Received: 08-01-2013 / Received: 08-02-2013
Accepted: 23-03-2013 / Published: 01-09-2013

DOI: http://dx.doi.org/10.3916/C41-2013-20

● Lucía Tello
Madrid (Spain)

Intimacy and «Extimacy» in Social Networks. Ethical Boundaries of Facebook

Intimidad y «extimidad» en las redes sociales. Las demarcaciones éticas de Facebook

ABSTRACT

The current paper aims to analyze how certain Facebook settings, model of new Information and Communication Technologies (ICT), have turned into an infringement of some existing privacy Ethical principles. This totally changed and modern paradigm has its clearest expression in recent Web 2.0, and omnipotent Communication Technology, and implies the reconsideration of each Ethical Principles, especially those related to Intimacy and Image Protection. Our research explains not just how these areas are affected by technological changes but also the way these imperative ethical principles are violated because users ignorance and confidence. This carefree attitude and the increasing communicative relevance have given networking precedence over Intimacy protection. The result of this action has been denominated «Extimacy» according to the author Jacques Lacan, a concept which can be translated as public Intimacy through networking activities, namely, exposed Intimacy. The goal we aim to achieve is to illustrate the different ways our Privacy can be damaged by some Facebook measures (as Privacy Policies Change, collecting tendencies of consumption, the use of private data and revealing users confidence). Likewise these arguments will be endorsed by international researches focused on Facebook privacy violations, which we are going to expose to understand how citizens can carry out different actions to defend our Intimacy and Image Rights.

RESUMEN

El presente trabajo analiza cómo ciertas herramientas de Facebook, modelo de las nuevas tecnologías de la información, han derivado en la vulneración de algunos planteamientos éticos vigentes hasta el momento. Este paradigma comunicativo que encuentra su máxima expresión en las redes sociales y la tecnología 2.0, implica un replanteamiento de los principios de la ética informativa relativos a la salvaguarda de la intimidad, la protección de la vida privada y el resguardo de la propia imagen. Esta investigación estudia cómo estas áreas no solo se ven afectadas por los cambios tecnológicos y la propia naturaleza de la fuente informativa, sino por la confianza y desconocimiento de los usuarios, quienes dan primacía a la comunicación por encima de la intimidad. Este fenómeno denominado «extimidad» por Jacques Lacan, se traduce como la intimidad hecha pública a través de las nuevas redes de comunicación o intimidad expuesta. En nuestro análisis expondremos los resortes a través de los cuales se quebranta nuestra privacidad en Facebook, especialmente por medio de la captación de pautas de comportamiento, el empleo de datos derivados de los perfiles, los cambios en la política de privacidad y el reconocimiento facial, avalando su transgresión con documentación derivada de investigaciones realizadas por organismos internacionales. En resumen, analizar la vulneración de la intimidad en las redes sociales y entender qué medidas pueden implementarse para defender nuestros derechos son el objetivo de esta comunicación.

KEYWORDS / PALABRAS CLAVE

Internet, ethics, Facebook, intimacy, extimacy, social networking.
Internet, ética, Facebook, intimidad, extimidad, vulneración, redes sociales.

◆ Dr. Lucía Tello Díaz is Honorary Researcher in the Department of Journalism III of the School of Information Sciences at the Complutense University of Madrid (Spain) (lucytel1959@hotmail.com).

1. Introduction

In the Information Age the boundaries of privacy have been dissolved. Ethical principles assumed as inalienable are subject to new ways of infringement so that the majority of states do not have legal formulations for eradicating them. That happens with personal privacy, whose conventional outline has been distorted by social networking and new communication reality «as hypothesized (the majority of Facebook users) perceive benefits of online social networking as outweighing risks of disclosing personal information» (Debatin, Lovejoy & al. 2009: 100). The users seem to be unaware of the use of their private data, their searches in browsers, products they acquire or links they visit. This information is stored and used without any consent or knowledge. As we examine, Facebook technology for Information Monitoring is specifically invasive in this field. Its architecture contributes to the reduction of users' control of their privacy though some settings and measures – such as privacy policy changes, collecting tendencies on consumption, the use of private data, a new Face Recognition feature and revealing users´ confidence. This improper violation of the users´ right to privacy has forced some countries like Ireland, the United States, Canada or Germany to elaborate reports about the full implications of this contravention. Facebook users do not know where their data goes and the uses to which they are put. This personal information is not relevant because it is private but also because it provides unnoticed details to unknown people. Although «we can definitively state that there is a positive relationship between certain kinds of Facebook use and the maintenance and creation of social capital» (Ellison, Steinfield, & al. 2007: 1.161), the fact is that the risks involved in terms of Privacy exceed its benefits and violate ethical precepts currently in force.

