ISSN (online): 2014-2242 / www.cac.cat

QUADERNS
DEL CAC

Protecting personal data and social networks: media obligations

Artemi Rallo
Professor of constitutional law at the Universitat Jaume I and former director of the Spanish Data Protection Agency (2007-2011)

rallo@dpu.uji.es

Ricard Martinez
Lecturer in constitutional law at the Universitat de València. Former coordinator of the Studies Area of the Spanish Data Protection Agency (2007-2011)

martiner@uv.es

Abstract
Social networks present a new scenario for citizen engagement and for defining a new model of the citizen-media relationship but, in order to operate in this medium, it's essential to take into consideration the data protection regulations in force. This article explores both the basic principles governing this area for the media and for social network users, as well as the conflicts that may arise from inadequately exercising freedom of expression.

Keywords
Social networks, privacy, data protection, freedom of expression, right to information.

Resum
Les xarxes socials presenten un nou escenari per a la participació ciutadana i per definir un nou model de relació entre ciutadans i mitjans de comunicació, però per operar en aquest mitjà és fonamental tenir en compte les normes vigents en matèria de protecció de dades. Aquest article explora tant els principis bàsics que regeixen aquesta matèria per als mitjans de comunicació i per a les persones usuàries dels espais en xarxes socials, com els conflictes que poden derivar d'un exercici inadequat de la llibertat d'expressió.

Paraules clau
Xarxes socials, privacitat, protección de dades personals, llibertat d'expressió, dret a la informació.

1. The media on social networks

Social networks[1] probably constitute the greatest new thing in the last decade for the media as they provide an interactivity that had been unimaginable until very recently. Traditionally radio was the medium that could regularly open up the microphones in real time to listeners. But this depended on the time available on the programming grid and the nature of the programme. Today, any medium worth its salt has set up a social network, either as a corporation or by opening up its most significant programmes to user interaction.

The possibilities of putting your followers centre stage multiply through this procedure, ranging from real-time conversation to provocation. Interaction on social networks therefore helps to integrate users within the programme's dynamic, boosting their loyalty, taking the pulse of public opinion in real time and, given the viral nature of these media, multiplying the impact of each broadcast.

In addition to the phenomenon of social networks is the impact of the so-called *blogosphere* which actually pre-dates them.[2] A opinionated citizen journalism (which is not always thorough) has been born and traditional media have striven to incorporate blogs on their own internet sites, either directed by their professionals or open to citizens.

At least two questions arise in this context from a legal point of view. What regulatory requirements are imposed on media companies that decide to set up a social network (here we will essentially focus on the fundamental right to data protection)? And, secondly, how will conflicts be tackled related to the publication of information or opinions by users themselves?

2. Data protection on social networks

To apply data protection rules it is fundamental to clearly understand the context. As noted by Castells,[3] the evolution of the internet encourages communities to be formed, both by transferring pre-existing social groups to the virtual world and also by

creating worldwide interest groups. Moreover, a large number of services related to these are aimed at leisure and to encouraging aspects directly related to personal or private life, such as sharing photographs, listening to music or sharing videos, or expressing opinions via brief tweets of 140 characters.[4]

There are also a number of elements of a technical nature, whose future influence is, today, unforeseeable. Firstly, ubiquity is one of the most notable characteristics of internet services. Mobile phones[5] have become a complete manager and organiser with functions that range from personal agendas to computer-controlled management in the so-called "internet of things",[6] including the adoption of decisions based on added value services such as GPS. The telephone is now a space for leisure and shared play, a tool to access social networks and a provider of access to interactive digital TV services.[7]

On the other hand, also from a technological point of view, the web universe is no longer passive but has become a highly dynamic social space. Users can express their opinions, obtain the opinions of others and show themselves as they are. It is a complex environment in which applications are not always the main provider[8] and users can be both betatesters and developers at the same time.

Web 2.0 therefore goes much further. It is not merely a series of more or less advanced programming resources but entails the birth of a social universe belonging to the network society and populated by communities that can move from what is closer to any kind of horizontal grouping (professional or social groups), vertical grouping (teamwork spaces) and even "informal" grouping without the limits of space or time. That is probably why people say Web 2.0 "is an attitude and not precisely a technology".[9]

2.1 Identity is the core element

In the information society, the currency is personal information.[10] As everyone knows, when someone surfs the internet, they leave an economically profitable trail. Thanks to the internet's operational routines (the IP tracking, basic information regarding the applications stored on our computers, cookies and browser logs), profitable user profiles can be produced to establish general browsing profiles with a certain market value.[11]

Following a browser trail, even without identifying the user specifically, provides extraordinarily valuable information if this is contextualised. Users unconsciously reveal preferences of all kinds; indicate what matters interest them, which graphics attract them or which publication they prefer. These electronic fingerprints are used to facilitate browsing and make it quicker, to present advertising in a certain way and carry out market studies, or to offer clients that have been identified personalised services adapted to how they surf the internet.

Whereas the internet presents a challenge in terms of protecting private life from the point of view of the basic and "traditional" way it works, this becomes more complex with regard to social networks, where generic profiles of a user or fictitious identities are not enough. In order to be effective on a social network, to achieve its aims, an individual must identify him or herself. And in this context identity is extremely valuable because, thanks to this, the information, message or advertising can be personalised. There is the capacity to establish or identify circles of trust[12] and, through this, the viral nature of messages multiplies the efficiency and effectiveness of the processing.

