SAFEGUARDING PRIVACY IN SOCIAL NETWORKS

Submitted: 24/05/2019
Revised: 20/06/2019
Accepted: 22/07/2019

David López Jiménez*
Patricia Vargas Portillo**
Eduardo Carlos Dittmar***

Abstract

Purpose – The purpose is to examine the degree of privacy protection in the social networking field. In this sense, we analyze the benefits of the self-regulation of the industry as a complement to the regulations.

Methodology/approach/design – We study the Spanish and the European regulations regarding personal data protection with respect to social networks.

Findings – The legislative regulations on this subject are insufficient due to their intrinsic limitations in the field. Therefore, we should encourage the approval of good legislation that complements and fills the gaps.

Practical implications – The advantages that are derived from the research on this subject are useful for service providers and the public and private sectors in the information society. Therefore, they are useful for society in general.

Originality/value – This research article includes the examination of the general utility of society. The aspects that are addressed are applicable to the industry and those who use social networks. The government must prevent infractions that damage consumers and/or users.

Keywords: Data Protection. Digital Economy. Privacy. Social Networks. Telecommunications.

INTRODUCTION

New technologies provide numerous advantages for those who use them; however, on occasion, certain problems arise as a result of their improper use. An

*Full Professor. EAE Business School, Madrid, Spain. Fellow at the University of Brasilia Center on Law and Regulation. Address: Joaquín Costa, 41, Madrid, Spain. E-mail: dlopez@eae.es.
**Senior Lecturer. ESIC Business & Marketing School, Madrid, Spain. E-mail: vargasjennypatricia@gmail.com.
***Senior Lecturer and Associate Dean. EAE Business School. Madrid, Spain. E-mail: ecdittmar@eae.es.

example in this regard relates to social networks and the potential privacy problems that may arise.

We are in an environment in which dignity and freedom are at stake. One must staunchly defend privacy using the law and self-regulation. The loss of personal data protection as a consequence of the implementation of new technologies is intolerable.

It is not easy to provide, a priori, a definition of the concept of privacy. An extended definition, although surpassed, was provided at the end of the 19th century by the American judge Cooley, who pronounced that privacy is "the right to be alone" and to be at peace (COOLEY, 1888).

The specific definition that is set forth will depend, to a great extent, on the specific term that we use: personal data protection. The important issue, more so than the legal designation, is that it is a fundamental right whose content is made up of different instruments that integrate personal data protection with a core that is unavailable even to legislators (LUCAS MURILLO DE LA CUEVA, 1999; GUERRERO PICÓ, 2006; REBOLLO DELGADO, 2008; McDermott, 2017).

The emergence of new technologies with a marked social character—blogs, wikis, podcasts, social networks, etc.—has created a high degree of interconnectivity among Internet users, allowing them to exchange opinions on different products and experiences with other people. The arrival of Web 2.0 has been a revolution since the user possesses a new role within the medium. That is, the user stops being a mere spectator of content and becomes one who chooses content, participates and creates content. In summation, Web 2.0 is a more collaborative approach that allows users to access and create unlimited knowledge, and as a result of this interaction, new business opportunities are generated for companies. Given that this is the reality, we must recognize that we are faced with a scenario that is subject to frequent privacy violations (BORGOHAIN, KUMAN, and SANYAL, 2015; PETRUCCO, 2019). In the present study, we limit ourselves to analyzing privacy in the field of social networks and highlight the extraordinary virtues that self-regulation from codes of conduct provide.

EFFECTS OF NETWORKS ON THE FUNDAMENTAL RIGHT TO DATA PROTECTION

In the electronic age, there is considerable concern about the individual right to privacy (CASTILLO JIMÉNEZ, 2002; OLIVIER LALANA, 2002; PRIETO ANDRÉS, 2002; ADAMS, 2017). The sense of freedom that the potential consumers have or users experience on the Internet is false and only

superficial. In fact, the user is unaware that any activity occurring in the electronic world leaves traces that can be followed and that, on occasion, will be exploited for spurious purposes (ROSSNAGEL, 2003; BALLESTEROS MOFFA, 2005; Spiekermann, 2015).

