THE PRIVATE USE OF THE SOCIAL NETWORKS BY THE CIVIL SERVANTS – A POSSIBLE "ACHILLES' HEEL'' OF PERSONAL DATA PROTECTION IN PUBLIC ORDER AND SECURITY INSTITUTIONS?

by

ALEXANDRINA-AUGUSTA BORA*

Public order and security systems represent structures in which both protection of classified information and protection of personal data are strictly regulated by laws, internal regulations and concrete measures to protect computer communication networks. We conducted an empirical study by interviewing a group of 150 people belonging to the public order and security institutions that shows that a significant percentage of them use social networks outside work program in private life. Based on the conclusions of the study and the empirical observations made on some of the public order and security institutions staff we outline the need to analyze the possible risks to their professional activity deriving from insufficient protection of their personal data during the use of social networks. Furthermore, we argue that these risks are amplified in the case of police officers who have to do undercover work using in the same time the mobile Internet. Finally, we argue that this type of attitude endangers law enforcement and security of the officers and it is influenced by two factors: the weakness of SNSs data protection regulations and the freedom of expression exercised carelessly by the public order and security institutions staff. In order to find remedies for this vulnerability created by this "security breach" derived from the private activity of public order and security institutions staff in social networks, we propose to continue the empirical study to find the reasons behind this type of behaviour and if they have reasonable expectations of privacy related to SNSs policies of data protection. Based on these findings we could be focused on de-

* dr.augustabora@yahoo.com; Babeş-Bolyai University.

veloping an adequate training programme concerning this issue for police officers or the public order and security institutions staff because they are professionals who might give a special attention to these issues.

KEYWORDS
social networks, civil servants, police officers, public-private distinction

1 INTRODUCTION

The protection of personal data represents a relatively new field for Romania's legislative space. Its' essence regards, in a generic form, the natural person's right of protection of those specific features which lead to his/her identification and the state's correlative obligation of adopting adequate measures to ensure an efficient protection.

There is need for a comprehensive discussion of the legal framework concerning personal data protection. Even so, we will only mention the main regulation in order to outline that the legal framework is not essential regarding the private activity of public order and security institutions staff in social networks. The most important regulation in this field are: Law No. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, Published in the Official Journal of Romania, Part I, No. 790/12 December 2001, amended and completed, Law no. 682 of 28th November 2001 on the ratification of the Convention on the protection of individuals with regard to automatic processing of personal data, adopted in Strasbourg on the 28th January 1981 Published in the Official Journal no. 830 of the 21 December 2001, Law no. 102/2005 regarding the setting up, organisation and functioning of the National Supervisory Authority for Personal Data Processing, Law no. 55 of 17th March 2005 on the ratification of the Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows, adopted in Strasbourg on 18th November 2001, published in the Official Journal no. 244 of 23 March 2005, Emergency Ordinance no. 36 from 9 of May 2007 for the annulment of the Law no. 476/2003 regarding the approval of the personal data processing notification tax which fall under the jurisdiction of the Law no. 677/2001 for the protection of persons regarding the processing of personal ata and the free movement of such data, published in the Official Monitor with no. 335 from 17 May 2007, Law no.

298/2008 on the retention of data generated or processed in connection with the provisions of publicly available electronic communications services or of public communications networks and for the amendment of Law no. 506/2004 on the processing of personal data and the protection of private life within the electronic communication sector, Published in the Official Journal no. 780 of 21st of November 2008.

Under the Law no. 677/2001 on the person's protection regarding the processing of personal data and the free circulation of these data, the acquis represented by the Directive no. 95/46/EC was implemented, which sets up the general juridical frame of the personal data protection at European Union level. For this purpose, a central authority empowered with such control competence, the National Authority for the Supervision of Personal Data Processing, came into existence in Romania, too. Under the Law no. 102/2005, the Authority exerts the competence established mainly by the Law no. 677/2001, in terms of independence from any public authority or private entity.