In no way should we doubt the contribution of social networks to public debate; the recent examples of democratisation in countries in North Africa are proof enough of this. But this does not mean that the actions of providers and users themselves should not be subject to rules.[13]

Consequently, the first question we should ask ourselves is whether there are principles that can be applied to the internet and to social networks in particular. And the answer is in the affirmative. The issue here, essentially, is therefore not whether basic applicable principles exist, as they evidently do, but rather whether they are truly taken into account in the initial design of the applications.[14]

2.2 Applying rules regarding data protection

Processing personal information constitutes a key element in social networks. And this is the case both from the perspective of the provider of services, whose business is based precisely on the benefits produced by exploiting this information, as well as from the perspective of users, who display their information and thereby expose themselves personally and professionally. Consequently, the right *par excellence* in this context must be the right to data protection.

2.2.1 The Lindqvist standard

Without any doubt, the case of Bodil Lindqvist provides a top level reference when attempting to establish criteria to apply data protection rules to social networks.[15] In this respect, it can be said that the Court of Justice has clearly defined the criteria to be followed in the case of personal data being processed on a website.

It is important to remember that behaviour consisting of publishing a photo, video or written text on a social network does not differ at all in material terms from the Lindqvist case: it is exactly the same situation. Technology has merely advanced and this can now be done without any prior technical knowledge and in a cooperative environment. In the Lindqvist case, the Court of Justice concluded that the conditions had been met to apply Directive 95/46/EC, in other words:

1. That processing existed.

> "27. The answer to the first question must therefore be that the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes 'the processing of personal data wholly or partly by automatic means' within the meaning of Article 3(1) of Directive 95/46/EC".

To this end, it referred to the processing categories that (and we should stress this) include disclosure by transmission and dissemination, actions that fall within the concept of transfer.

> "25. According to the definition in Article 2(b) of Directive 95/46, the term "processing" of such data used in Article 3(1) covers "any operation or set of operations which is performed upon personal data, whether or not by automatic means". That provision gives several examples of such operations, including disclosure by transmission, dissemination or otherwise making data available. It follows that the operation of loading personal data on an internet page must be considered to be such processing".

2. That the exception of private life was not applicable.[16]

> "47. That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people".

3. That the conflict between the right to data protection and the freedom of expression or right to information must be resolved by the competent authority or national judge.

> "90. The answer to the sixth question must therefore be that the provisions of Directive 95/46 do not, in themselves, bring about a restriction which conflicts with the general principles of freedom of expression or other freedoms and rights, which are applicable within the European Union and are enshrined *inter alia* in Article 10 of the ECHR. It is for the national authorities and courts responsible for applying the national legislation implementing Directive 95/46 to ensure a fair balance between the rights and interests in question, including the fundamental rights protected by the Community legal order".

Consequently, if we literally apply the conclusions of this case to the "wall" of a social network, it's evident that, under certain conditions, there will be processing subject to the Directive. And the same thing happens when a photograph is tagged or a video uploaded concerning identified or identifiable people.

In practice, as we will now see, the exception of *private life* is only applicable when the space on the social network is configured in such a way that it is only visible to a group of friends and is expressly authorised. If not, the Lindqvist case would apply fully.

2.2.2 The Opinion of the Article 29 Working Party

In Opinion 5/2009 on online social networking,[17] the Working Party establishes the conditions for applying Directive 95/46/EC[18] based on the consideration that, in a legal sense, social networks are information society services. It is evident that, in order for this kind of service to work, personal data need to be processed firstly in the registration and then to configure the user's profile. On the other hand, and since the ultimate purpose of a social networking site is to interact with other users, each of them provides information in the form of descriptions, opinions, photographs, etc. and the social networking site provides them with tools (lists of users, private messaging, email, etc.) that facilitate this and require some kind of processing to be carried out.

From this point of view, there are no doubts regarding the applicability of the Directive. For this reason, the Working Party focuses its efforts on thoroughly analysing each of the elements of this processing. Along these lines, there is one aspect that is in no doubt: the Directive's provisions regarding data protection apply in most cases to the providers of the social networking services, even when their head office is outside the EEA.[19] Nevertheless, the complexity of this kind of service means that criteria must be established to identify other possible responsible parties. These would be external providers of applications when they process data and could also be users themselves under certain conditions:

- When the social networking site is used as a collaboration platform for an association or company.
- Secondly, according to the Working Party, when access to profile information extends beyond self-selected contacts, in particular access exceeds the personal or household sphere when all members within the social networking service can access a profile or when the data can be indexed by search engines. Equally, if users take an informed decision to extend access beyond their self-selected "friends", they assume the responsibilities of a data controller. In practice, the same legal regime is applied as when any person uses other technology platforms to publish personal data on the internet.
- Lastly, the application of the household exemption is also constrained by the need to guarantee the rights of third parties, particularly with regard to sensitive data.

Finally, the Working Party repeats that there may be cases in which the household exemption does not apply but where rights prevail such as the freedom of expression, the right to information or freedoms of artistic or literary creation. Similarly, the application of general provisions of national civil or criminal law cannot be excluded.

