Regulating privacy on Online Social Networks (OSNs), possibility or utopia in the digital era?

By Despina D. Spatha

I. Introduction

The evolution of social networks constitutes an example to make us believe that borders disappear in favor of universal communication.

However, personal information disclosed without permission may cause injury. The challenges of protecting private life are crucial. The online social networking is a tool of control for employers, a surveillance tool for public authorities, a prospecting tool for professionals and the space of circulation of huge amounts of personal data.

Currently Facebook is the second most visited website in the world and the pioneer of social networks. Facebook users connect offline with online life, which presupposes the proliferation of personal data on the digital environment and within this service there are instruments to facilitate such disclosure. Beyond this observation, the exposure of real personal information augments the value of information since it is personal data which can be exploited.

Regarding the online protection of personal data, digital networks emphasize the application of laws. OSNs represent the field of application of legal systems being sometimes contradictory or similar. Finally, in a digital environment already quite controversial the OSN services demonstrate the necessity of taking a position in the traditional debate between protecting the fundamental rights and the economic interests of exploiting personal data.

II. The law implementation within social networks

The architecture of the information flow and the practices of OSN operators cause a range of factors which reduce the possibility of managing online privacy, which interne the threat to personal safety and make the protection of privacy extremely complex.

Firstly, the instantaneity of information involves the risk of not having the time to minimize adverse effects. Secondly the digital message remains in the system for an unlimited period. Thirdly users can not identify senders of personal data and the context in which this information can be reproduced.

However, OSNs are services provided usually by two or more companies located all over the world having affiliated companies or agencies based in Europe. These companies are governed by different laws and addressing a global audience which explains a mixture of regulatory privacy systems.

Since the law has traditionally been created to deal with human activities, aiming at the efficient function of society, legislation inevitably determines the OSN's policy.

Nevertheless, the application of legal norms within cyberspace is not always easy. Still other modes of regulation exist that could sometimes influence the protection of user privacy.

A. The European aspect of Privacy

According to American culture personal data may be any information. Due to this, personal data is often considered commodity and it is rather the market and not the legislator that determines the conditions of processing. This differs from the European aspect where personal data is nominal, inviolable, inalienable and unassignable.

The European privacy framework imposes several rules and restrictions in favor of the balance between the free flow of personal data and the protection of individuals.

The 95/45/CE Directive sets certain basic principles such as the quality of the data and the legitimacy of data processing. It also provides data subjects with the right to information, the right to access and the right to object. In the scope of the EU privacy Directive data controller has important responsibilities and obligations such as the confidentiality and security of processing. Finally, the processing of sensitive personal data is prohibited unless the data subject has given his explicit consent.

In 2009 the Article 29 Working Party, has published an opinion about the online social networks (WP 163). This opinion focuses on the way in which social networking sites can meet the requirements of European legislation of data protection. It is mainly intended to provide guidance to the OSN providers and the measures to ensure compliance with EU law. Thus the Article 29 WP sets out the obligations of OSN providers:

The service operator should inform users of his identity and provide clear and comprehensive information about the purposes of processing personal data and the various ways to do this. Specifically: The OSN provider must set up the default settings respecting of privacy. He must inform and warn the users against the risk to privacy when they upload data on social networks. He should recommend that users not upload pictures or information about other people without the consent of those concerned. He must include in the homepage a link to a "complaints office" for the members and non-members. The commercial activity must obey the rules established by the EU Privacy Directive and the E-commerce Directive (2002/58). He must provide a maximum period for storing the data of inactive users. Inactive accounts must be deleted. He must take adequate measures to limit risks to minors.

B. U.S. legislation and the Safe Harbor

On the other hand, the existing context in the USA creates obstacles against the establishment of a protecting framework of privacy. For the Americans, a very strict regulation creates problems in the development of the Internet. Thus, the USA law tends to favor the commercial activity rather than the consumer's activities, while the case law tends to ensure the freedom of expression. Regarding the online protection of personal data the United States have no comprehensive law equivalent to the European Directive. Although they have signed the OECD Principles, the regulatory privacy framework consists of the legislative regulation and self-regulation, rather than follow exclusively the letter of law.

The privacy legislation tends to intervene *ad hoc*, under special circumstances. In fact, the right to privacy is somewhat overvalued on the other side of the Atlantic, where the economy imposes the rules without restrictions imposed by the law.

The origin of this phenomenon is the conflict between the right to freedom of expression and the right to privacy. The priority of the first one is rather obvious when it is explicitly guaranteed by the First Amendment of the Constitution while the right to privacy is an implicit right as interpreted by the Supreme Court of the U.S.

While there are certain rules that protect privacy, there is no law which lays down specific rules concerning the collection, storage or use of personal data. The Federal Trade Commission is the only body having authority over such activities. It enforces laws, but it cannot create new ones.