The competences of the National Authority for the Supervision of Personal Data Processing are specific for any institution of control, including the investigation of personal data processing conducted under the Law no. 677/2001 and the sanctioning, if it comes out that the legal dispositions were infringed by the personal data processors, as a result of self-notification or based on complaints filed by the people who's rights were infringed.

The Authority has the goal of protecting the fundamental rights and freedoms of the natural persons, especially the right of intimate, family and private life, in connection with the processing of personal data and the free circulation of these data.

The National Authority for the Supervision of Personal Data Processing carries out its' activity in terms of complete independence and impartiality. The authority supervises and controls the legality of the personal data processing which falls under the Law no. 677/2001. For this purpose, the supervisory authority exerts the following prerogatives: receives and examines the notifications on the processing of personal data, authorizes the data processing in the situations stipulated by the law, can decide, if it ascertains the infringement of this law, the temporary suspension or the cessation of the data processing, the partial or entire erasure of the processed data and can inform the penal bodies or sue, informs the natural and/or juridical persons about the necessity of complying with the obligations and carrying out the

procedures stipulated by Law no. 677/2001, keeps and lays at public disposal the register of recording the personal data processing, receives and solves the complaints, intimations or requests of the natural persons and communicates the given solution or, according to each case, the approaches carried out, performs preliminary controls, if the data processor processes personal data which are liable of presenting special risks for the persons' rights and freedoms,performs investigations, at self-notification or at the reception of complaints or intimations, is consulted when normative acts regarding the protection of persons' rights and freedoms, concerning the personal data processing, are drafted, can make proposals regarding the drafting of normative acts or modifying of normative acts in force, in the field of personal data processing, cooperates with the public authorities and public administration bodies, centralizes and examines their annual reports regarding the people's protection concerning the processing of personal data, issues recommendations and approvals on any matter connected to the protection of the fundamental rights and freedoms, concerning the personal data processing, at any person's request, including public authorities and public administration bodies, cooperates with similar authorities from abroad, for mutual assistance, as well as with persons with residence or premises abroad, for the protection of the fundamental rights and freedoms which may be affected by the personal data processing, carries out other competences stipulated by law.[1]

Because public order and security systems represent structures in which both protection of classified information and protection of personal data are strictly regulated by laws, and other regulations, we are interested in describing the behaviour of civil servants related to the use of the social networks outside work program in private life.

We can say that, in terms of legislation and organization in institutions like Romanian Police, Romanian Gendarmerie, Anti-Corruption General Directorate, General Directorate of Intelligence and Internal Protection, there is a good protection of the personal data of the subjects which are investigated. Moreover, in certain areas of processing information with a high level of classification it is not allowed the introduction by the civil servants of any tools that might store data or of any device which has an Internet connection to transmit any information held in the spaces. So even if these

[1] http://www.dataprotection.ro/index.jsp?page=about&lang=en, the site of National Authority for the Supervision of Personal Data Processing, consulted at 06/02/2013;

measures are restricting civil right to communicate freely even in the professional environments, the internal communication networks of public order and security institutions limited the access to social networking, namely using UGC services (User Generated Content).

We conducted an empirical study by interviewing a group of 150 people belonging to the public order and security institutions that shows that a significant percentage of them use social networks outside work program in private life.

2 THE PUBLIC-PRIVATE DISTINCTION IN SOCIAL LIFE

Before presenting the findings of our empirical study, we searched to explain some issues which might come into discussion in our results and conclusions:

2.1. The public-private distinction in social life.

2.2. The concept of "social networks" and the difficulty of sustaining a public/private distinction in social networks; the need for a tool of keeping the private and the public dimension of life as distinct as the individual wants.