2. Procedure, materials and method

As stated in the introduction, we observe the infringement of ethical principles of privacy and personal data/image through a content analysis of the most relevant reports carried out by international organizations. We support our results on scientific papers and press articles relating to intimacy infringement and privacy violation. We also employ reports published by states which have gone ahead, illustrating how Social Networking Sites invade users' personal privacy. Such reports have been made public by the Hamburg Office of Data Protection and Freedom of Information (Germany), the Federal Trade Commission (United States), the Privacy Commissioner of Canada and the Office of the Data Protection Commissioner of Ireland, which are going to contribute to the shaping of the outlines of privacy abuse through Social Networking Sites. In order to discover the particular characteristics of the Facebook Privacy System we employ a qualitative and deductive method, analysing different categories relating to the keywords «privacy», «intimacy» and «personal image», items that allow us to determine which categories are given priority in each country. These international organizations belong to the only four countries which have intervened in connection with Facebook personal privacy violation, in order to discover if the company guarantees any level of data security. Finally, we support our results on previous studies carried out by international researchers and published in prestigious journals such as the ARPN Journal of Systems and Software, Cyberpsychology, Behaviour and Social Networking, Journal of Computer-Mediated Communication and Harvard Business Review.

3. Social networking sites as context: the age of global communication

Human activities are necessarily social and this fact results in a conglomeration of networks which provides us with interpersonal interaction circuits. This interconnection is not a reality arisen from our present context, not in vain, trade, communication and interpersonal contact belong to our nature, although in the age of new technologies, intercommunication becomes global:

A new kind of relationships with no bounds is arising between people. Globalization is transforming our lives. This characteristic defines our current society and gives it its most distinctive feature (Javaloy & Espelt, 2007: 642).

With the Internet humanity is «increasingly interconnected» (Ehrlich & Ehrlich, 2013: 1) and that makes global communication possible. Interconnection and data transmission are now qualitative and quantitative far better than they were before. Since Tim O´Reilly defined the Online Communication model in «What is the Web 2.0. Patterns and Business Models for the Next Generation of Software», the Internet has spurred a renewed communication system that goes beyond the traditional concept of linking: «As synapses form in the brain, with associations becoming stronger through repetition or intensity, the web of connections grows organically as an output of the collective activity of all web users» (O´Reilly, 2007: 22). Therefore, connectivity is now more real than ever:

There's been a corresponding burst of interest in

network science. Researchers are studying networks of people, companies, boards of directors, computers, financial institutions –any system that comprises many discrete but connected components– to look for the common principles. (Morse, 2003: 1).

In the age of the Web 2.0 network interconnection implies a continuous feedback between people, although it also entails a constant distortion of the privacy concept by users, who judge more important to show their intimacy than to protect it:

The way we constitute and define ourselves as subjects has changed. Introspective view is deteriorated. We increasingly define ourselves as what we exhibit and what the others can see. Intimacy is so important to shape who we are that we have to show it. (Pérez-Lanzac & Rincón, 2009).

This debilitation of the introspective process was already enunciated by Jacques Lacan (1958) under the revolutionary concept of «extimacy», a term linked to the expression of once-private information through social networks:

«Extimacy» breaks the inside-outside binary and gives an external centre to a symbolic area, which produces a rupture in the very heart of the identity, an emptiness that cannot be fulfilled (Extimidad, El curso de orientación lacaniana, 2012).