2.2.3 Contributions by the Spanish Data Protection Agency

The Spanish authority has carried out several actions in this area, promoting and taking part in studies,[20] issuing reports and applying the disciplinary regime. We should review those documents that in some way help to define the institution's position in this matter. In this respect, the document entitled *Recomendaciones a usuarios de internet 2009* [Recommendations to internet users 2009] should be read attentively. This document represents an interesting change in perspective. In previous editions, users were conceived as passive subjects whose data were processed. However, the recommendations

contained in points X and XI of the 2008 text reveal a new focus. Firstly, there is the initial premise that normal use of Web 2.0 resources may determine the processing of data and images of people who have not consented and the authority recommends taking special care in this area.[21]

On the other hand, the text also covers users who consciously use Web 2.0 resources for informative purposes and, referring to this, the *Recommendations* of point twelve are very concrete and clearly aimed at raising the awareness of users regarding the conditions for exercising the right to information on the internet.[22]

In addition to this promotional activity, the Agency has also adopted decisions with legal significance insofar as its reports and decisions serve to guide the action of providers. It has issued a report on this area, 615/2008,[23] regarding such a common issue as the actions of individuals who share, via their websites, photos of their children carrying out out-of-school activities.

Firstly, the report analyses if the conditions exist to apply the household exception. Regarding this aspect, it notes two conclusions. The first, with reference to the Bodil Lindqvist case, is that this exception does not apply because we are not in the area of the private or family life of individuals when information is projected beyond the domestic sphere, something that, with images on the internet, is established as "there is no limitation to accessing these". A second criterion, in line with the aforementioned Opinion 5/2009, when considering which evidence points to the existence of processing subject to the Directive, concludes that "for us to be considering the exclusion established in article 2 of the Spanish Data Protection Act, what is relevant is the fact that this is an activity that befits a personal or family relation, comparable to what might be carried out without using the internet, so that those cases do not apply in which publication is carried out on a page that is freely accessible by any person or when the high number of people invited to contact this page is indicative of the fact that this activity extends beyond what is appropriate for this sphere.

Consequently, the application of what has been said so far related to this case supposes that the Spanish Data Protection Act shall not apply when the activity of the consulting party is limited, under the terms in question, to the personal or family sphere. On the other hand, when the exclusion established in article 2 of this Act does not apply, i.e. when the activity exceeds this sphere, this rule shall be applicable and consent must be obtained from the parents or from the minors themselves when they have the capacity to give it, both to obtain the image and to publish it on the website, insofar as the latter constitutes a transfer or disclosure of data of a personal nature as defined by article 3 j) of the Spanish Data Protection Act, i.e. as 'Any disclosure of data carried out by a person other than the interested party'".

In conclusion, the configuration of the web space is highly relevant for the purpose of determining the applicability of data protection legislation.

Lastly, we should refer to different opinions given within the context of disciplinary procedures and/or protection of rights that affect typical Web 2.0 services. Firstly, there are those cases where images are issued on portals that offer video files. In this area, the Spanish Data Protection Agency (AEPD) has employed the doctrine of article 29 of Working Party Opinion 4/2004, of 11 February, regarding the processing of personal data via video camera surveillance, and has concluded that "data comprising of image and sound are personal". The identifiable nature of these data "can come from a combination of the data with information from third parties or even from applying, in the individual case, specific techniques or devices". Based on this premise, it concludes that:

> "The recording and reproduction of images from passers-by in the street, which constitute data of a personal nature, and their publication on *"YouTube"*, accessible by any internet user, is subject to the consent of the data subject, in accordance with that established by article 6.1 of the Spanish Data Protection Act".[24]

This position has been further defined and adapted to the reality of the internet by prioritising the exercise of the right to cancel as a means of resolving conflicts, reserving disciplinary procedures for more serious cases.[25]

2.3 Recommended actions

Given the statements by courts and authorities on the protection of personal data, one preliminary conclusion seems evident: a medium that opens up a space on Facebook must comply with some basic normative principles in this area.

Having studied six of the main media,[26] and excepting any possible author error, only one of these media -Cadena SER- has any kind of rules[27] for its users:

> "Rules of participation
>
> The aim of the Facebook pages managed by Cadena SER is to establish a direct relationship between the radio station and its different programmes and fans.
>
> To achieve this, the following rules of participation are established, in addition to the rules of Facebook. The latter can be consulted at http://www.facebook.com/terms.php?locale=EN:
>
> - All opinions are welcome but avoid insults and language that incites hatred, discrimination, that promotes illegal activities, that is offensive, racist, violent or xenophobic. Publish your opinion but respect the rest of the users and Cadena SER.
> - Write your comments just once and avoid using capitals, which are considered to be shouting on the internet. Abusive writing will be treated as spam.
> - In the case a subject is put forward for debate, keep to this subject. The internet has many other places where you can discuss whatever you want.
> - The Facebook pages managed by Cadena SER do not accept advertising of companies, events of any kind or political propaganda. Nor the promotion of other Facebook groups or pages or other social networks that do not

belong to Cadena SER or other companies in the Prisa Group.
- Do not share content protected by copyright without the copyright holder's permission.
- Do not publish personal data, as they will be visible to all visitors.[28]

The team administering the Facebook pages managed by Cadena SER reserves the right to erase any message or content that does not comply with these rules or to block any users if they repeatedly violate them, and is not liable for any breach or for the consequences this may involve".