2.1 THE PUBLIC-PRIVATE DISTINCTION IN SOCIAL LIFE

Social and legal theorists have grappled with the subtleties of the public/private distinction. Nissenbaum[2] introduces the concept of contextual integrity, which states that within a context of an interaction, people have expectations about what information is appropriate to collect and whether it should be distributed. Nissenbaum stresses that ideas about contextual integrity vary across time, place, and culture. However, she does not account for variations within a particular context. People have different expectations about what information can be shared or what constitutes sensitive information. One useful lens for understanding differences in expectations about identity and content sharing within social networks is the concept of the fractalization of the public and private.[3] Nissenbaum argues that some privacy is required for individuals to self-actualize. Privacy is arguably necessary for advancing the self and protecting the integrity of relationships. Having insulation against outside scrutiny is important for experimenting with aspects of the self without fear of retribution.

---

[2] Nissenbaum, H., 2004, Privacy as contextual integrity. Washington Law Review, 79(1), 101–158;

[3] Lange P.G., 2008, Publicly Private and Privately Public: SocialNetworking on YouTube, Journal of Computer-Mediated Communication, 13 361–380, International Communication Association, p.362;

The terms 'public' and 'private' have described social phenomena ranging from the political and economic to the spatial and personal.

As it was argued in some a recent work, at this sociohistorical juncture, it is more appropriate to treat public and private as anchors at either end of a continuum, with multiple and fluid interstitial categories.[4]

Our days, the separation between public and private became less absolute. The breakdown between public and private is apparent on a number of levels. While work is still 'public' and home and leisure are still 'private', the distance between them, physical, temporal, and spatial, has shrunk.

This situation is reflected also in juridical decisions. For instance, the decision in Von Hannover v Germany (No. 2) is the second of two given on 7 February 2012 by the Grand Chamber concerning the balancing of privacy and freedom of expression. In a unanimous decision, the Grand Chamber found that Germany had not failed in its obligation to respect the applicants' Article 8 rights when it refused to grant an injunction against the publication of a photograph taken of Princess Caroline and her husband while on holiday at a ski resort in Switzerland. Von Hannover (No. 2) attempts to narrow the focus when attempting to balance two equal but competing rights. This judgment was unanimous and appears to place a higher value on the protection of one's image than to the protection of one's reputation, the latter of which must attain a certain level of seriousness in order to engage Article 8. The judgment will doubtless be a welcome contribution to the English privacy law debate and it will be interesting to see how the English courts apply these principles in future cases.[5]

We cannot make anymore a clear analysis of the privacy concept because this concept became 'blurry' or we can say that its limits depend on the situation related to the idea of privacy. As a comprehensive study[6] on this issue stated in conclusion, "the public/private distinction is one of the most influential concepts of the modern era, both in terms of social theory and in terms of everyday life. The assumption that public and private are a dichotomous pair has influenced numerous aspects of social life, ranging from the gendered division of labor to the development of the suburb. For many,

[4] Sarah Michele Ford, 2011, Reconceptualizing The Public/Private Distinction In The Age Of Information Technology, Information, Communication & Society, 14:4, 550-567;

[5] Case Law: Von Hannover v Germany (No.2) – Unclear clarification and unappreciated margins – Kirsten Sjøvoll
http://inforrm.wordpress.com/2012/02/10/case-law-von-hannover-v-germany-no-2-unclear-clarification-and-unappreciated-margins-kirsten-sjovoll/

[6] Sarah Michele Ford, 2011, op.cit., p.567;

public and private have been treated as completely separate. However, the division between the public and private realms was not impermeable. The public and private realms have bled over into one another, and can no longer be treated as a dichotomous pair". Based on patterns of social change and examples from mass media and information and communications technologies, the author has shown that a more fruitful conception of the public/private realms is one that treats them as anchors on either end of a continuum, with liminal categories being created and destroyed as needed. The final idea is that the line between public and private has become blurry; these concepts are no longer polar opposites, and the social world is attempting to sort out how to deal with the loss of one of its fundamental categories.

2.2 THE CONCEPT OF "SOCIAL NETWORKS" AND THE DIFFICULTY OF SUSTAINING A PUBLIC/PRIVATE DISTINCTION IN SOCIAL NETWORKS

Social network websites were described as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site.[7]

The concept of ''social networks'' is difficult to define. Wellman[8] argues that online and offline social networks do not exist as such, but that they are useful analytic constructs for understanding social dynamics. A social network will look different depending upon how one measures it (counting the number of interactions between members versus rating the closeness of relationships, for instance). A social network is defined here as relations among people who deem other network members to be important or relevant to them in some way.[9]

Currently, there are no reliable data regarding how many people use SNSs, although marketing research indicates that SNSs are growing in popularity worldwide.