«Extimacy» and the increase of data transmission in the age of Social Networking Sites have generated an enormous amount of useful personal information. In this sense:

The Internet became the Bible of publicists who track potential consumers among the most relevant online communities identifying opinion leaders and carrying out Social Media Monitoring. […] the Internet offers increasingly precise information about features and preferences of these new niches of spectators (Lacalle, 2011: 100).

These data not only inform about users´ preferences, but also reveal an important segment of their intimacy. Therefore, users' information does not only allow «to articulate and make visible their friendship networks» (Kanai, Bahrami, & al., 2012), or to establish «connections between individuals that would not otherwise be made» (Boyd & Ellison, 2007: 210), but also provides «some predictive power» (Jones, Settle & al., 2013) about tendencies and attitudes. Even when «some individuals prefer to keep intimate details such as their political preferences or sexual orientation private» (Horvát, Hanselmann & Hamprecht, 2012), the information revealed by his/her contacts can divulge what the user prefer to conceal. Although many people consider that the most serious risk of the Social Networking Sites lies in their capability to «facilitate behaviours associated with obsessive relational intrusion» (Marshall, 2012: 521), another unnoticed threat lies in their own formulation and their unauthorized compilation of personal information.

> Tthe majority of Facebook users perceive benefits of online social networking as outweighing risks of disclosing personal information. The users seem to be unaware of the use of their private data, their searches in browsers, products they acquire or links they visit. This information is stored and used without any consent or knowledge. As we examine, Facebook technology for Information Monitoring is specifically invasive in this field. Its architecture contributes to the reduction of users' control of their privacy though some settings and measures – such as privacy policy changes, collecting tendencies on consumption, the use of private data, a new Face Recognition feature and revealing users´ confidence.

3.1. Social networking sites and Facebook

Users' remoteness and a constant technological renewal define Social Networking Sites: «The social conversation propelled by a deep and continue communication technologies metamorphosis is becoming

more and more prominent on the Web 2.0» (Ruiz & Masip, 2010: 9). In this context appears Facebook, the most prominent Social Network Site on the Internet. Although GeoCities or MySpace were consolidated sites, Facebook (created by Mark Zuckerberg in 2003) was implanted transforming the concept of interaction: «users create, share and consume information in a very different way than before» (Yuste, 2010: 86), and this situation has «created a favourable atmosphere for making intermediary disappear –users have direct access to information sources– and for generating an abundant content of a diverse origin» (Yuste, 2010: 86).

The current erosion of users´ privacy from numerous fronts is perturbing, the cause stems from three vast forces: the first one is the technology itself, which makes possible to be on anyone's track with instantaneous precision […] The second one is the pursuit of profits, which makes companies monitor consumer's tastes and habits in order to personalize advertising. At last we find Governments which collect many of these data in their own servers.

According to the report «Spanish Habits and Social Networking», Facebook has replaced the rest of Social Networks in our country (Libreros, 2011), being used by a 95 percent of users (followed by YouTube, Tuenti and Twitter), who utilize it for sending private messages (60%) and public messages (50%), for sharing and uploading pictures (37%), for updating their profile (32%) and becoming a fan or to follow commercial trademarks (26%) (Libreros, 2011). These particular five activities will be relevant in order to categorize users, to discover tendencies and to establish parameters of their profiles.

3.2. Infringement of the right to privacy and data protection

To be connected to the Internet and to have a power source are the two required elements for accessing our personal information from all over the world. New communication technologies offer an uncontrollable data reproducibility and they allow accessing this extremely up-to-date information not just for consulting it, but also for using it:

The current erosion of users´ privacy from numerous fronts is perturbing, the cause stems from three vast forces: the first one is the technology itself, which makes possible to be on anyone's track with instantaneous precision […] The second one is the pursuit of profits, which makes companies monitor consumer's tastes and habits in order to personalize advertising. At last we find Governments which collect many of these data in their own servers (Garton, 2010).