In general, in the USA, the one that can access data has the right to process, even if such data is collected without permission. The eHealth Insurance Portability and Accountability Act of 1996 (HIPAA), and the Fair and Accurate Credit Transactions

Act of 2003 (FACTA), are two examples of U.S. federal law with provisions that tend to promote the efficiency of information flow and the benefits of its exploitation over the rights of individuals to control their privacy. The Privacy Act of 1974 -the most important law on citizens' privacy- applies only to processing by the federal government and does not regulate processing in the private sector.

Although the Supreme Court has interpreted the right to privacy in the case of *Griswold v/Connecticut*, very few states recognize the right to privacy, with the remarkable exception of California where several social networks are located. An inalienable right to privacy is included in the first article of the Constitution of California from which several laws have been promulgated to protect this right.

The California Online Privacy Protection Act (OPPA) of 2003 forces the OSN operators who collect personal information from California residents to publish very clearly and obviously a privacy policy and to comply with it.

A Bill on privacy in social networks has been proposed recently. California social networking Act (SB 242) would set limits to the service operators, indicating that profiles should be private by default. Within that framework, users had to adjust their privacy settings during the registration process and the only information shared by default would be the username and the city of residence. It would also be required for administrators of social networking sites to remove any information after a request from the user within 96 hours. The implementation of such legislation would be too protective for the standards of Silicon Valley and since it would limit the business activities of social networks, the project was rejected by the Senate. The OSN companies strongly opposed this legislation. (Facebook also called the Act, a "serious threat" to Facebook).

American companies of OSN services have reacted in the same way about the proposed Bill called SB 761 "Do not track Act". In the same context, this Bill prohibited any selling, sharing or transfer of sensitive data concerning a consumer. Facebook opposed the establishment of such legislation arguing that it is unnecessary and a menace to California's economy.

Obviously, not only the framework but also the aspect of the privacy in the U.S. is not the same as in Europe. Besides U.S. law protects only the residents of the United States, leaving out the regulation of processing of personal data transferred from Europe.

The various social, political and economic relations between European countries and the U.S. have created a gap in the privacy which does not facilitate the free flow of data and the development of the economy based on the exploitation of information.

The implementation of the 95/46/EC Directive could therefore limit the ability of U.S. organizations to get involved in any transactions with European counterparts, because it prohibits the transfer of personal data to non-EU countries that do not meet the adequacy standard for privacy protection.

Accordingly, the U.S. Department of Commerce has developed the "Safe Harbor" in order to provide a way for U.S. companies to demonstrate the conformity to the directives of the European Commission and thus to simplify business relations.

The European Union approved the Safe Harbor in July 2000. Organizations that join this plan are certified as providing "adequate" protection under the terms of the Directive, allowing transaction between these organizations and European organizations to proceed easily and comply with the law.

Several OSNs have joined the program. However, the notion of "adequate" and the effectiveness of this system has been challenged since there is a big difference

between the two systems because the EU are in favor of regulatory protection, while the U.S. rely more on the self-regulating private sector [KOBRIN 2004].

C. The impact of the strictest legislation on the field of OSNs

At the time of cyber globalization user's trust support the financial development and presupposes guarantees for the protection of their privacy. Despite legal differences, all countries face common challenges in the field of cyberspace. In this sense all States want to ensure prosperity of its citizens by intervening for strengthening the digital economy as well as for the protection of rights against online dangers. In this way the marketplace is influenced by the initiatives of lawmakers.

In 1948 the United Nations General Assembly proclaimed the Universal Declaration of Human Rights, which contains a clause on the right to privacy. In 1981, the Council of Europe produced the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Subsequently, the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* deal with the exchange of information and proposes a set of guidelines on the collection and the exchange of personal data. These guidelines recommend information be always collected directly from the individual and used only for the primary purpose. They also suggest the person be informed of the operation, have access and be able, if necessary, to correct it. They further recommend appointing an independent officer to ensure the application of clauses on the protection of privacy.

The democratization of the digital world as well as the overall participation in social networks indicate the urgent need to implement initiatives to resolve in a fair and uniform way the circulation of personal data over the Internet. The new digital environment of socialization creates the need for special standards required to obtain a legal status that could better protect human freedoms and promote the global economy.

OSNs are worldwide services directed to clients with different cultures connecting them to interact instantly. In social networks users develop solidarity links. In the digital world the strength of the diffusion can easily deconstruct the public image of a company (see the scandal of Beacon application in Facebook). The compliance with legislative requirements strengthening the protection of privacy creates a secure and confidential environment, which is obviously desirable by all OSNs. The adoption of such a perspective by one of them, multiplies simultaneously the conditions to be prescribed for other competitors who want to attain in the same way the reliability and consideration of Internet users.

Within this context it is worth recalling the example of Microsoft that has pledged to modify its *Passport authentication system*, after the publication of the opinion of Article 29 WP relating to the online authentication services (WP 69). In this document the practice of Microsoft was examined with great criticism. The Article 29 WP said that the development of online authentication services should respect the principles of data protection provided by the 95/46/EC Directive and the national laws.

Since then users can get more information and make a choice about which data they wish to provide and the conditions under which this data is processed by Microsoft or sites involved.