---

[7] Boyd, D. M., & Ellison, N. B., 2007, Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), article 11;

[8] Wellman, B.,1996, Are personal communities local? A Dumptarian reconsideration.Social Networks, 18(4), 347–354.

[9] Wellman, B. ,1996, op.cit.;

This growth has prompted many corporations to invest time and money in creating, purchasing, promoting, and advertising SNSs. At the same time, other companies are blocking their employees from accessing the sites. Additionally, the U.S. military banned soldiers from accessing MySpace[10] and the Canadian government prohibited employees from Facebook[11], while the U.S. Congress has proposed legislation to ban youth from accessing SNSs in schools and libraries.[12]

Even in our country, in public order and security institutions as Romanian Police, Romanian Gendarmerie, Anti-Corruption General Directorate, General Directorate of Intelligence and Internal Protection Moreover, it is not allowed the introduction by the civil servants of any tools that might store data or of any device which has an Internet connection to transmit any information held in the spaces. So even if these measures are restricting civil right to communicate freely even in the professional environments, the internal communication networks of Romanian public order and security institutions limited the access to social networking. Therefore, there are tensions between law enforcement and individual freedom in this work environment.

Researchers have investigated the potential threats to privacy associated with SNSs. In one of the first academic studies of privacy and SNSs, Gross and Acquisti[13] analyzed 4,000 Carnegie Mellon University Facebook profiles and outlined the potential threats to privacy contained in the personal information included on the site by students, such as the potential ability to reconstruct users' social security numbers using information often found in profiles, such as hometown and date of birth.

Acquisti and Gross[14] argue that there is often a disconnect between students' desire to protect privacy and their behaviors, a theme that is also ex-

---

[10] Frosch, D., 2007, May 15, Pentagon blocks 13 web sites from military computers. New York Times. Retrieved July 21, 2007, from http://www.nytimes.com/2007/05/15/washington/15block.html;

[11] Benzie, R., 2007, May 3, Facebook banned for Ontario staffers. The Star. Retrieved July 21, 2007 from http://www.thestar.com/News/article/210014;

[12] Boyd, D. M., & Ellison, N. B, 2007, Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), article 11. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html;

[13] Gross, R., & Acquisti, A., 2005, Information revelation and privacy in online social networks. Proceedings of WPES'05 (pp. 71-80). Alexandria, VA: ACM;

[14] Acquisti, A., & Gross, R., 2006, Imagined communities: Awareness, information sharing, and privacy on the Facebook. In P. Golle & G. Danezis (Eds.), Proceedings of 6th Workshop on Privacy Enhancing Technologies (pp. 36-58). Cambridge, UK: Robinson College;

plored in Stutzman's[15] survey of Facebook users and Barnes's[16] description of the "privacy paradox" that occurs when teens are not aware of the public nature of the Internet. In analyzing trust on social network sites, Dwyer, Hiltz, and Passerini[17] argued that trust and usage goals may affect what people are willing to share—Facebook users expressed greater trust in Facebook than MySpace users did in MySpace and thus were more willing to share information on the site.[18]

SNSs are also challenging legal conceptions of privacy. Hodge[19] argued that the fourth amendment to the U.S. Constitution and legal decisions concerning privacy are not equipped to address social network sites. For example, do police officers have the right to access content posted to Facebook without a warrant? The legality of this hinges on users' expectation of privacy and whether or not Facebook profiles are considered public or private.

3 THE EMPIRICAL STUDY

Considering these findings we were interested in studying the police officers behaviour in SNSs in their spare time outside the work environment and the way this privacy/public balance regarding the share of personal data could influence some of their work activities.