When a user indicates a preference, declares her/his interest to an advertisement or chooses an airline, she/he leaves «traces» which illustrates inclinations and consumption habits. What used to be personal becomes now collective: «the massification on Social Networking Sites has generalized a concept denominated «extimacy», something like revealing intimacy with its roots in the rise of 'Reality Shows' and the Web 2.0» (Pérez-Lanzac & Rincón, 2009). If we assume that intimacy means personal information which should not be revealed (Kieran, 1998: 83), or information that «we seriously and legitimately protect from being published» (Olen, 1988: 61), the fact that our presence on the Internet could be tracked, implies an infringement of our civil rights:

To renounce intimacy in our online purchases may seem to be mild. To renounce intimacy buying flights may seem reasonable; even a closed television circuit can give the impression of not to be problematic. Nonetheless, when all of them are added up we find that we do not have intimacy at all (Johnson, 2010: 193).

4. Forms of privacy infringement on Facebook

Many aspects of privacy and intimacy are unprotected in Social Network Sites, especially on Facebook, the platform with more access to the users´ personal data. Facebook collects this information through different settings, particularly data derived from profiles and the famous «Like» button:

Facebook Likes, can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, reli-

gious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender (Kosinskia, Stillwella & Graepelb, 2013).

Although there are more than one hundred fifty-seven patterns of personal data which Facebook can obtain from users (Facebook´s Data Pool, 2012), we are going to analyse uniquely those which have given rise to an international heated debate: «collecting tendencies on consumption», «the use of Private Data» and «Privacy policy changes without consent and Face Recognition Feature».

4.1. Consumption patterns

The monetization of users´ personal data is one of the most controversial aspects of Facebook. It entails not just to reveal personal information, but also to obtain profits revealing it without the consent of the data subjects: «a report was published proving that Facebook had given to advertisers, names, ages and profession of each user that had clicked in its advertisement» (La historia oculta de Facebook, 2010). However, the majority of Facebook users do not know that the firm provides information to third party companies with their own purposes. According to Mark Zuckerberg: «I have over 4,000 emails, pictures, addresses, SNS. People just submitted it. I don't know why. They trust me» (La historia oculta de Facebook, 2010). In 2009 this excessive processing of private data prompted controversy and the rise of critical positions claiming the right of the users to control their privacy. In the United States, the Federal Trade Commission (FTC) received a large number of denounces of users who demanded to be informed about which sort of data patterns Facebook collected and shared:

The proposed settlement requires Facebook to take several steps to make sure it will live up to its promises in the future, including giving consumers clear and prominent notice and obtaining consumers' express consent before their information is shared beyond the privacy settings they have established (Facebook settles FTC Charges, 2011).

The social networking service changed its architecture accordingly, an architecture which allowed the users to personalize their privacy and security level. Although Elliot Schrage, Vice President of Communications, Public Policy and Platform Marketing at Facebook, argued that Facebook had the intention to give more control to the users, the complexity of new tools was uncommon for a Social Network site: «To opt out of full disclosure of most information, it is necessary to click through more than 50 privacy buttons, which then require choosing among a total of more than 170 options» (Bilton, 2010).

4.2. Unnoticed uses of users´ profile data

In the context of Social Network Sites, a profile is equivalent to an identity document, its information concerns personal privacy and it is necessarily confidential without the consent of the data subjects. Nonetheless, Facebook has breached certain data confidentiality offering private information to different advertisers. The rise of interest of third party companies has elicited massification and personalization of unsolicited advertising. This dark data processing was reported by the Privacy Commissioner of Canada in 2009 before determining that this activity infringed the law. In response to the critics, Facebook resolved to amend its Privacy Policy: The Internet portal has announced that from now on applications developed by third parties should specify which data they are going to access as well they should ask prior permission to disclose them. Facebook will demand applications to specify which categories of users´ data they want to access, getting the user consent before they share her/his information (Facebook, 2009).

Nonetheless, the data protection regulation implemented by the company was repeatedly infringed:

Facebook promised that users could restrict their information to a limited audience, using certain privacy settings. But the truth, says the FTC, is that even when a user went to Facebook's Central Privacy Page, clicked a link to «Control who can see your profile and personal information» and limited access to certain people –for example, «only friends»– the user's choice was ineffective when it came to third-party apps that users' friends used (Fair. 2011).