Microsoft has decided to apply the new requirements not only to European users, but all users. Microsoft's strategy in building the confidence of its customers is not planned by chance because the distinction of implementing privacy rules depending on country could jeopardize its reputation. In the same direction in 2009, Facebook

decided to make very significant changes in favor of privacy following the recommendations of Privacy Commissioner of Canada. These changes applied to everyone and not only to Canadian people.

These examples indicate that globalization of OSNs can contribute to the harmonization of legislation concerning the protection of personal data on social networks just because OSN providers due to technical, financial and political reasons cannot differentiate their policy according to the residence of their members. In consequence, the guarantees laid down by the strictest legislation tend to provide the same level of protection for all users [WU 2005]. From this perspective, countries can participate in discussions detailing the requirements for the protection of privacy and focusing on their implementation.

D. The European Privacy framework within social networks

In Europe the current governing privacy law is the 95/46/EC Data Protection Directive which has been viewed as a leader in the regulation of data privacy for several years. Understanding the challenge of new technologies and the web revolution, the European Commission has published recently its proposals to reform the EU's Data Protection Directive. In the scope of the modernization of the Directive some significant changes are proposed such as the implementation of one law and a single DPA for each business to be determined by the Member State in which the business has its main operations, the simplification of transfer to non European countries, the establishment of «the right to be forgotten», «the right to data portability» and the principles of «privacy by default» and «privacy by design». Moreover, specific rules on consent and special protection of children's rights are inserted in the proposal as well as the implementation of the Mandatory Data Protection Officer. Finally, general notification requirement is abandoned and violations become more expensive.

These changes will fortify the privacy of OSN users. However, some issues in the field of social networks seem to remain obscure. In particular, the gap of privacy conception, the multi-level involvement of participants within social networks, the OSNs interoperability and the classic issue of law enforcement reveal that special attention has to be paid to the regulation of social networks.

There will be at least two years before the new privacy rules are in force, and many provisions may be modified or removed during the revision process. Nevertheless, the new framework proposed by the EU, and the position taken on certain issues raise thoughts and influence policymakers worldwide. In fact, the Obama Administration has already unveiled a «Consumer Privacy Bill of Rights» as part of a comprehensive blueprint to protect privacy. The Bill is intended to bring about conformity to the privacy principles that have become the norm in other countries such as in Europe.

The 95/46/EC Directive combines the principle of the submission of processing to the national laws of the State in which the data controller is established and performs processing or, if not based in the European Union, to the national law of the State in which the means used by the controller are located. At this point, several issues raised mainly by the definition of data controller simply because in the field of social networks too many participants are involved in the process (OSN operator, affiliated companies of OSN operator, application providers, users, other third parties) and as a result it is not clear where data is located and by whom it is processed.

Given that the applicable law is the law of the establishment of data controller in which the processing takes place, the decisive criterion in finding the applicable law is not the place where the processing is performed entirely or partly, but a) the place of

the permanent establishment of the controller and b) the framework of activities of each establishment. It is therefore necessary to evaluate the level of involvement of establishment activities.

Nonetheless the problem relies on the multiple OSNs' locations. Moreover, data is collected and processed via a common platform which makes it difficult to find which data is processed by whom and where the establishment is. In this direction the reform of EU Directive tries to give a solution omitting the condition of the equipment used and installed within Europe. It focuses on a single set of rules on data protection, valid across the EU and the application of these rules even to companies not established in the EU, if they offer goods or services in the EU or monitor the online behavior of European citizens.

However, the issues remaining are the conflict of different legal privacy systems; the eventual constant delocalization of services as well as the force of implementing such rules when companies are situated outside the European boundaries (remember the famous Yahoo case). In fact, the issue of the application of legal requirements exists already and many OSNs are not complied with it.

1. The consent

In privacy the concept of consent plays a major role. To begin with, it is a form of control related to the fundamental right of personal autonomy. In addition, the valid consent presupposes transparency that leads to the lawful processing of personal data. The Article 29 WP in its opinion dealing with the definition of consent highlighted the validity of consent under the applicable legislation (WP 187). Specifically:

- Consent may not be valid if the subject is not able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent.
- The consent must be given with respect to different aspects of processing, clearly defined. It cannot cover "all legitimate purposes" followed by the data controller.
- Due to the uncertainty as to whether the lack of action is intended to indicate your consent, "not to click" cannot be considered unambiguous consent

At this point - and without interfering with the illegal collection of personal data without the knowledge of those involved - it must be notified that by using OSN service, users give their consent to a) OSN operator by registering, after accepting the Terms of Use and the Policy of the site and b) application providers, when installing applications. In the first case OSN users usually provide a non-exclusive, transferable, sub-licensable, royalty-free, worldwide IP license. However, the user, when surfing in the great number of privacy policy pages, cannot find an explicit and clear clause defining the categories of the processing and the purposes of OSN operator as data controller. Besides, "general consent" of the data subject is not consent within the meaning of Article 2 § 2 h) of Directive 95/46/EC. In the case of processing by application providers the consent validity mainly depends on their privacy policies. However, it is true that many providers linked to OSN do not define clearly their privacy policies or they don't have any at all. The problem here comes down to user's confusion with respect to the purposes of processing. The users give exclusively the application provider the right of access to their data but there are often clauses stipulating that personal data will be processed for commercial purposes that are not assessed or read by the user. Furthermore, regarding the installation of an application, the user must agree not only to the processing of his personal data directly by the application provider, but also to transmitting data from OSN operator to the application provider.

