seen as a justification. In reality, the distinction ought not to be based on a qualification of the facts but on the public interest in knowing the information.

Technological progress has led the ECHR to shift the boundaries between the public and private domains (12). Privacy has thus been argued in order to challenge electronic data capture (13), the systematic storage of public data (14), the disclosure of visual data obtained by video surveillance of public places (15) or even the storage in a font file of personal data, the accuracy of which is questionable (16). However, it would seem that the requirement as to the qualification of privacy elements does not afford sufficient protection to individuals and the lack of relevance of a connection between the right to be forgotten and the right to respect for private life is even more marked in the current context of the digital environment. Social media service providers, for instance, collect information that is initially private but which, when shared, is treated like any other information that one may decide to make public. Thus, even if the information is specific to the user, the user no longer has the monopoly on its use and may lose control over that information. Indeed, once private data is considered "public", the administrators of the social network or the search engine, subsidiaries, partners, advertising customers or other third parties may use it. It may be noted that Facebook has expressly developed this concept of "public information" that was originally private. The social network provider states that this is *"[s]omething that's public can be seen by anyone. That includes people who aren't your friends, people off of Facebook and people who use different media such as print, broadcast (ex: television) and other sites on the Internet*" (17). When a person shares information about another member on the network, he may choose to make that information public, though he himself may have chosen to

make it visible to a restricted audience on his own profile. Lastly, some information is always considered public, such as name, profile photos and cover photo, networks used, gender, user name and ID. Similarly, some group content on LinkedIn, a professional social network, may be public and available on the internet if the group owner has made the group public (18).

In this context, one can think that "*privacy has become an irrelevant concept*" (19) especially because it only addresses part of the problem raised by the right to be forgotten. "*On the Internet, there are public activities, while others involve a number of interests relating to privacy. In order to establish an approach consistent with the imperative of balance between all human rights, consideration must be given to the continuum aspect of public and private situations. In cyberspace, nothing is wholly public or wholly private, as if there were only black and white. The public and private intensity of situations is in varying shades depending on the context and circumstances*" (20). This is what explains the interest there is in re-exploring measures for protecting personal data.

II - The alternative basis for the right to respect for private life: the protection of personal data

The European authorities took hold of the right to be forgotten by adopting, on 25 January 2012, a draft Regulation making direct reference to it (21) - a choice that the European Parliament nevertheless revised (22) without, however, amending all the provisions inducing it. The measures for protecting personal data can be applied when information constituting personal data is subject to processing by a controller (section A). However, any information falling within the scope of these measures is not eligible for the right to be forgotten. Its implementation must be subject to certain criteria (section B).

A - The processing of personal data

The measures protecting personal data are broad in scope. Flexible and adaptable, they are likely to cover a wide variety of data processing despite the developments of digital technology and the internet. Where case law relies on the measures protecting personal data, it does not question the public or private nature of the information disseminated. The result is that information made public by the data subject or against his will (particularly when the publication is of legal origin or by journalists) is eligible for the protection scheme provided by Directive 95/46/EC if it constitutes personal data processed by a data controller.

Personal data is not necessarily an element of privacy. Surnames, for example, do not fall within the scope of privacy. Defined by Article 2 of the *Informatique & Libertés* Act of 6 January 1978 (23), personal data can be extremely diverse and one may consider that very little personal information falls outside the scope of the classification, which makes it of particular interest when faced with the issue of the right to be forgotten. Additionally, the legislature reserves even more protective measures for so-called sensitive data than those applicable to other data. This is the case for "*personal data that reveals, directly or indirectly, the racial or ethnic origins, political, philosophical or religious opinions or trade union affiliations of persons, or which relate to the health or the sexual life of said persons*" (24).

The processing of personal data is, in turn, to "*any operation or set of transactions (of personal data), whatever the process used [...]*" (25). The data processing concerned is extremely diverse and again covers a wide range of activities that may be carried out with the data.