Despite the company pledges, Facebook users are not properly informed about which companies are going to make use of their personal data:

People do not know how their personal data can be shared. They end up in sharing their private information with unauthorized people because of their ignorant attitude. We also conclude that complexity of privacy settings and lack of control provided to the user is equally responsible for unintentional information sharing (Zainab & Mamuna, 2012: 124).

This privacy policy allows other companies to access inappropriately to users´ private data: For a significant period of time after Facebook started featuring apps onto its site, it deceived people about how much of their information was shared with apps they used. Facebook said that when people authorized an app, the app would only have information about the users

«that it requires to work». Not accurate, says the FTC. According to the complaint, apps could access pretty much all of the user's information – even info unrelated to the operation of the app (Fair, 2011).

Although Facebook expresses in its statutes that the company will never reveal personal data to any advertiser unless the express agreement between the company and the user, this commitment was violated during the interval between September 2008 and May 2010, when «the User ID of any person who clicked on an ad was shared with the advertiser» (Fair, 2011).

4.3. Privacy policy changes without consent and facial recognition

The Office of the Data Protection Commissioner of Ireland (DPC) reported Facebook in 2011 because its lack of transparency. The company was requested to «revise privacy policy protection for non-American users because the measures adopted were excessively complex and opaque» (Facebook, 2012). However, Ireland is not the only European country to be in conflict with the American company. The Office of Data Protection and Freedom of Information in Hamburg (Germany), has reopened a research into Facebook's facial recognition software, a controversial technology which has given rise to an intense debate. According to Johannes Caspar, Commissioner in Hamburg: «The social networking giant was illegally compiling a huge database of members' photos without their consent» (O´Brien, 2012). Despite the efforts to reach a consensus, Facebook refused to change its privacy policies: «We have met repeatedly with Facebook, but have not been able to get their cooperation on this issue, which has grave implications for personal data» (O´Brien, 2012). Although facial recognition contravenes European Union legislation, Facebook has not modified its software in order to adjust its use to European laws:

The company's use of analytic software to compile photographic archives of human faces, based on photos uploaded by Facebook's members, has been problematic in Europe, where data protection laws require people to give their explicit consent to the practice (O´Brien, 2012). Even though users are able to remove a tag from a photo or deactivate their accounts, their private data remain on Facebook indefinitely. This fact infringes EU legislation and has caused controversy in the United Kingdom:

Facebook does allow people to 'deactivate' their accounts. This means that most of their information becomes invisible to other viewers, but it remains on Facebook's servers – indefinitely. This is handy for anyone who changes their mind and wants to rejoin. They can just type their old user name and password in, and they will pop straight back up on the site - it will be like they never left. But not everyone will want to grant Facebook the right to keep all their data indefinitely when they are not using it for any obvious purpose. If they do want to delete it permanently, they need to go round the site and delete everything they have ever done. That includes every wall post, every picture, and every group membership. For a heavy Facebook user, that could take hours. Even days. And it could violate the UK's Data Protection Act (King, 2007).

This controversy is a response to Facebook Terms of Service, which informs about its right to keep permanently user's personal data:

You grant us a non-exclusive, transferable, sublicensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (Facebook Terms of Service, n.d.).

In this matter, Spanish citizens can seek protection in the Law of Cancellation, which allows users to request companies to delete their data once their reciprocal relation has been extinguished: «Personal data that we voluntarily publish on our Social Network Site profile, should be deleted when we remove our consent» (Romero, 2012).

Nevertheless, Facebook arrogates to itself the right to change the Privacy Policy conditions without prior warning and without express consent of the Social Network users, even «certain information that users had designated as private –like their friend list– was made public under the new policy» (Fair, 2011).

Likewise, it is known that Facebook has designated: Certain user profile info as public when it had previously been subject to more restrictive privacy settings, Facebook overrode users' existing privacy choices. In doing that, the company materially changed the privacy of users' information and retroactively applied these changes to information it previously collected. The FTC said that doing that without users' informed consent was an unfair practice, in violation of the FTC Act (Fair, 2011).

In view of the fact that Facebook has committed excesses with regard to privacy, some citizen's platforms as «Europe vs Facebook» have emerged for the sole purpose of contributing to increase transparency to the American company processes.