Subsequently, according to Articles 10 and 11 of Directive, the data controller is responsible for informing data subjects. The Article 29 WP stipulates that this information must be in plain text, without jargon, in a comprehensible and prominent manner and more information must be given directly to individuals as it is not sufficient to just have the information "available" to them.

According to the position of Article 29 WP, data controllers should seek to examine, after a certain time, the choices of data subjects, for example, by informing them of their current choice and offering them the opportunity to confirm or withdraw their consent. The data subject must also be properly informed about the particular risk of data transfer to a country that lacks adequate protection. Finally, information properly adapted for children, is recommended.

As regards the voluntary disclosure of data subjects it should be specified that the European Directive 95/46/EC places sensitive data in a different system in comparison with non-sensitive personal data. For this category of data, the processing is prohibited with the exception of Article 8§2 of the Directive. This provision allows among others the processing of sensitive data in cases where data is clearly made public by the data subject. Given that privacy settings usually make information public by default, all misinformed people are no longer protected. In general, OSN operators make no distinction for sensitive data circulating on the site.

By evaluating the quality and proportionality of the information provided by data controllers within the OSNs, it is true that the validity of consent is not certain and it is doubtful if new rules will also be respected by the providers of the service.

2. The rights of data subjects

In compliance with the 95/46/EC Directive, the OSN operator must ensure the right of access and opposition. In this sense some social networks dispose some tools facilitating the exercise of these rights of Internet users.

Furthermore, if a user decides the deactivation of his account, Social Networking sites often maintain copies of certain documents for technical reasons, while the duration of this retainment is not specified. The Article 29 WP specifies in its 5/2009 opinion that the service operator should make inaccessible the profile of an inactive user and delete it after a while.

The modernization of data Directive will also establish the "right to data portability" so that can users access and transfer easily personal data from one service provider to another (e.g. from Facebook to Google+). Although this idea is expected to encourage competition between services, it raises some risks and practical difficulties.

The portability of data should be made with respect to the article 5 b of the Proposal for a General Data Protection Regulation or the Article 6 of the 95/46 Directive, which stipulates that personal data should be collected for specified, explicit and legitimate purposes and not be further processed in a way incompatible with those purposes. In the application of data portability there is also the risk of the automated collection of user information without the operator's consent and the risk of failing to identify the user requesting the transfer. Finally, the data portability depends always on technical conditions such as the format of the storage data in order to exchange it.

The reform of the Directive will also provide OSN users with «the right to be forgotten» by which users will have more control of their online privacy. However, it is argued that the «right to be forgotten» may stumble upon the speech rights of others. Facebook Company believes that the «right to be forgotten» is against the will of the users who leave intentionally their traces on network. This aspect, which is

shared by many providers, reveals the fact that the «right to be forgotten» will be effective on condition of its acceptance in an international basis.

3. The data transfer

With regard to the processing of personal data outside the European Union users usually give their consent for transferring their own data to other countries.

Within the European Directive the transfer is permitted exclusively to countries that provide an adequate level of protection. For personal data transfers to countries with no adequate protection, there are legal instruments providing guarantees such as contractual clauses adopted by the European Commission and *Binding Corporate Rules*. However, despite the contractual commitments, the issue here looks like that of the cloud computing when the data is processed all together from a common platform and that creates obstacles to the determination of the location of processing.

4. OSNs' users as data controllers

In an interactive context users can qualify simultaneously as data subjects and data controllers or processors [WONG 2009, VAN EECKE 2010].

This happens when both parties mutually define the purposes (for example online communication or data storage on the cloud) and the means/conditions of processing (permission of the persons having access to their information, selection of certain applications installed and duration of the availability of personal data). Indeed, every network member that posts data legally or not, can be considered a controller with the exception of the purely personal or household activity (Article 3 § 2 of the Directive).

On the other hand users often publish personal data of other persons by determining on their own the purposes of such processing. In this case OSN operator is considered the processor, thus it is the one that sets rules and conditions**.**

Article 3§2 of the Directive excludes the liability of users processing personal data within an exclusive personal or household activity. However, it is very difficult to demonstrate the nature of the activity in which a person interacts on network, and here comes the theory of limits of the "private sphere" on the Internet.