As can be seen, these are the policies of use for a forum and they only allude vaguely to the protection of personal data.

However, if we consult the space produced by the Spanish Data Protection Agency[29] in order to hold an international conference, we can read the following information:

"When you become a fan of this page you consent to the following: 1) to your personal data being processed in the Facebook environment in accordance with its <http://www.facebook.com/policy.php?ref=pf> privacy policies; 2) the AEPD accessing the data contained in the fan list; and 3) to news published on the event appearing on your wall.

The AEPD will not use the data for other purposes nor to send additional information. If you want to withdraw, you merely have to click on the hyperlink that appears bottom right "Unlike". You can exercise your rights to access, rectify, cancel or oppose at any time by sending a written document to Agencia Española de Protección de Datos, Secretaría General, C/ Jorge Juan no. 6, 28001 Madrid or by sending an email to privacyconference2009@agpd.es, accompanied by a photocopy of the official document that identifies you. Should you exercise your rights by email, the document must be digitally signed in the message or a scanned official document attached.

In the context of this processing, you must take into account the fact that the Spanish Data Protection Agency can only consult or withdraw your data as a fan. Any rectification of the data must be carried out by yourself by configuring your user. Email address: ciudadano@agpd.es".

What is the reason for this significant difference? It is evident that, when a company acts on a social network, it must comply with the provisions of the law in force.[30]

We can differentiate between different scenarios, although the most common is when a user registers on the most widely used sites, i.e. Facebook, Tuenti, Twitter and possibly YouTube. This is a hybrid situation as, on the one hand, the organisation is acting as just another user of the social network and, on the other, it assumes legal liabilities for the action carried out. So, when a page is opened on a social network, the organisation will act as what the Spanish Data Protection Agency and jurisprudence have defined as a *controller*:

"Also resulting from the repeated sections of art. 3, as has already been stated, is the differentiation of two responsible parties according to whether the power to decide is directed at the data file or the data processing per se. So, the file controller is the body that decides to create the file and its application and also its purpose, content and use; i.e. the body that has decision-making power over all the data recorded in this file. The data controller, however, is the body that determines the specific activities of a certain data processing, albeit in a specific application. This covers all those cases where the power to decide must be differentiated from the material performance of the activity involved in the processing".[31]

As a consequence of the aforementioned ruling, article 5 of Royal Decree 1720/2007, of 21 December, approving the Regulations for implementing Organic Act 15/1999, of 13 December, on the protection of data of a personal nature (RLOPD), has defined this figure as:

"q. File or data controller: natural or legal person, of a public or private nature, or administrative body, that alone or together with others takes decisions regarding the purpose, content and use of the processing, although it may not materially carry this out. Bodies without legal personality can also be file or data controllers when acting as differentiated subjects."

Consequently, the circumstance defined in the ruling and precept occurs in this case. This is processing in which the user, when opening his or her account, does not have any control over the file owned by the social network. As a result, the obligations resulting for the organisation regarding compliance with the Spanish Data Protection Act are limited and, for example, there is no duty to register a file or to take out a data access contract on behalf of third parties.

It should be assumed that, in this kind of case, use is limited exclusively to joining the social network and using the tools on it and there is no decision-making capacity regarding the structure, arrangement or material management of the data other than that of the social network. Moreover, other conditions must be met to be able to state that a body is acting merely as a user:
- Behaving as a user that interacts in the social network system.
- Not incorporating personal data in own resources.
- Not entering into any agreement regarding the provision of services to develop or maintain the space with the social network provide.
- Not entering into any agreement with the provider regarding additional services, such as an analysis of the behaviour, tracking or production of user profiles, associated or not with the issuing of behavioural advertising.[32]

In this case, in order to ensure suitable compliance with the Spanish Data Protection Act, the medium must:
- Comply with the duty to inform so that, as there is processing, the principles and obligations are respected resulting

from article 5 of the Spanish Data Protection Act. The following is therefore recommended:
- Place brief information in the space of the account provide by the social network with the basic information on the identity and location of the person responsible, the intended purpose and how rights are exercised.
- Set up a welcome procedure for new friends with an email message that includes this information.
- Hyperlink to corporate privacy policies.

And, as stated by the Article 29 Working Party in Decision 5/2009 mentioned previously, particularly provide information on:
- Usage of the data for direct marketing purposes.
- Possible sharing of the data with specified categories of third parties.
- The use of sensitive data.
- Integration within the environment of third party applications that record and/or process the data of "friends" when this integration depends on the wishes of the user responsible for the account.