We conducted an empirical study by interviewing a group of 150 people belonging to the public order and security institutions about their behaviour in SNSs and the concern they show for the protection of the privacy of their personal data. We were interested to find whether they understand how to protect their privacy and their personal data on SNSs. The issue might become relevant to their work because the police officers often come into contact with criminal environments while working, the risks they are

---

[15] Stutzman, F., 2006, An evaluation of identity-sharing behavior in social network communities. Journal of the International Digital Media and Arts Association, 3 (1), 10-18;

[16] Barnes, S., 2006, A privacy paradox: Social networking in the United States. First Monday, 11 (9). Retrieved September 8, 2007 from http://www.firstmonday.org/issues/issue11_9/barnes/index.html;

[17] Dwyer, C., Hiltz, S. R., & Passerini, K., 2007, Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. Proceedings of AMCIS 2007, Keystone, CO. Retrieved September 21, 2007 from http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf;

[18] Boyd, D. M., & Ellison, N. B., 2007, Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), article 11. ,http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html;

[19] Hodge, M. J., 2006, The Fourth Amendment and privacy issues on the "new" Internet: Facebook.com and MySpace.com. Southern Illinois University Law Journal, 31, 95-122;

subject to being extended beyond the working hours, sometimes in private life, including in their activity on social networks.

Although there are methodological problems with determination of representative sample, with collection of data and therefore there are doubts about methodological accuracy, we searched for some answers to the questions which have not been asked before in Romanian public order and security institutions.

We asked the questions presented below:

1. How often do you access the Internet in the following environment: at home, at work, in other places?

1=every day; 2=a few times a week; 3=once a week; 4=a few times per month;5=rarely;6=never;

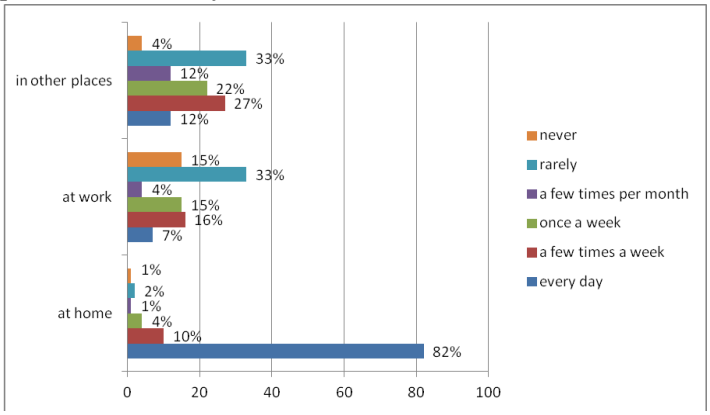

Chart no. 1: *The frequency of accessing the Internet*

These findings show that a significant percentage of the subjects (82%) use Internet outside of the work program, in private life. We assume that this kind of behaviour is determined by the security measures taken in the work place to protect computer communication networks and the information they work with.

This raises the following question: do they understand that they need to protect their privacy and even their personal data? Are the security measures as important in private life as they are in their work environment? In order to establish that, we asked the next questions.