The subjectivity of personal objectives as well as the complexity of the OSN architecture tends to complicate the notion of *interactive activities*. Where are the limits of such private activity and which elements can lead to the reliable qualification of an activity as public or household? The Court of Justice (ECJ) has expressed its position in the Lindqvist decision [ECJ dec.of 6/11/03, Bodil Lindqvist, C-101/1]**.**

In this case, a Swedish Internet user disclosed, on web page information about herself and her colleagues, including their full name or their phone number. She also noted that one of those had been injured. She had not informed her colleagues, she hadn't obtained their consent nor had she notified the Data Protection Authority.

The ECJ decided that the operation of mentioning on an internet page details about various persons and identifying them by name or by other means constitutes processing of personal data. The Court also mentioned that household activity refers 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 is made accessible to an indefinite number of people*». Moreover, the Court affirms that, within the meaning of 95/46 Directive, the notion of «*data transfer to a third country*» does not exist.

By applying the contributions of this jurisprudence in the field of social network, it is clear that the disclosure of personal data from an "open to everyone" profile cannot be considered as an activity exclusively personal or domestic provided that this information is available to an indefinite number of people. The same argument holds

for any publication containing personal data that is adjusted to allow "access to everyone". However, the practice of OSNS challenges the "access criterion" of an indefinite number of persons. Since users can adjust the privacy settings of their profile, they can restrict access to certain persons and define a private club of friends who have access to specific data. Whether these are 5 friends, or 300 friends; they can be clearly defined by the disseminator of information. But even if the user makes an exclusively personal use of social network, the publication of any personal data which is available to 300 Internet users will not probably fall within the field of a private or household activity.

However, the constant disclosure of a considerable amount of personal data to a limited circle of people creates uncertainties in terms of qualification as private activity. It is clear from this observation, that the number of people who have access to personal information is only an indication of the application of the *household exception*. The reliable criteria could be defined not only by the number of people having access but also by taking into account a combination of elements such as the objectives of the distributor, the nature of each publication, the quality of the recipients and the implementation of privacy settings.

On top of that, it is obvious that users of social networks have neither consciousness nor the appropriate means to fulfill their obligations as data controllers. As mentioned, data controllers must comply with certain basic principles such as the principle of proportionality and that of legitimacy according to which any processing should be performed only under the conditions of Article 7 of the Directive. As far as the users are concerned the requirements are limited to cases of point 7 a) which presupposes the unambiguous consent of the person and point 7 f) which requires the existence of legitimate interests pursued by the data controller.

In practice, OSNs' users are posting personal information of others without first requesting permission of those involved. In reality, users are not familiarized with the idea of personal data and they overestimate the significance of rights violated. In legal terms, the disclosure of personal information of third parties may be legally based on the achievement of a legitimate interest of users. However, the law requires a balance of conflicting rights, which is once again related to the fact that people must have a good knowledge of the data controller's responsibility.

In addition, we need to highlight the fact that a data transfer to a different data controller (for example to the operators of applications using user's friends list) is secondary processing in which case the user is incompatible with the principle of legitimacy unless it is based on the exception of household activity.

Furthermore, users are unable to protect personal data against accidental or unlawful destruction, unintentional loss, alteration, disclosure or unauthorized access to data published on the network. Although a user can determine the purpose of publishing personal information online and the terms of such publication, he remains incapable of ensuring the security of released data simply due to the lack of information control. Based on the online information, the user is limited to means provided by the service operator. To explain that, a user can partially authorize access but once the information is published, it moves away from the sphere of influence of the user. The nature of social network does not also allow the fulfillment of other formalities such as the information obligation simply because that depends not only on the intention of the publisher but also on the will and the privacy settings of other users. Often the unsubscribed persons do not have access to user profiles dealing with their own personal data and they can not oppose processing. Consequently, there is a practical difficulty in the exercise of the rights of third parties.

From another point of view, the user has certain obligations as data controller when transferring data to a third country. First of all it is necessary to clarify the notion of transfer within the social network. According to the ECJ *« There is no 'transfer to a third country' within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, Thereby,, making those data accessible to anyone who connects to the internet, including people in a third country »*. Interpreting this jurisprudence in the field of OSNs as long as the operator possesses his own site hosting facilities in the United States, there is a data transfer to a third country and the explicit consent of data subjects is required. However, the adoption of standard contractual clauses for the transfer of personal data outside the EU between OSN operator and each user does not seem a realistic option.

Although the operator, processes personal information of third parties as data processor (theoretically on behalf of the data controller), he remains autonomous and independent and users who are data controllers cannot provide appropriate directions to the operator (the data processor)

However, it should be mentioned that the jurisprudence of the European Court does not entirely comply with the complexity of participants in social networks. In addition, the application of certain rules of privacy can be extremely difficult -if not impossible- in the social network. The role of the OSN operator is predominant in the protection of user's privacy. The operator has almost all the technological means for implementing the system for the proliferation and exploitation of personal data. Users are considered in some cases data controllers but they lack the autonomy to set the framework within which the processing takes place nor can they meet their obligations because they are always subjected to the rules and technology laid down by the OSN operator.