Secondly, it should be noted that the legitimate cause for processing personal data in this area is consent, as in article 6 of the Spanish Data Protection Act.[33] It should be understood that this consent is given when someone is asked to "become a friend of" or when they accept an invitation. The following should be taken into account:
- Consent only affects the data of the person joining, never those of third parties related to the "friend" whose profile is open.
- The possible existence of exceptions to the consent rule must be examined case by case and fully respecting the regulation. Request?
- An open profile "does not imply consent". It should be remembered that, in accordance with that established by the Spanish Data Protection Agency in its Report 0342/2008, the internet and therefore social networks are not publicly accessible sources.
- Including data, such as email addresses, in the systems themselves constitutes processing subject to the Spanish Data Protection Act and the fact that these data are accessible in a social network environment does not necessarily legitimise their processing.
- The guarantee of the rights of "friends" is of limited content. The rights to access, rectify, cancel and oppose processing apply. Notwithstanding this:
  - The content of the right to access will be defined by the possibilities offered by the network and by the capacity to access information from the profile of each specific user. Consequently, it will practically be enough to offer, to anyone exercising this right, images of the screens showing which data is accessed.
  - The right to oppose, rectify and cancel will be modulated. The data controller should comply with this regarding those aspects of application that are under its control, such as modifying or eliminating a comment from the wall itself. The rectification of aspects related to the user's profile is normally exercised before the provider. Cancellation and opposition, when this consists of "unfriend", can be exercised by both parties.
- There must be limits regarding the use of data. The principle of purpose constitutes an impassable limit and must be defined by:
  - The social network's conditions of use, which might prohibit specific uses.
  - The information available and effectively provided in "Add Friend".
- The principles of security and secrecy apply for any user regarding the data controller but must be adapted to the specific conditions of the environment and will only affect any processing effectively carried out.

3. Social network user opinions and information

To complete our examination of issues related to the use of social networks, we should also look at what is undoubtedly the essential aim of these sites: to encourage users to express their opinion freely.

In principle, and given the nature of the environment, in other words space on a medium related to citizens exercising the rights of article 20 of the Spanish Constitution, the conditions exist to exclude the application of the rules protecting personal data.[34] In this respect, the Spanish Data Protection Agency has usually recognised the prevalence of the rights of article 20 of the Spanish Constitution.[35] Notwithstanding this, it should be noted that, at least in one case, the High Court has considered the right to data protection prevalent, when considering that the information published did not require the accompaniment of the image of one of the victims of a terrorist attack, applying a judgement of proportionality.[36]

When the body processing personal data is a user on his or her own wall, the Agency usually redirects the question to the procedure to protect rights of article 18 of the Spanish Data Protection Act and orders the data to be cancelled by the person responsible for the social network.[37]

All these criteria help us to comprehend the legal nature of the opinions posted on a medium's wall based on two types of judgement. Firstly, a judgement concerning the content will help us determine whether the user is exercising his or her right to inform or express his or her opinion and whether the conditions exist for this right to prevail over the rights of third parties. In other words, whether the information is based on true facts or perceived as such, and has public relevance to shape public opinion. The second criterion is based on determining the liability of the person owning the wall. Here the Agency's point of view is framed within the line defined by Act 34/2002, of 11 July, on the services of the information society and electronic com-

merce, and stated by Opinion 5/ 2009, considering the owner of a social network as the provider of information society services.

This is substantially different from the liability of the publishing body, for example, in the traditional "letters to the editor". Spain's Constitutional Court Sentence 3/1997 summarises very accurately the criterion of the court that, based on the fact that there is a prior examination of the letters published, requires in some way the application of a double filter regarding the identity of the person sending the letter and the relevance of the content when identification is not reliable. It therefore considers the publishing body is responsible for this content.[38]

In short, and using elementary analogue reasoning, in those internet spaces where content is directly developed by the owner and space is provided for participation, liability would be focused on verifying the identity of the reader publishing his or her opinion. This doctrine would not be applicable in the context of a social network since the way in which it functions prevents, today, any identification and, moreover, the speed when publishing comments and the number of these comments makes it impossible to control, except after the event.

For this reason, as stated by Opinion 5/2009, in this case there is the provision of an information society services subject to that established in Act 34/2002, of 11 July, on information society services and electronic commerce. Consequently, when Spanish legislation applies, the liability of the provider regarding this document must be governed by articles 16 and 17 of this Act. Two elements must therefore occur for there to be liability:

- Effective knowledge. This shall occur when a claim is notified by means of the social network's complaints space or when an authority, such as the AEPD, demands some kind of action.
- Absence of diligence in removing the information.

In any case, this is a complex situation that transfers some ethical responsibility to the media. As democratisation has occurred through the extension of the possibility to exercise the freedom of opinion for any citizen, and as the media themselves provide these spaces on social networks, it would be most advisable to encourage the training of users via ethical codes or rules of use.[39]

This is particularly necessary when specific regulations are absent. Neither Organic Act 1/1982, of 5 May, on the civil protection of the right to honour, personal and family intimacy and one's own image, nor Organic Act 2/1984, of 26 March, governing the right to rectify, offers suitable solutions to resolve these problems. Clear evidence of this is that citizens are increasingly exercising the right to cancel established in article 16 of the Spanish Data Protection Act for this kind of case.

Conflicts in this area go far beyond social networks and have spread to citizen journalism and blogs and to the so-called *right to be forgotten.* Directive 95/46/EC authorised member states to develop this area in the sphere of the media. Perhaps the time has come to insist that this development is essential.

Notes

1. This article is largely due to a previous monograph. Rallo Lombarte, A.; Martínez Martínez, R. (coord.). *Derecho y redes sociales*. Cizur Menor (Navarra): Civitas, 2010.
2. Cerezo, J.M. *La blogosfera hispana: pioneros de la cultura digital* [Online]. Biblioteca de la Fundación France Telecom España, 2006. <http://fundacionorange.es/areas/25_publicaciones/publi_253_9.asp> (Available: 19/03/2010)
3. Very graphically, Castells points out:

   "(The internet) is an extension of life as it is, in all its dimensions, and with all its modalities. Moreover, even in role-playing and informal chat rooms, real lives (including real lives on-line) seem to shape the interaction on-line."