5. Conclusions

In the light of the documentation presented, it is legitimate to claim that Facebook has achieved a privi-

lege status never seen before. However, the infringement of the users' right to privacy has resulted in international complains destined to demand more transparency for personal data appropriation. It has been observed that the contract signed by each user allows Facebook to collect data about people without their knowledge. This fact has been criticized by Canada and some countries in Europe, despite the American company still maintains its obscurity in the process of treatment, transference and appropriation of users´ data. It has been also analysed how some citizens have decided to palliate such deregulation reporting Facebook excesses to the relevant institutions in different countries. Nevertheless, we have proved that users' ignorance of their rights and the current tendency to «extimacy» permit on the Web 2.0 to have an effortless access to users´ personal data: «To protect their personal profile», «to remove a tag from a photo» and «to check users´ visibility» (Boutin, 2010), are three essential elements which are not usually considered by users. Moreover, disclosure of personal data, complexity of Facebook´s site architecture, data storage in perpetuity or third party interests, are some of the controversial areas which have not been adjusted to International legislation. In connection with these infringements, the Office of the Data Protection Commissioner of Ireland has carried out a report in which experts recommend some necessary measures in order to improve Facebook´s Privacy Policy:

• (To create) a mechanism for users to convey an informed choice for how their information is used and shared on the site including in relation to third party apps.

• A broad update to the Data Use Policy/Privacy Policy.

• Transparency and control for users via the provision of all personal data held to them on request and as part of their everyday interaction with the site.

• The deletion of information held on users and non-users via what is known as social plug-ins and more generally the deletion of data held from user interactions with the site much sooner than presently.

• Increased transparency and controls for the use of personal data for advertising purposes.

• An additional form of notification for users in relation to facial recognition/«tag suggest» that is considered will ensure Facebook (Ireland) meeting best practice in this area from an (Irish) law perspective.

• An enhanced ability for users to control tagging and posting on other user profiles.

I guess we should resign ourselves to accept that the modern world is like this. «Privacy has died. Get used to», as Scott McNealy, cofounder of Sun Microsystems, said once. Or we can defend ourselves; we can try to recover part of our lost intimacy. We can do it setting our own rules and sharing them with the others. We can do it applying pressure to companies like Facebook, whose users are after all, its source of income. We can also demand three exigencies: to put a curb on citizen's privacy invasion; to regulate and to control meddling companies […] The same technologies which reduce our right to privacy can also help us defend ourselves.

• An enhanced ability for users to control whether their addition to groups by friends (Data Protection Report, 2012).

Until these recommendations will be internationally standardized, the users have to resort to self-regulation, showing a higher knowledge and conscientiousness on the matter of their own privacy:

I guess we should resign ourselves to accept that the modern world is like this. «Privacy has died. Get used to», as Scott McNealy, cofounder of Sun Microsystems, said once. Or we can defend ourselves; we can try to recover part of our lost intimacy. We can do it setting our own rules and sharing them with the others. We can do it applying pressure to companies like Facebook, whose users are after all, its source of income. We can also demand three exigencies: to put

a curb on citizen's privacy invasion; to regulate and to control meddling companies […] The same technologies which reduce our right to privacy can also help us defend ourselves (Garton, 2010).

At present, until a unitary regulation will be established, we should demand users to protect their own rights, although it implies to decide on what terms they use Social Networking Sites and in which way they share their personal data.

References

Acebedo, R. (2011). *La historia de Facebook desde adentro*. La Tercera, 29-01-2011. (www.latercera.com/noticia/tendencias/2011/01/659-341582-9-la-historia-de-facebook-desde-adentro.shtml) (10-11-2012).

Bilton, N. (2010). Price of Facebook Privacy? Start Clicking. The New York Times, 12-05-2010. (www.nytimes.com/2010/05/13/technology/personaltech/13basics.html?_r=0) (10-10-2012).

Boutin, P. (2010). 3 Essential Stops to Facebook Privacy. The New York Times, 13-05-2010. (http//gadgetwise.blogs.nytimes.com/2011/06/21/3-essential-steps-to-facebook-privacy) (05-11-2012).