5. The installation of *cookies*

OSN operators as providers of electronic communications services are also subject to the obligations of the 2002/58/EC Directive as it has been amended by the 2009/136/EC Directive. However, the obligations imposed are not met in their totality by OSNs. For example, the use of cookies on OSNs does not comply with the requirements of European privacy system. In particular, Article 5 § 3 of the Directive allows storage of data, in a user's computer provided that the user is informed about how the data is used, and whether he can refuse this storage operation. Data storage for technical reasons is exempted from this law. The problem in this field lies in insufficient information to users. OSNs usually notify users about the need to use cookies as well as the possible use of personal information by advertisers. Nevertheless, they do not always specify the types of cookies used or the duration of their retainment.

The e-Directive demands clear, accurate and complete information of users about the purpose of cookies as well as a right to oppose, consecutively exercised by making choices in the browser. This puts into question the information provided by the site regarding the use and the "opt out" of cookies.

However, the Article 2.5 of 2009/136/EC Directive which amended the e-Directive sets a new regulatory framework of the right of each user to accept or reject explicitly the installation of a cookie in his terminal. In the scope of such regulation rather than the "Opt out", the OSN providers must obtain the explicit consent of their members and shall adopt an "Opt In" system to be able to store cookies on the hard disc.

III. The alternative methods of regulation

The market demands the free circulation of information that should include personal data with the minimum of legal or regulatory barriers. The international order takes into consideration the importance of trade, the freedom of information flow and the freedom of expression. The regulation of processing personal data on social networks seems more than ever necessary. In this context the EU and the OECD advocate the free exchange of information and the prohibition of restrictions on market.

Given that OSNs are developed in a free economy, the market rules are sometimes useful in the regulation of privacy. Nevertheless, these forms of regulation have major drawbacks especially in terms of control which involves their efficiency. Conversely the legal norms have the power to guarantee a better protection of personal data. However, the legislation on the threshold of the evolution of new technologies should be adapted to new requirements of the Web 2.

A. The market rules

Eric Przyswa wrote "*In the current situation, it seems preferable to let industries take the responsibility to clearly and quickly adapt to the challenges of the Internet rather than go headlong into repressive actions, even if sometimes necessary, but evading the real issues*". [PRZYSWA 2010]

Speaking about the economy of personal data we cannot underestimate the pressure of commercial trends and consumers' reactions that can shape the operators' practices. That can create normative standards in the scope of social networks.

1. The *Laissez Faire* model

Personal data, as information has a financial value for all businesses and the doctrine of *laissez faire* requests the maximum exploitation of this information. According to this idea, expressed by several philosophers and economists, like Adam Smith and James Mill, the market has the effective mechanisms to respond to consumers by creating a system which guarantees in the end the consent of data subjects. Social networks may therefore serve their members and their clients without any public intervention and with no legal constrains. In this regard social acceptability of practices used by providers plays indeed a vital role in regulating privacy.

This concept in OSN scope is explained in the following context: First of all OSNs are services provided by profit companies whose revenues depend on the usage of the service. The more the number of users multiplies, the more the turnover increases. If for any reason users unregister from the network, the OSN Company will lose money. Indeed social networks want their members satisfied. That's why they pay attention to public relations and organizes online deliberations before any review of their privacy policy. By targeting the loyalty of their members, social networks are always looking for a formula to succeed not only in users' consent but also in their active involvement in operating practices when processing personal data.

The *laissez faire* model is based on the rule that requires companies to be pleasant to its customers. In general, if an OSN uses personal data in an unacceptable way, users will withdraw their consent for such a use, they will stop sharing information or at worst, they will leave the platform.

In addition, when this network does not respect its commitments to privacy, that creates a sense of insecurity and it further has a negative impact on the reputation of this network just like the example of Beacon application on Facebook. As explained by Edwars and Brown, Facebook introduced an opt-in system, not because it was threatened by legal action, but simply because Beacon was a PR disaster and users were ready to leave the network if Facebook did not make any change.

The major failure of such a regulating method within social networks is the inability of OSN's users to verify that the Company complies with its own commitments concerning privacy. Control doesn't go through users because they don't have access to methods of processing (e.g. face recognition technology) and they only know the information provided by the operator. If, therefore, the information is incomplete, users do not have the capacity to confirm the operator's violations.

Subsequently, a positive image of the network to the "customer-user" can contribute to the creation of strong links of trust between users and the operator which is a vicious circle leading to the constant reduction of control due to this confidence.

Moreover, due to the nature of information, an unauthorized disclosure or any use of personal data without wide public acceptance is perceived only by the consequences. In this sense, personal data is protected only in the case of the revelation of an information flow because no one wants to publish such a scandal in security breach. To make it clear, we don't know what happens with our personal data until the time we learn (if we ever learn) about this from the media. On top of that this regulatory pattern rejects the rights of minorities who do not really have the force of influence. Assuming that a minority believes that personal data cannot be protected because of the photo tagging, these users would stop providing personal information, they would eventually delete profiles or photos so as not to be tagged, they would create a page of manifestation, they would send emails to inform their friends etc. However, any measures they took, they could never bring a change to the operator's policy in this field because the volume of all these actions remains limited.