   Castells, M. *La galaxia Internet. Reflexiones sobre Internet, empresa y sociedad*. Barcelona: Areté, 2001, p. 139. The chapter in this book on virtual communities is particularly useful to understand the capacity of networks to define community spaces (p. 137-158).
4. See <http://twitter.com/>
5. See Martínez Martínez, R. "¿Interrogantes jurídicos ante los smartphone?" *Actualidad Jurídica Aranzadi*, no. 822, p. 13.
6. See <http://www.theinternetofthings.eu/>
7. When true interactivity is produced by digital terrestrial television, the processing of personal data by this channel will multiply. Martínez Martínez, R. "Los contenidos audiovisuales en la multidifusión digital. Nuevos retos para la protección de datos personales". In: Francés i Domenech, M. (coord.). *Hacia un nuevo modelo televisivo. Contenidos para la televisión digital*. Barcelona: Gedisa, 2009, p. 83-95.
8. Particularly relevant in this respect are the findings by the Canadian authority regarding data protection in the investigations carried out on Facebook:

   148. According to Facebook's developer blog (June 4, 2009):

   "The growth we have seen on Platform has been tremendous. Today there are over 350,000 active applications on Platform from over 950,000 developers living in more than 180 countries. These range from simple applications created by single users to share with their friends to impressive businesses employing hundreds of people and reaching tens of millions of users every month and generating tens of millions of dollars of revenue. For example, close to 10,000 applications have 10,000 or more monthly active users, and more than 100 applications have more than 1 million monthly active users."

   149. When users add an application, they must consent to allow the third-party application developer to have access to their personal information, as well as that of their friends. Moreover, as CIPPIC has correctly pointed out, unless users completely opt out of all applications and block specific applications, they are not given the option of refusing to share their names, networks, or lists of friends when friends add applications. [...]

1) Facebook had inadequate safeguards to effectively restrict these outside developers from accessing users' profile information, along with information about their online friends.
2) Facebook was not obtaining users' meaningful consent to the disclosure of their personal information to application developers when either they or their friends add applications."

Denham, E. R*eport of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act. July 16, 2009*. Office of the Privacy Commissioner of Canada. PIPEDA Case Summary #2009-008
<http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm> (Available: 16/04/2010), p. 38 and 94.

9. See <http://www.maestrosdelweb.com/editorial/web2/>

10. See Alamillo Domingo, I. "La identidad electrónica en la red". In: Rallo Lombarte, A.; Martínez Martínez, R. (coord.). *Derecho y redes sociales*. op. cit. p. 37-53.

11. See SCHWARTZ, P.M. "Internet privacy and the State". *Connecticut Law Review*, vol. 32, 2000, p. 815-859.

12. In fact, this is Google's most recent proposal with its own social network, Google +:

"The first of the tools or services included is Circles, a tool that helps to create circles of people through which their members can debate, publicise and share all kinds of information only with defined groups of contacts, such as family, school friends, workmates, teammates, friends, etc.".
<http://www.puromarketing.com/16/10334/google-project-nueva-social-google-llega.html>

13. Regarding those who state that it is impossible to impose legal limits on the phenomenon of the internet, and without ignoring the fact that specific actions are required from the legislator, we must consider whether, in the context of information and communication technologies, it is necessary to modulate or adapt the rules as, in the area of the internet, regulations are not projected on instruments but on their use and design. See Trías Sagnier, J . "Informática y privacidad. ¿Se pueden poner puertas al campo?" *Cuenta y razón*, no. 63, 1992, p. 98-101.

14. Along these lines, over the last few years further studies have been carried out on the methodologies of *Privacy Impact Assessment* and *Privacy by Design*, whose aim coincides with the one stated here: providers and programmers must take into account, in their design, a priori, methods that guarantee the right of users to a private life is respected.

As Lessig has pointed out, programmers have the capacity to define operational rules for the environment that effectively act as regulations and therefore the possibility to define operational modes that guarantee compliance of the principles included in legal regulations. Lessig, L. *El codi i altres lleis del ciberespai.* Madrid: Taurus, 2001 and Lessig, L. *Code version 2.0.* Basic Books. New York: Perseus Books Group, 2006. Available at: <http://pdf.codev2.cc/Lessig-Codev2.pdf>

There are increasingly more documents in this area, although the reference methodology is that of the British Information Commissioner's Office.

- ICO. Privacy Impact Assessment (PIA) handbook (Version 2). 2009.
<http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html> (available: 22/03/2010).
- Homeland Security (USA) Privacy Impact Assessment EINSTEIN Program.
<http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf> (available: 22/03/2010).
- Treasury Board of Canada Secretariat. Privacy Impact Assessment - Policies and Publications.
<http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist-eng.asp> (available: 22/03/2010).
- Privacy by Design http://www.privacybydesign.ca/.