2. Do you have a profile on SNSs (as Facebook, Myspace etc.)?

1=yes 2=no

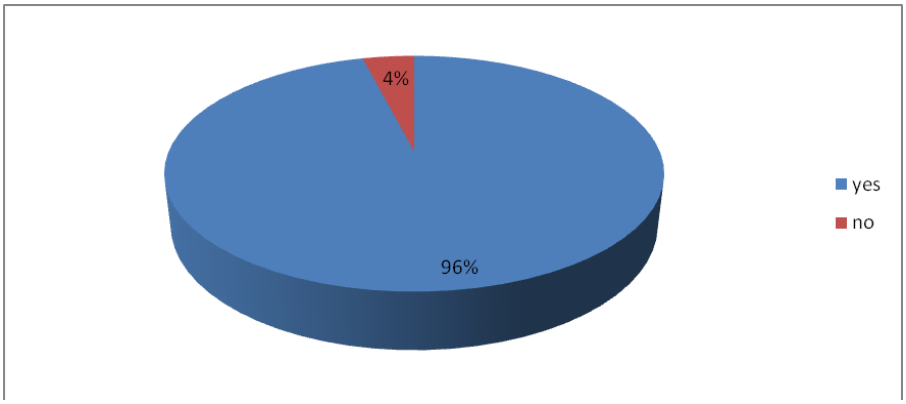

Chart no. 2: *The existence of an account in SNSs*

3. How often do you use this account?
1=every day, 2=every week, 3=rarely, 4=never

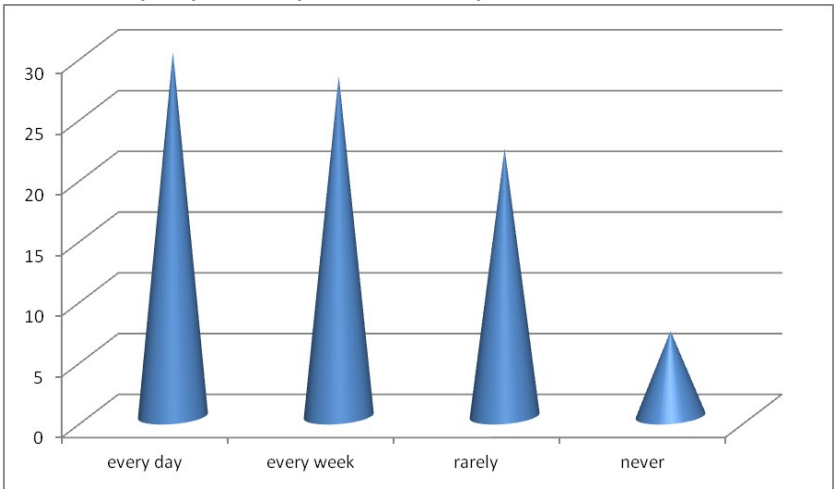

Chart no. 3: *The frequency of using the account*

First of all, we find that over 90 % of the police officers created a SNSs account and that over a half of them are using this account quite often (30% daily and 25% weekly).

Based on findings and the empirical observations made on some of the public order and security institutions staff, we outline the need to analyze the possible risks to their professional activity deriving from insufficient protection of their personal data during the use of these accounts. But first we needed to find what kind of information do they share on these SNSs.

The results were quite surprising considering the expectations we had from this type of group (trained in security issues and data protection regulations).

4. What type of information did you share on SNSs (when register or using it)?
    1. Financial information
    2. Identification number
    3. Name
    4. Adress
    5. Hobbies
    6. Personal photos
    7. Friends
    8. Mobile phone number
    9. e-mail

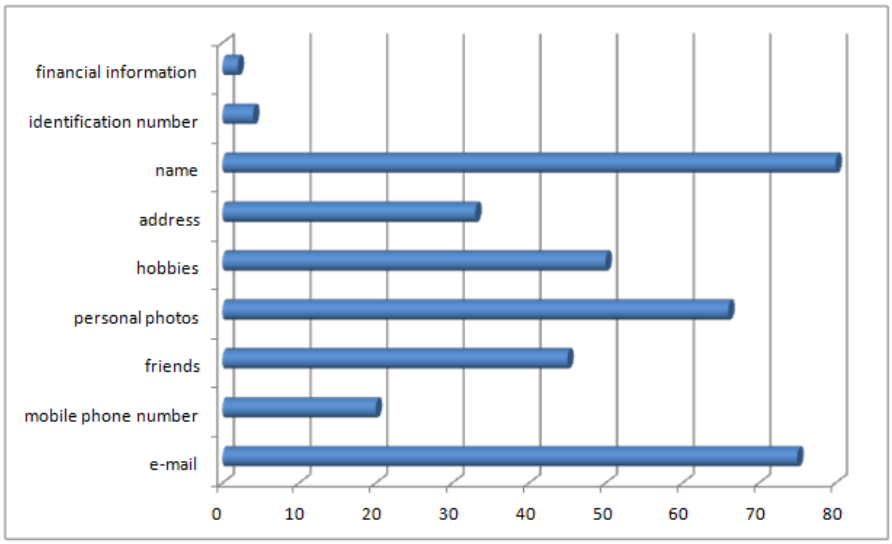

Chart no. 4: *Type of information shared on SNSs account*

As the results show, over 80% of the participants share the name, almost 70% share personal photos, almost 80% give their e-mail and over 30% revealed even their postal address.