Boyd, D. & Ellison, N. (2007). Social Network Sites: Definition, History and Scholarship. Journal of Computer-Mediated Communication 13, 210-230. (DOI:10.1111/j.1083-6101.2007.00393.x) (28-03-2013).

Debatin, B. Lovejoy, J.P. Horn, A.K. Hughes, B.N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication. 15*, *1*, 83-108. (DOI:10.1111/j.1083-6101.2009.01494.x). (02-11-2012).

Ehrlich, P. & Ehrlich, A. (2013). Can a Collapse of Global Civilization be Avoided? Proceedings of *The Royal Society B. 280: 20122845. Royal Society Publishing. Biological Sciences.* (http://dx.doi.org/10.1098/rspb.2012.2845) (29-03-2013).

El Economista (30-05-2010). *La historia oculta de Facebook*. (www.eleconomista.es/interstitial/volver/acierto/telecomunicaciones-tecnologia/noticias/2188124/05/10/La-historia-oculta-de-Facebook-La-gente-confia-en-mi-son-tontos-del-culo.html) (04-11-2012).

Ellison, N., Steinfield, L. & Cliff, C. (2007). The Benefits of Facebook «Friends»: Social Capital and College Students' Use of Online Social Network Sites. *Journal of Computer-Mediated Communication*, *12*, 1.143-1.168. (DOI:10.1111/j.1083-6101.2007.00367.x) (27-03-2013).

El Mundo (Ed.) (2012). Facebook y Linkedin se comprometen a reforzar su privacidad. *El Mundo, 29/06/2012*. (www.elmundo.es/elmundo/2012/06/29/navegante/1340955573.html) (04-11-2012).

El País (Ed.) (2009). Más intimidad en Facebook. *El País, 27-08-2009*. (http//tecnologia.elpais.com/tecnologia/2009/08/27/actualidad/1251363663_850215.html) (01-11-2012).

Facebook (Ed.) (2012). *Facebook s Data Pool. Europe vs Facebook. 03-04-2012*. (http//europe-v-facebook.org/EN/Data_Pool/data_pool.html) (03-11-2012).

Fair, L. (2011). *The FTC's settlement with Facebook. Where Facebook went wrong.* Federal Trade Commission Protecting America´s Consumers. 29-11-2011. (http//business.ftc.gov/blog/2011/11/ftc%E2%80%99s-settlement-facebook-where-facebook-went-wrong) (02-11-2012).

Federal Trade Commission (Ed.) (2011).Facebook settles FTC Charges that it Deceived Consumers by Failing to Keep Privacy Promises. *Federal Trade Commission Protecting America s Consumers, 29-11-2011.* (http//ftc.gov/opa/2011/11/privacysettlement.shtm) (03-10-2012).

Garton, T. (2010). Facebook: restablecer la privacidad. *El País, 11-10-2010*. (http//elpais.com/diario/2010/10/11/opinion/1286748-011_850215.html) (04-10-2012).

González-Gaitano, N. (1990). *El deber de respeto a la intimidad. Información pública y relación social*. Pamplona: EUNSA.

Horvát E.A., Hanselmann M. & al. (2012). One Plus One Makes Three (for Social Networks). *PLoS ONE 7(4)*, e34740. (DOI: 10.1371/journal.pone.0034740) (27-03-2013).

Johnson, D.G. (2010). *Ética informática y ética e Internet*. Madrid: Edibesa.

Jones, J.J., Settle, J.E., Bond R.M. & al. (2013). Inferring Tie Strength from Online Directed Behaviour. *PLoS ONE 8(1)*, e52168. (DOI:10.1371/journal.pone.0052168) (29-03-2013).

Kanai, R., Bahrami, B., Roylance, R. & al. (2012): *Online Social Network Size is Reflected in Human Brain Structure.* Proceedings of The Royal Society B. 280: 20122845. Royal Society Publishing. Biological Sciences, 2012 279. (DOI:10.1098/rspb.2011.1959) (28-03-2013).

Kieran, M. (Ed.). (1998). *Media Ethics*. London: Routledge.