Lastly, see Warren, Adam. "Privacy Impact Assessments: the UK experience". *31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. Madrid, 4-6 de noviembre de 2009*. <http://www.privacyconference2009.org/program/Presentaciones/common/pdfs/adam_warren_speech_en.pdf>

15. As will be remembered, Ms. Lindqvist was a Swedish catechist who, at the end of 1998, used her personal computer to set up various websites so that her fellow parishioners preparing for their confirmation could easily obtain information that might be useful. The pages in question contained information about Mrs Lindqvist and 18 colleagues in the parish, sometimes including their full names and in other cases only their first names. Mrs Lindqvist also described, in a mildly humorous manner, the jobs held by her colleagues and their hobbies. In many cases family circumstances and telephone numbers and other matters were mentioned. She also stated that one colleague had injured her foot and was on half-time on medical grounds. After being fined and appealing, the Swedish court consulted the Court of Justice regarding the conditions for applying Directive 95/46/EC.

Ruling by the Court of Justice of 6 November 2003 on case C-101/01.Request for a preliminary ruling presented by Göta Hovrätt (Göta Court of Appeal).
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:007:0003:0004:EN:PDF>

16. Personal data protection rules do not apply, as established by article 4 of the Regulations implementing the Spanish Data Protection Act, to processing "carried out or maintained by natural persons while carrying out exclusively personal or household activities.

Processing shall only be considered as related to personal or household activities when it is related to activities belonging to the context of individuals' private or family life".

17. Article 29 Working Party. *Opinion 5/2009 on online social networking*. (01189/09/EN WP 163). (Available 31/03/2010)

18. Directive 95/46/EC, of 24 October, on the protection of indi-

viduals with regard to the processing of personal data and on the free movement of such data.

<http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm>

19. The party has pointed out that there is processing that cannot be carried out without resorting to using a user's own computer, in general by employing cookies, so that media would be used that are in European territory. See WP148, Opinion 1/2008 on data protection issues related to search engines.

20. Agencia Española de Protección de Datos. INTECO. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Madrid, 2009.

21. Users are guided by two specific recommendations:

- "Take particular care when publishing audiovisual and graphic content on your profiles, especially if images related to third parties are going to be uploaded.
- Do not label audiovisual content with the real identity of the people involved or offer third party data on your site without their consent."

And a reminder:

- "When you publish a photo or write in the blog, you might be including information about other people. Regarding their rights."

<http://www.inteco.es/file/aiYG6hA575_aXKiMJlkT_g>

22. "The resources made available to us by computing and the internet allow us to carry out a lot of activities on the internet. Thanks to these, we can edit audio and video files and share them with the whole world, publish our photographs and share them, organise virtual activities, arrange dates and mass meetings and carry out citizen journalism. [...]

- Do not publish information that does not meet the requirements of truth, public interest and respect for the dignity of people and in particular regarding young people and children.
- Do not spread rumours or unverified information.
- Rectify or remove information when someone affected justifiably requests this.
- Never publish information that endangers the family and in particular children, nor friends, neighbours, etc.
- Take special care regarding the publication of information regarding the locations where the user or a third party is at any time. This might endanger users, given that it allows possible offenders to know, at any time, where users are, what they are doing and where they are going, which might entail a serious risk to their person.
- Do not record or publish images, videos or any other kind of recording without the consent of those concerned.
- Do not process the personal data of third parties, especially when disclosed to third parties without the knowledge or consent of those affected.
- When applicable, comply with the obligations of the Organic Data Protection Act.
- Inform users about their duties in the procedures of subscription and registration.
- Draw up and publish ethical codes that guarantee minimal rules of action for users or communities on social networking sites."

23. <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdfs/2008-0615_Inaplicaci-oo-n-LOPD-a-actividad-de-particulares-que-comparten-fotos-de-sus-hijos-a-trav-ee-s-de-Internet.pdf>

24. See PS/00479/2008, available at <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2008/common/pdfs/PS-00479-2008_Resolucion-de-fecha-30-12-2008_Art-ii-culo-6.1-LOPD.pdf>.

25. "It's true that the reality of the internet requires an interpretation of the principle of consent that avoids a strict application that would paralyse it or turn it into a network brimming with violations of the personal data of millions of people that are easily accessible by merely using a search engine and of data for which prior consent is not required.

It is therefore not convenient to interpret the requirement for consent in a maximalist way but the principle must be considered which, when legal regulations offer various solutions and all other alternative formulas have been exhausted, is the most appropriate, if this is possible, for which reason the use of the right to cancel data with the aim of stopping the processing of personal data must prevail. This procedure would enable the speedy correction of the data included in order to redress this situation prior to defence due to violation or to the bringing, if applicable, of a disciplinary procedure, which would be punitive in nature if this were not made to disappear.

This premise must not prevent the fact that, in specific cases - particularly sensitive data or rights affected of particular seriousness, as well as breach of professional secrecy - it may apply to use the disciplinary procedure in order to sanction especially serious conduct that does not come under the internet rules, as occurs in the case brought". See PS/00508/2008.

26. Cadena SER, Cadena COPE, Onda Cero, Televisión Española, Telecinco and laSexta.

27. <http://es-es.facebook.com/cadenaser?sk=app_214923178538944>

28. Underlined by the authors.

29. <http://es-es.facebook.com/AEPD?sk=info>

30. See Vilasau Solana, M. "Privacidad, redes sociales y el factor humano". In: Rallo Lombarte, A.; Martínez Martínez, R. (coord.). *Derecho y redes sociales*. op. cit. p. 66-71.

