

LEGAL PROBLEMS OF SOCIAL NETWORKS

The increasing popularity that the social networks have acquired in the recent times, have highlighted the legal problems posed in the obvious risk for the privacy and data protection rights.

Following the definition of social networks in wikipedia, supported by the Report on Guidance of Privacy in social networks elaborated by the International Working Group on Data Protection in Telecommunications on March 4th, 2008, and the Resolution adopted by European authorities for protection of data privacy on the services of social networks, we are dealing with “*services focuses on the building and verifying of online social networks for communities of people who share interests and activities, or who are interested in exploring the interests and activities of others, and which necessitates the use of software. Most services are primarily web based and provide a collection on various ways for users to interact*”.

Although these networks give many benefits to users by facilitating communication between them and the exchange of any kind of information in real time, this social networks represents a serious threat to the privacy rights and their data protection or to third parts related to them (family, friends, etc.) because the data they dump on the social networks (contact information, photographs, videos, etc.) are accessible in a public and global way.

From a legal point of view, the principal risks who social networks may arise can be organized in three different sections:

1. **Violation user’s data protection rights.-** The inclusion by the users of personal details regarding to themselves or other users in a social network involve a risk of violation in data protection subject:
 - Not agree data transfer.- Data, once published, are dumped to the network and are available to the public in general. Moreover, it results very easy to the social network members or to other networks to copy the data, because these personal details are leaked to other servers and even indexed to general search engines.(Search as google)
 - Violation of the quality or the principle data purpose.- The secondary uses of the personal data are other example of this right violation. A comprehensive percentage of human resources managers admit to use data from social

networks services for their works, to verify and/or complete data of job applicant.

Likewise, there are many marketing firms that use the data published on social networks to make surveys and statistics about various products. In some cases, even these companies have nothing to do with social networks are allowed to send questionnaires to users for commercial use

- Difficulty in exercising to cancel right of the data.- The problem of the users who dump the data in a social network is its lack of protection to the data coping, and the usual “indexing” by search engines, making it difficult from exercise the cancellation rights.

2. Identity Fraud.- The vast amount of information related to a user in the social network represents a risk to his safety and privacy if we consider the possible use of the data by unauthorized third parts to misappropriate our identity

3. Absence of uniform rule at the international level.- Absence of international standard regulation to use the social network can only increase the lack of security for the users.

Although at the European level, the Directive 95/46, on Oct. 24, regarding the data treatment of personal data, likewise other specific that complement and guarantee the data protection rights in the European Union level, most of service providers of social networks (for example Facebook), are domiciled outside the scope of the European Union, so that it is not implementing the aforementioned regulation.

Therefore, it is necessary to create globally applicable rules able to respond to global problems which due to its nature usually pose this kind of networks.

In response to the problems exposed, and in view of the unprecedented increase of the personal data information spread the International Working Group on Data Protection in Telecommunications, in their meeting in Rome on the latest March, and the European Data Protection Authorities, at the Conference held in October this year, have analyzed the potential dangers that the social networks means to the privacy and they have established some recommendations to be followed, both by users as by these services providers, to avoid them, or at least, to decrease them.

Regarding to the recommendations addressed the users of social networks, the organizations and associations that represent them must carry out an educational labor directed to the users, in order to protect their personal details. According to experts, the things than all users should know and implement are measures like the ones hereunder exposed:

- Before publishing personal data in a network profile, think also about whether you would like to be confronted with information or pictures in a job application situation.
- Pay attention to the activity of your children in Internet, especially on social network websites where it is unadvisable to reveal the telephone number or the address.
- It's very useful using a pseudonym instead, but note than even then you have only limited control over who can identify you, as a third parts may be able to lift a pseudonym.

The proper use of the online social networks by users is complemented with the providers' responsibility of them. In accordance with this assertion, the experts in this field recommend the establishment of the following measures:

- Talking about social network that provide services acting in different countries they should respect the privacy rules of the countries where they provide their services, seeking advice of the National Authorities of Data Protection if needed.
- Provide users with transparent and open information about the processing and use of personal information, warning users, in an understandable way, about the potential consequences of disclosing their own personal data in a profile, the security risks as well as about the possible legal access by third parts.
- Improve the users control over the use of community members of their own profile data.
- The establishment of configurations which respect the user privacy by default.
- Improve and maintain the security of their information systems and protect users from illegal access to their profiles.
- Allow the user cancellation as a membership, deleting his profile and all information published at the network in an easy way.

- Take appropriate measures in order to prevent “spidering or blue harvesting” of profile data by third parts.
- Ensure user data profile could only be explored by search external engines subject to the prior user consent. The non-index-linking of profiles should be an option by default.

Therefore, the main legal problem of social networks sites is the lack of international uniform regulation which guarantee the right of privacy and the personal data protection, not only of the users and third parts who lose the control of the information that they join to the network but also to any citizen whose personal data, even in the case of not being membership, had been incorporated to them by other people with personal links.

The global character of the controversy provoked by the online social network, involves that the only solution is subject to the approve of an international rule that regulates the users rights, turning out to be advisable, that while it is not approved, the users and the providers of the above mentioned networks should follow the experts recommendations (International Working Group on Data Protection on Telecommunications).

Authors:

Pablo Álvarez de Linera Granda (J&A GARRIGUES)

Nelly Sánchez Mouriz (J&A GARRIGUES)

Sofía Cuervas-Mons Ruiloba (J&A GARRIGUES)

Sources:

http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491

http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

https://www.agpd.es/portalweb/canaldocumentacion/conferencias/common/pdfs/30_conferencia_internacional/resolucion_redes_sociales.pdf