Currently, personal data have extraordinary value. The personal profiles that are built are bought and sold at considerable prices. Worst of all, buying and selling personal data violates our privacy because, in many cases, these actions are not at all known, let alone approved (ZARSKY, 2013; BARBANELL, 2015; CARPENTER, 2016).

The term personal data refers to the physically identified or identifiable information about a person. Such data are considered personal data regardless of whether the data refer to oneself or to a third person.

Privacy policies constitute one of the relevant legal points that must be taken into account when developing activities related to interactive advertising, electronic procurement and other related matters. The importance of policies goes far beyond simple compliance with the current legislation (Marotta-Wurgler, 2016). In effect, with policies, it is not just a matter of guaranteeing the fulfillment of a set of normative obligations because their content, on numerous occasions, goes beyond them and covers a certain legal void. This extreme can be linked to both the advocacy work of legislators regarding self-regulation - of which privacy policies are a manifestation - and that the companies themselves significantly value the privacy concerns that citizens generally express.

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (general data protection regulation, GDPR)is the basis for the changes in the privacy policies of WhatsApp and Instagram (both owned by Facebook).

The Council of Europe and then the community legal order developed complete regulations that incorporate sets of rules for guaranteeing individual data protection rights. Such norms, which contribute to the creation of a truly European market that facilitates the free exchange of people, goods, services, and capital, are found in, among other documents, relevant community directives. For example, they were included in Article II-68 of the Treaty establishing a Constitution for Europe that was replaced by the Treaty of Lisbon on 13 December 2007.

THE PROTECTION OF PERSONAL DATA IN SPACES OF SOCIAL INTERACTION

The fundamental right to data protection, which is specifically defined in article 18.4 of the Spanish Constitution, must be differentiated from the right to privacy of Article 18.1 of the Spanish Constitution (which offers special constitutional protection to private, personal and family life). The law provides individuals with a set of powers that essentially force third parties to adapt or omit certain behaviors related to data privacy (DÍAZ ARIAS, 2008). As Constitutional Court Sentence 292/2000 states, this right gives its owner the power to "control the use of their personal data, including, among other things, the opposition of citizens to certain personal data being used for purposes other than the legitimate purpose that justified obtaining the data." In this sense, for our purposes, for several decades, those who believe that they retain control over the use of their personal data after having provided the data to a third-party perceive less invasion of their privacy than those who may suspect that they have lost control of their data (TOLCHINSKY, MCCUDDY, ADAMS, GANSTER and FROMKIN, 1981). The possibility of controlling our own information excludes control by others. Each person should be able to control the degree of privacy that he or she wishes to have and how far he or she wants to go without unjustified interference. In this last respect, we can, among others, highlight the Cambridge Analytica data scandal. In December 2015, the British newspaper The Guardian uncovered a scandal over the fraudulent use of the data of more than 87 million Facebook users. The Cambridge Analytica consultancy firm intended to use the data to manipulate the presidential election of the United States in 2016, which was won by Donald Trump (BECHMANN and BOWKER, 2019).

These progressively important electronic social spaces, such as social networks, are not exempt in any way from risks or possible malicious attacks (BERROCAL, 2013). In this sense, we are concerned with national, European and international organizations' competencies in the areas that are affected by the use of social networks. This has driven the development of standards and recommendations to ensure secure access for all users, including minors and the disabled, to these new virtual interactive instruments.

The main regulatory initiatives at the community level came from both the European Commission and the Article 29 Working Group. In Opinion 5/2009 of 12 June, they made certain statements regarding the privacy and the security of networks, social networks, collaborative websites and other interactive means on the Internet.