Finally, the data controller is "*the person, public authority, agency or body that determines its purposes and means*" (26). The definition of the data controller is very broad and thus covers the vast majority of operators. It even includes, *a priori*, journalists, archivists and scientists. There are, however, derogations relating to the purpose of the processing that they perform. However, in the current context of the digital environment and networks, there is no doubt that the definition covers internet players. Under cover of a right to be forgotten, it is possible for victims to sue website publishers, social network service providers (27) or search engine service providers to obtain either the deletion or dereferencing of online content. In *Google Spain v AEPD*, the Advocate General denounced the risks of an extensive vision of the concept of data controller which did not, according to him, include search engine providers (28). Rather, the ECJ considered that it is their specific processing activity, which differs from but is added to that of website publishers who feature data on web pages, which serves in equating them to data controllers.

B - Implementing the criteria of the right to be forgotten

For the right to be forgotten to come into play, the processing performed must be classed as unlawful. A person's objection to such data processing renders the latter unlawful on certain conditions. As regards requests made to search engines, there is no vested right to be dereferenced or forgotten. The request will be rejected if, for specific reasons, such as the role played by the person in public life, the interference with his fundamental rights is justified by the overriding public interest in having access to the information in question. However, the ECJ stipulated that the right to be forgotten prevailed, in principle, not only over the economic interests of the search-engine operator, but also over the public's interest in accessing information when making an online search using a person's name.

The implementation of the right to be forgotten involves building a grid of indicators that could be taken into account to justify the deletion of dereferencing of data. The criteria are gradually emerging under the influence of case law (29), the European authorities (30) and operators themselves (31).

The time criterion is not absent from the data protection measures which, in our view, makes it even more relevant for the victims. The legislature pays particular attention to the time limits for storing data. It is true, however, that the provisions governing such periods are sparse and sometimes lack clarity. In the present state of positive law, it is impossible to identify a time sequence. The solutions are often very factual and the outcome will depend very much on the context. The implementation of the right to be forgotten via indexing or deletion can therefore come up against the issue of identifying the timeframe within which a request may be submitted. In *Google Spain v AEPD*, the ECJ made the passage of time a parameter for assessing the right to be forgotten. It allows the loss of relevance of information to be qualified. It is not, however, the only criterion. The capacity of the person concerned is also a criterion for recognising the right to be forgotten. More specifically, what about information which, at the time of the withdrawal request, concerns an illustrious unknown who later becomes a public figure, a politician perhaps? The benefit of accessing the information on the basis of the person's name is likely to evolve and bypasses an objective approach to timeframes. There is no doubt that if data protection measures overcome the shortcomings of the right to respect for private life, they do not solve all of the problems arising from the implementation of the right to be forgotten.

Notes:

(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, as amended by a Directive of 12 July 2002, itself complemented by a Directive of 25 November 2009.

(2) F. Nietzsche, *On the Genealogy of Morals* (1887); published in translation in France as *Généalogie de la morale* by Flammarion, 1996

(3) V. Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age,* 2009, Princeton University Press, 237p.

(4) M. Boizard (dir.), *Le droit à l'oubli*, Rapport pour la Mission de recherche Droit et justice, fév. 2015, p. 12.

(5) CJEU, Case C-131/12: L. Marino, « *Un droit à l'oubli numérique consacré par la CJUE* », JCP G 2014, 768 and JCP G 2014, p. 768. - G. Busseuil, « *Arrêt Google : du droit à l'oubli de la neutralité du moteur de recherche* », JCP E 2014, 1327. M. Griguer & D. Clarenc, *« Conditions et modalités d'exercice du droit à l'oubli numérique. - ou les apports de l'arrêt CJUE, 13 mai 2014* », C-131/12,
JCP E 2014, 1326. A. Debet, « Google Spain : Droit à l'oubli ou oubli du droit ? », Communication Commerce électronique n° 7-8, Juillet 2014, étude 13. - V.-L. Benabou & J. Rochfeld, « *Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte I : Le moteur, facilitateur d'accès, agrégateur d'informations et responsable de traitement autonome* », Dalloz 2014, p 1476. - N. Martial-Braz & J. Rochfeld, « *Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? Acte II : Le droit à l'oubli numérique, l'éléphant et la vie privée* », Dalloz 2014, p. 481.