2. S*elf-regulation*

In the absence of uniform social norms that can delineate the rights to privacy in the digital world, the establishment of rules laid down by the managers of a universal site, is significant and even necessary for the preservation of peaceful participation.

What characterizes the most famous OSNs beyond legal and cultural discrepancies is the common objective of communication. This goal gives to every OSN a dynamic force and on account of this common goal, users impose on themselves rules of conduct concerning the interaction within the site.

In practice, the regulation of online activities goes through the *contractualization of law* and it is very logical because OSNs provide services to people located all over the world so they must guarantee the fairness of rules imposed. The regulation by the terms of use of the site (agreement) is a well-known phenomenon in the digital world.

The OSN marketing requires good relationships between managers and user in favor of the last one. Therefore OSN does not ignore the value of the dialogue process. Apart from the fact that OSNs enable the creation of open discussion groups with regard to the protection of personal data, they also dispose sections dedicated to informing people about safety tools and the adjustment of privacy settings.

The practice of self-regulation in OSNs also provides a quite interesting direction in competitive terms. If the model of regulation imposed by Facebook can contribute to the use of the site with the agreement of users, this fact is an indication of success of this regulation as a solution facilitating the interactions**.** The massive acceptance of terms of use as well as the increasing number of users daily connected, indicate that this market model, works well. However, as already stated, what is not always evident is the awareness of users regarding their rights protecting their privacy.

Certainly, these processes of dialogue among the parties of the network are developed in a theoretically democratic way but in any case they tend to strengthen the trust of users and especially the acceptance of good behavior as perceived by most of the community network. On the other hand, the function of law is not the creation

of a user-friendly environment but the guarantee of protection of fundamental rights and especially the protection of the rights of minorities.

3. Fair privacy Policies and Practices

With the aim of reinforcement of user's confidence Facebook in 2010 has joined the French Association of Community Internet Services (ASIC) which prepared discussions regarding privacy.

However, the same company (as well as Google) didn't want to join «The charter on the right to be forgotten» developed on the initiative of Nathalie Kosciusko-Morizet, responsible for foresight and development of digital economy. In this charter the signatories agreed to implement the principles of consent, the right to information and the right of rectification and opposition. The fixing of the storage duration and the existence of updating processes should allow respect for the principle of the "right to be forgotten". Thereby, we observe that while charters and best practices go in the right direction, they do not replace the power of the law, since the OSN Companies decide whether to comply or not according to subjective criteria that suits them.

4. The solution of Certification

The certification (*labeling*) is understood as a form of control by a third independent body which imposes a predefined number of commitments on the site operator.

In practice Facebook has a license of the *TRUSTe privacy program*® in accordance with the Safe Harbor framework as set by the EU and US Department of Commerce. TRUSTe ensures that Facebook provides users with sufficient information of its privacy practices. TRUSTe also intervenes to resolve the differences concerning confidentiality (TRUSTe Watchdog Dispute Resolution Service).

Nevertheless, this is a certificate issued by a private company, which calls into question the credibility of the certifier. Taking into account the reputation of these companies, they both benefit their business relationship. Facebook is always certified by TRUSTe whether it has obviously made violations to its own commitments or not, therefore the role of certification with respect to its control over the practices of processing is controversial [ROCHELANDET 2010].

The key question remaining is the monitoring mechanisms and penalties for breaking the rules that the company has given by itself. To sum up, for the adequate and credible implementation of the certification, it seems compulsory to use independent authorities and not private profiting certifiers.

B. A solution adapted to the particularities of social networks

At the time of explosion of new technologies and Web 2, it is true that legislation is no longer enough to guarantee alone the online privacy. The pace of the technological evolution is so fast that the legislator fails to frame it effectively. However, the principles resulting from the design of privacy permeate and affect the business practices of the services of the information society. Currently the European system is the most comprehensive on the protection of personal data which cannot be ignored by the most popular online networks. However, the explanation of this attitude cannot be summed up strictly to its compliance with legal requirements. The circulation of personal information and the main goal of social networking aim at the loyalty of every member. In the prospect of enforcing the confidentiality of their members, OSNs decide which potential tools should be available to users in order to provide them with the sense of security and control of their digital identity which results consequently in the proliferation of a considerable amount of personal data [CAZIER 2007].

This approach of the architecture of the integrated information flow to new practices and technologies of data processing is based on the respect and willingness of users to specify the terms of revelation of their data. This aspect of protecting privacy was proposed for the first time by the Information and Privacy Commissioner of Ontario Ann Cavoukian who suggested the integration of the respect for private life straight in the design and operation of IT systems and networks, and also in the development of responsible practices. Europe is also ready to establish this principle of «privacy by design» in the reform of 95/46/EC Directive.

Privacy by design is based on seven fundamental principles: 1) proactive and preventive measures rather than reactive and remedial measures; 2) privacy by default; 3) integrate the protection of privacy into the design of systems and practices; 4) full functionality in a positive-sum paradigm; 5) safety from beginning to end; 6) visibility and transparency; 7) respect for user privacy.