The need to legally and privately regulate personal data protection for social networks is based on, among other factors, the extraordinary importance of

the subjects we address. This includes addressing the volumes of important personal data that users - both minors and adults - publish in their profiles (which establish their true digital identities that facilitate the quick identification of their contact data, preferences and habits) and the risks to which they are exposed. Considering this, it is recommended that public authorities and private parties collaborate to address comprehensive privacy protection in social networks.

Next, we will analyze the concept of social networks, their modalities, the specific privacy risks that potentially exist, and the critical moments in which there may be further damage to personal data protection. We will also study the measures established by legislatures to ensure a greater degree of privacy protection, especially for vulnerable groups such as minors and the disabled.

Concept of a Social Network

Although it is a relatively recent phenomenon, the progress of social networks is persistent. The origin of such interactive tools can be traced to 1995, when Randy Conrado created the Web Classmates website to maintain or reestablish contact with former classmates, such as college, institute and university classmates. The growth model of such networks is based on a viral process in which an initial number of participants send email invitations for others to join their website.

Notably, these social networking services are powerful communication and interaction channels that allow users to act as segmented groups. They are also important instruments for concerted social activities of various kinds.

Before providing a definition of a social network, it should be noted that there is no unanimously accepted definition. In other words, there are as many definitions as there are authors who have addressed the subject. In fact, before defining a phenomenon social network, we must narrow our focus to differentiate a traditional social network and a virtual social network. The definition should, in any case, be based on the premise that a social network is a form of interaction between members and/or social spaces.

We can, in any case, define digital social networks as services that are provided through the Internet that are accessible through different technical tools, such as computers, mobile phones, and tablets, and that enable users to build profiles that provide certain personal information, such as text, images or videos, through which they will be able to interact with other users and locate them according to the provided data.

Modalities of Social Networks

The criteria that classify social networks are certainly numerous. In this regard, different types of parameters can be assessed, such as chronological parameters, territorial parameters, the content, the purposes of the networks and

the potential end-users. In this study, we will distinguish the typology of social networks that currently exist based on their contents. To this end, we can differentiate between generalist or leisure networks and professional networks without addressing that the former can be subclassified into different categories.

We must note the concurrence of common characters in these two types of networks. Thus, the two modalities are primarily used to contact different people. The way in which the latter will be achieved will be an invitation sent by the issuer, which must be accepted by the recipient. Such platforms enable interactions among users, for example, by sharing information, facilitating direct contact between users, etc. From here on, the possibilities for communication are unlimited.

Likewise, it should be emphasized that leisure social networks are, to some extent, a result of the personal data that they contain, which makes them more susceptible to violating the privacy of their users. Indeed, in the case of general social networks, unlike those of a professional nature, users both display their contact information - including postal and email addresses, telephone numbers, etc. - and they publicize their personal preferences in many areas. This means that the amounts and categories of personal data that are made available to all interested parties are significantly higher than those of professional social networks.

Leisure Social Networks

The primary objective of leisure social networks is to facilitate and enhance the personal relationships between the users who are their real or potential consumers. The generalist social networks, which we examine in this section, can be subclassified according to their purpose into three categories.

1. Social networks that are created to exchange information. They enable the inclusion of certain content - photographs, videos, and text - that can be viewed by those who, in principle, desire it. However, prior registration will allow interested parties to post certain comments relative to the aforementioned content and, in certain cases, rate it.
2. Profile-based social networks. This subcategory of social network tends to be directed to specific topics, and they thus establish powerful sources of information on a particular subject. This type of social network is currently being used the most.
3. Microblogging social networks. In this case, users write comments about the activities they are doing at any given moment. These descriptions, which are made by the owner of the space, will be edited in both their own profile and that of their contacts.

Professional Social Networks

This typology of social network is a tool for establishing professional contacts with other users. The personal data that are usually recorded in such platforms are professional because different companies, as well as the time period for which professional services have been provided, can be included.