31. See the Decision of 5 June 2004, of the Third Administrative Appeals Chamber of the Final Court of Appeal on differentiating between the file controller and the data controller, confirmed by the Decision of 16 October 2003 of the First Administrative Appeals Chamber of the High Court, given for appeal number 1539/2001. Available at: <http://bit.ly/oDvST6>.

32. Behavioural advertising is based on the continual observation of individuals' behaviour. Its aim is to study the characteristics of this behaviour via actions (repeated visits to a specific site,

interactions, keywords, production of online content, etc.) to develop a specific profile and thereby provide users with advertisements tailor-made to the interests inferred from their behaviour. Behavioural advertising normally involves the collection of IP addresses and the processing of unique identifiers (using cookies). The use of these devices helps to isolate users, even though their real names may not be known. Moreover, the information gathered refers to the characteristics or behaviour of a person and is used to influence this specific person. This profile is accentuated when we take into account the possibility that profiles are linked at all times with directly identifiable information provided by users, such as the information provided when registering.

We should note that here a technologically available possibility is being defined. The decision whether to use such techniques corresponds to editors, advertisers and advertising service providers.

See Article 29 Working Party. *Opinion 2/2010 on online behavioural advertising*. 00909/10/EN WP 171, available at *http://bit.ly/dsAN9F*, and Peguera Poch, M. "Publicidad online basada en comportamiento y protección de la privacidad". In: Rallo Lombarte, A.; Martínez Martínez, R. (coord.). *Derecho y redes sociales*. op. cit. p. 354-380.

33. See Arenas Ramiro, M. "El consentimiento en las redes sociales on line". In: Rallo Lombarte, A.; Martínez Martínez, R. (coord.). *Derecho y redes sociales*. op. cit. p. 117-144.

34. Another thing would be the improper use of personal data by social network users on their own walls, which in some cases might determine liabilities regarding personal data protection. For example, by publishing images or comments with personal data in a private environment of a social network without the consent of the people affected.

35. See case no. E/00871/2005, <http://bit.ly/nx7oMt>.

36. "The image, therefore, is a piece of information that comes under Organic Act 15/99 but a detailed examination of the case shows that, although the images are not good quality, it can be understood that the processing of the data of the image has been excessive, taking into consideration the fact that it is not covered by the consent of those affected (there is no evidence that they were aware of the images' publication) and neither is it covered by the freedom of information and, in any case, it seems that an disproportionate use has been made of the image as personal information since the newsworthy nature of the information was sufficient without the need to include direct images of the sick people. Consequently, the hearing must continue regarding the possible use of the data of the image without justification". Sentence of 9 July 2009, by the First Administrative Appeals Chamber of the High Court, given in appeal number 325/2008.

37. See proceedings no. TD/00690/2009. Available at <http://bit.ly/n9DwdR>.

38. "C) In particular, regarding those cases when the medium authorises the publication of a text from a person entirely unconnected thereto, we have specified that "the duty of diligence of the newspaper's Director involves the verification of the person's identity who figures as the author of the letter, before authorising its publication", as is habitual practice. Adding that, if this specific diligence were not possible, "the following would not be duly determined, respectively: the exercise of freedom of expression of a person unrelated to the medium, which this makes possible by publishing the letter, and the right related to the newspaper to inform its readers of this opinion"; and this would also suppose "that the right of readers to receive true information would be affected, guaranteed by art. 20.1 d) of the Spanish Constitution". Verifying the identity of the person who has written the text therefore helps "this person to assume his or her liability should the letter constitute an offence", given that, otherwise, "the door would be opened to the creation of spaces immune to possible violations of the constitutionally guaranteed right to honour" [STC 336/1993, legal ground 7, B)].

3. However, the above doctrine does not necessarily result in the decision that the action of the medium authorising the publication of a "letter to the editor" from a person that is not identified involves, in all cases, the former's liability and that, for this purpose, verification would be enough that this specific diligence has not existed. When the issue is to hear a possible violation of the right to honour of a third party via an unrelated document published by the medium, what is decisive is not only the fact of the publication but to determine, attending to the content of this document, whether this fundamental right has been violated or not.

In effect, when authorising the publication of an external text whose author has been previously identified, it is the latter who will assume any liability that may result from this if its content injures the honour of a third party. However, the situation is very different if the external text is published without the medium knowing the identity of its author, as in this case it does not constitute an action that may be divorced from that of its publication by the medium, in accordance with the doctrine stated in STC 159/1986. So that, on authorising the publication of the text in spite of not knowing the identity of its author, it must be understood that the medium, because of this, has assumed its content. This entails a dual consequence: firstly, exercising the freedoms recognised and guaranteed in art. 20.1 this will have to be examined, exclusively, in relation to the medium, given that the writer of the text is unknown. Secondly, whether the medium will ultimately be liable for the text if its content has exceeded the constitutionally protected sphere of the freedom of information and, if applicable, freedom of expression, injuring the honour of third parties or, alternatively, if it has been respected". STC 3/1997.

39. See Agencia Española de Protección de Datos. INTECO. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Madrid, 2009, p. 92.