(6) TGI Paris, interim order of 19 December 2014, Marie-France M. v Google France & Google, Inc: www.lefigaro.fr/secteur/high-tech/2015/01/16/01007-20150116ARTFIG00005-google-condamne-pour-la-premiere-fois-en-france-sur-le-droit-a-l-oubli.php. (paywall)

(7) ECHR, *Costello-Roberts v United Kingdom*, Application no. 13134, judgment of 25 March 1993, para. 36.

(8) ECHR, *Niemietz v Germany*, Application no. 13710/88, 16 December 2012.

(9) For a negative response, see Cass. 2nd civ., 24 November 1975, Dalloz 1976 somm. 36: there is a discretionary power to oppose the re-disclosure of private fact. For a positive response: CA Paris, 13 March 1986 Dalloz 1986 IR 445 obs. Lindon, known aspects of the life of Y. Noah.

(10) Cass. 2nd civ., 22 May 1996, JCP 1996, IV, 1571. 1st civ. 30 May 2000, CCE 200, 801, obs. A. Lepage; 3 April 2002 Dalloz 2002 jur. 3164 notes and 2003 Bigot, somm. 1543, obs. Caron; Cass. 2nd civ., 3 June 2004, No. 03-11.533.

(11) T. Hassler, « *Droit de la personnalité : Rediffusion et droit à l'oubli* », Dalloz 2007, p. 2829, §8. - See also Cass. 2nd civ., 14 November 1975, Dalloz 1976, jur 241, note B. Edelman; Cass. 1st civ., 20 November 1990 ; Cass. 1st civ. 30 May 2000, Dalloz 2001, somm. 1989 obs. L. Marino.

(12) K. Blay-Grabarczyk, « *Vie privée et nouvelles technologies* », RDLF 2011, chron. n°7.

(13) ECHR, *Wieser and Bicos Beteiligungen Gmbh v Austria*, Application no. 74336/01, 16 October 2007.

(14) ECHR *Rotaru v Romania*, Application no. 28341/95, 5 May 2000.

(15) ECHR, *Peck v United Kingdom*, Application no. 44647/98, 28 January 2003.

(16) ECHR, *Khelili v Switzerland*, Application no. 16188/07, 18 October 2011.

(17) "Public information" section - Facebook Privacy Policy.

(18) Clause 2.10. "Groups" - LinkedIn Privacy Policy.

(19) A. Bensoussan, in J.P. Sueur, *Numérique, renseignement et vie privée : de nouveaux défis pour*

le droit, Rapport d'information sénat, n° 666, 27 juin 2014, p. 57.

(20) P. Trudel, « Quelles limites à la googleisation des personnes ? » *in La sécurité de l'individu numérisé, Réflexions prospectives et internationales*, S. Lacour (dir.), L'Harmattan 2010, p.52.

(21) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM/2012/011 final - 2012/0011 (COD).

(22) European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

(23) The amended proposal for a Regulation on the protection of personal data aims to be more complete, see Art. 4 (2).

(24) Art. 8 (1) of Directive 95/46/EC and the 1978 Act.

(25) Article 2 of the 1978 Act. Article 4 (3) of the proposed Regulation does not proceed with such a flagrant amendment.

(26) Art. 3, 1978 Act. See Article 4 (5) of the proposed Regulation.

(27) See in this respect Opinion 5/2009 of the Article 29 Working Party, 12 June 2009, on online social networks.

(28) Case C-131/12, conclusions of Advocate General Niilo Jääskinen, para. 29.

(29) In particular, CJEU Case C-131/12, Google Spain v AEPD and TGI Paris, 19 December 2014, above.

(30) Guidelines issued by the Article 29 Working Party, October 2014.

(31) The Advisory Council to Google on the right to be forgotten, 6 February 2015.