King, B. (2007). Facebook Data Protection Row. *Channel 4, 17-11-2007*. (www.channel4.com) (01-11-2012).

Kosinskia M., Stillwella, D. & Graepelb, T. (2013). *Private Traits and Attributes are Predictable from Digital Records of Human Behaviour. Proceedings of the National Academy of Sciences (PNAS)*. University of California, Berkeley. (DOI:10.1073/pnas.1218772110) (29-03-2013).

Lacalle, C. (2011). La ficción interactiva. Televisión y Web 2.0. *Ámbitos, 20*.

Libreros, E. (2011). *Las redes sociales en España 2011*. IEDGE, 01-12-2011. (http//blog.iedge.eu/direccion-marketing/marketing-interactivo/social-media-marketing/eduardo-liberos-las-redes-sociales-en-espana-2011) (02-11-2012).

López-Reyes, Ó. (1995). *La ética en el periodismo. Los cinco factores que interactúan en la deontología profesional*. República Dominicana: Banco Central.

Marshall, T. (2012): Facebook Surveillance of Former Romantic Partners: Associations with PostBreakup Recovery and Personal Growth. *Cyberpsychology, Behavior and Social Networking*, *15*, 10 (DOI:10.1089/cyber.2012.0125) (29-03-2013).

Morse, G. & Watts, D. (2003). The Science behind Six Degrees. *Harvard Business Review Online*, Febrero. (http//hbsp.harvard.edu/b02/en/hbr/hbrsa/current/0302/article) (05-11-2012).

Olen, J. (1988). *Ethics in Journalism. Englewood Cliffs.* New Jersey: Prentice Hall.

O'Brien, K. (2012). Germans Reopen Investigation on Facebook Privacy. *The New York Times, 15-08-2012*. (www.nytimes.com/2012/08/16/technology/germans-reopen-facebook-privacy-inquiry.html) (01-11-2012).

O´Reilly, T. (2007). What is the Web 2.0. Design Patterns and Business Models for the Next Generation of Software. *Munich Personal RePEc Archive (MPRA)*, 4.580, 07-11-2007. (http//mpra.ub.uni-muenchen.de/4580) (05-11-2012).

Pérez-Lanzac, C. & Rincón, R. (2009). Tu «extimidad» contra mi intimidad. *El País, 24-03-09*. (www.elpais.com) (20-10-2012).

Report of Data Protection Audit of Facebook Ireland Published (2012). *Oficina del Comisionado de Protección de Datos de Irlanda* (www.dataprotection.ie/viewdoc.asp?DocID=1175) (02-11-2012).

Romero-Coloma, A.M. (1987). *Derecho a la intimidad, a la información y proceso penal*. Madrid: Colex.

Romero, P. (2012). A las redes sociales les cuesta «olvidar'. *El*

Mundo, 05-03-2012. (www.elmundo.es/elmundo/2012/02/20/navegante/1329751557.html) (03-11-2012).

RUIZ, C., MASIP, P., MICÓ, JL. & AL. (2010). Conversación 2.0 y democracia. Análisis de los comentarios de los lectores en la prensa. *Comunicación y Sociedad, XXIII, 2*.

VARIOS (Ed.). *Declaración de licencia y términos de uso del sitio web de Facebook*. (www.facebook.com/legal/terms) (05-11-2012).

VARIOS (2007). *Psicología social*. Madrid: McGraw Hill.

WARREN, S. & BRANDEIS, L. (1890). *El derecho a la intimidad*. Madrid: Civitas.

WATTS, D.J. (2004). *Six Degrees. The Science of a Connected Age. (Primera edición de 1971)*. New York: W.W. Norton & Company.

YUSTE, B. (2010). Twitter, el nuevo aliado del periodista. *Cuadernos de Periodistas, diciembre, 86*. Madrid: Asociación de la Prensa de Madrid.

ZAINAB, A. & MAMUNA, K. (2012). Users' Perceptions on Facebook's Privacy Policies. ARPN *Journal of Systems and Software, 2, 3*. (http//scientific-journals.org) (DOI.10.1111/j.1083-6101.2009.-01494.x).