These findings raise some questions regarding the level of protection of the personal data of civil servants who often come into contact with criminal environments during working hours, the risks they are subject to being

extended beyond the working hours, sometimes in private life, including in their activity on social networks. Based on these results, we outline the need to analyze the possible risks to their professional activity.

We argue that these risks are amplified in the case of police officers who have to do undercover work using in the same time the mobile Internet. They can be easily identified and even their location could be compromised.

4 CONCLUSION

Before analysing the results of this empirical study, we blamed the weak protection of personal data available on these websites. After the final results of the study, we think that this type of attitude endangers law enforcement and security of the officers and it is influenced by two factors: the weekness of SNSs data protection regulations and the freedom of expression exercised carelessly by the public order and security institutions staff.

So, this posible ”Achilles' heel” of personal data protection in public order and security institutions, as we named it in the title of the paper, could be a vulnerability created by this "security breach" derived from the private activity of public order and security institutions staff in social networks related mainly to their behaviour in SNSs. This careless attitude makes it possible for individuals with connections in criminal environments to view the personal data of civil servants or police officers and to become a risk to law enforcement institutions work and security. However, even if this is the main factor for this vulnerability, we could not say that the personal data protection system in SNSs is helping the process of law enforcement from this point of view. We think that securing the personal data, these social networks could facilitate changing regulations within the public order and security institutions, so that they could be included as additional databases in investigating crimes and for identifying suspects, with the observation that the information they offer would be used with respect to the human privacy and dignity.

In order to find remedies for this vulnerability created by this "security breach" derived from the private activity of public order and security institutions staff in social networks, we propose two steps.

First, we need to continue this empirical study in order to find out the reasons and cause of this particular behaviour of the public order and security institutions staff in social networks. We need to find out if they are

aware of the risks, if they have reasonable expectations of privacy related to SNSs policies of data protection.

After that we could suggest some remedies, which, in our opinion, since the option "secure Facebook" is not realistic, could only be focused on developing an adequate training programme concerning this issue for all the public order and security institutions staff, that should be conducted starting with their initial training years. Still, an issue remains: does the SNSs agreement adequately explain how the data is being used and whether the consent provided by the user is sufficient to cover all the activities carried out by the service? We dare to say that it is not. As an additional argument to sustain this idea we can say, after looking at the results of this empirical study, that not even the trained personnel in security issues and personal data protection regulation was not aware of the risks of their consent of sharing information on SNSs.

We also think that different kinds of professional activity of the SNSs users require distinctive levels of protection from outside parties; these are manifested in varied levels of publicness and privacy in SNSs activity. The police officers or the public order and security institutions staff are a type of professionals who might give a special attention to these issues. As argued, the notice and consent paradigm is worthless. Some simplification of those terms is possible, but there's really very little competitive force at work there. No one knows that one company's privacy agreement is better than another's, or has the time to find out. Harry Lewis sees that "the only real solution for the long run is education: teaching kids to think critically about the information they give and are given".[20]

So, as we already stated, there are no significant legal implications of the findings of this empirical study. There are many regulation concerning personal data protection in public order and security institutions. The legal solution cannot solve an educational issue. Public order and security institution have to decide if the investment in trainings concerning those specific issues is justified by the possible risks. By these empirical findings, we identified a vulnerability, just opened a gate for scientific studies of the risks derived from the private activity of public order and security institutions staff in social networks.

[20] "The Public-Private Distinction Does Not Work Anymore"by Harry Lewis — 23.11.2011; http://theeuropean-magazine.com/387-lewis-harry/388-the-dark-side-of-technology.