In front of the challenges of data protection in the online digital world, the legislative trend seems to favor the privacy by design, which will probably create new responsibilities for OSN operators. In these circumstances, OSNs should evaluate the advantages and benefit from an initiative to control personal information, thus limiting the risk of user's privacy and strengthening their trust at the same time.

IV. Conclusion

As for the privacy protection on online social networks we fall on the classic question of the effectiveness of legislation in an international digital environment quite complicated. Nevertheless, the control of a public institution and the force of sanctions are standards necessary for the protection of personal data.

On the other hand, we cannot refuse the contribution of approaches developed in the liberal aspect of the influence by the market, which can also form a more reliable framework. Finally, by taking into account the particularity of the digital environment of Social Networks, a minimum harmonization in the principles protecting privacy could lead as well to the reformation of the architecture of information flow which seems to have high effectiveness thanks to users.

Social networks are powerful tools of interaction. In this instance the excessive alarmism is not suitable. Unlike what has to be viewed with skepticism is the uncontrollable margin of autonomy of every online service provider in the effort to create a more personalized web by making financial gain without respecting the principles of transparency and proportionality. This trend is forcing social networks to expose by default more and more personal data. Besides, it is true that everyone wants a more personalized WEB. Though, WEB should not be social by default. In this sense the rules of protecting privacy in social networks are essential.

Despite the existing divergences between legal systems as well as the various modes of regulation, OSNs are promoting the global socialization, the right to the information society and democratic participation. Therefore they should be regulated collectively. However, the key question lies in what the user scarifies in return. In lack of information what user loses is his self-management.

Of course any state intervention in the way that users manage their own personal data would cancel all the guarantees of protection of privacy and the rights and freedom. Instead, the establishment of a regulatory system more oriented toward user information and prevention can contribute to the safe use of social networks

Obviously a minimum harmonization in basic principles ruling activities on OSNs is advisable. However, the Facebook case indicates once more the gap of values in the right to Privacy and the difficulties of the legislator to adapt to a digital world in

constant transformation. Ruebhausen and Brim argue that «*The essence of privacy is no more, and certainly no less, than the freedom of the individual to pick and choose for himself the time and circumstances under which, and most importantly, the extent to which, his attitudes, beliefs, behavior and opinions are to be shared with or withheld from others*» [RUEBHAUSEN&BRIM 1965]. In the era of social media the great majority of users are poorly informed or without the ability to understand the new online technologies, which leads to a perception of privacy as the price of the participation to the global online community. Briefly, the key issue is not finding the measures to protect privacy in social network, but how to ensure the freedom of choice. This freedom presupposes the awareness against the risks of exposure and digital intrusion of personal information to others.

Since each individual defines his private life according to his ability or his desire to manage the disclosure and the use of such information, the management of privacy falls on individual skills. Therefore, the priority is rather teaching people to manage their digital identity on social networks. In this way users could participate strongly informed in regulating online privacy since their reaction defines the business practices of service providers. The dependence between service provider and users is bidirectional so that despite the imminent threats of the WEB 2, service providers cannot do anything but correspond eventually to the demands and requirements that can be formed not by any one user but only by conscious users of OSNs.

References:

-Stephen J. Kobrin (2004), *Safe harbors are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance in* Review of International Studies Vol. 30 British International Studies Association, 111-131

-Yves Poullet (2000), *Les Safe Harbor Principles - Une protection adequate?* online at http://www.juriscom.net/uni/doc/20000617.htm

-Joel R.Reidenberg (2001), *L'encadrement juridique de l'internet aux États-Unis* , in proceedings L'internet et le droit, droit français, européen et comparé de l'internet organisé par l'École doctoral de droit public et de droit fiscal de l'Université Paris I les 25,26/9/00, Collection Légipresse, Paris,139-156

-Tim Wu (2005), *The International Privacy Regime,* in Anupam Chander et al., Securing Privacy in the Internet Age, Stanford University Press, 91-107

-Rebecca Wong (2009) *Social networking: a conceptual analysis of data controller,* Communication Law Vol.14, No 5,142-149

-Eric Przyswa (2010) *Cybercriminalité et contrefaçon*, FYP

- Lilian Edwards, Ian Brown (2009), *Data Control and Social Networking : Irreconcilable Ideas?* in A. Matwyshyn Harboring data: Information security, law and the Corporation, Stanford University Press

- Patrick Van Eecke, Maarten Truyens (2010), *Privacy and social networks,* Computer Law&security Review 26, Elsevier, 537-539

-Fabrice Rochelandet (2010), *Économie des données personnelles et de la vie privée* , la Découverte, Paris, 94-96

-Joseph Cazier et al.(2007), *Sharing information and building trust through value congruence,* Information Systems Frontiers ,vol. 9, N^{o} 5,Springer, 515-529

-Oscar M. Ruebhausen, Orville G. Brim (1965), *Privacy and behavioral research,* in Columbia Law Review, Vol. 65, No. 7, 1184-1211