Potentially Invasive Privacy Practices

Regarding personal data protection, this is precisely where the greatest number of situations that are potentially unfavorable to the rights of users occur. This is because social networks base their content on the profiles that the owners of social networks frequently register and update.

Notably, at the legislative level, certain situations are not specifically regulated at the national, community and international levels, which can actually arise as a consequence of the use of social networks and collaborative websites. The aforementioned absence of legal regulations with different territorial scopes (national, community and international) along with the vertiginous and unstoppable evolution of the services of the information society can lead to scenarios that make users doubt the defense of their rights. With regard to the moments in which the privacy of a potential user may be compromised, with respect to social networks, it is possible to distinguish the following three-time points.

1. When registering, there is the possibility that the privacy security of the profile is not configured correctly. Therefore, certain particularly sensitive data could, with relative ease, be exposed given that one's own profile and those of third parties (since some contact data for other users would also be visible) would be accessible by any interested person. In addition, it must be realized that, as a consequence of accepting the registration conditions, some social networks are able to transfer all of the content itself, including that which is voluntarily provided to the platform, which makes it possible for the social network to economically exploit the data and users. In any case, the consent that is given by the user must be granted from the moment he/she decides to accept the privacy policy and conditions of use of the platform. Notably, privacy policies should be transparent, accessible and clear.
2. Users participating in the network and the advertising content may represent significant risks for the owner and third parties. Although users voluntarily publish their data, the effects on privacy can have significantly greater impacts than what was initially considered since social networking platforms have powerful information exchange tools.

Regarding third parties, the data and images that may directly or indirectly affect them must be compliant; otherwise, the third parties will be entitled to demand their immediate withdrawal. The International Telecommunications Data Protection Group on March 4, 2008, approved the *Rome Memorandum* that states that "one of the challenges that can be observed is that most of the information that is published on social networks is done under the initiative of the users and based on their consent." We should not, in this regard, forget that social networks are based on making the maximum possible amount of personal information of the profile owner available to the general public. For privacy purposes, the complex legal situations that can arise have been considered, to a greater or lesser extent, by the legislation itself and by the complementary codes of good practice.

3. At the moment of unsubscribing from a portal, although this will have effects, the subscription will not be fully ceased. Indeed, for a certain period of time, Internet search engines, including Google, will include the profiles of users in their searches who may have already decreased their use of the social network and that particular individual's contact information, images, and linked profiles. In addition, it is possible that social networks retain the traffic data that are generated by the users in the system and then use those data as tools to classify and analyze their preferences for targeted advertising. In this regard, article 94 of the new Protection of Personal Data (LOPD in Spanish) addressed the rights to be removed from Internet searches. The aforementioned precept recognizes two specific modalities of the right of suppression, or the right to be removed, which are regulated in articles 17 of the GDPR and 15 of Organic Law 3/2018. Article 93 establishes the rights of "everyone" with respect to Internet search engines and article 94 addresses "social network services and equivalent information society services."

As for the specific risk assumptions regarding the privacy of potential owners of social network profiles, some are worth mentioning. Below, we provide a nonexhaustive list of these risks by making certain assessments with respect to each of them.

1. Receiving unsolicited emails, which are commonly called spam. Social network users have been experiencing this in recent years. The advances that social networks and collaborative platforms implement are modifying commercial practices. This redefines the electronic form of

offering goods and services through hypertargeted advertising according to user profiles, diversifies the market and creates new communication channels. Spammers can use the personal information that is available on social networks to collect email addresses so that when they send spam, it seems to be sent from their direct contacts. In this sense, an email that is received from the address of a contact is much more likely to be opened because it will appear to be a "safer" email. In addition, spammers collect information regarding hobbies or interests to create messages of interest to the user, which, together with being received from a known contact, will increase the chances that the user will open the malicious email and that the malware that it may contain will be activated. In other words, social networks have become powerful marketing tools for companies when promoting their products and services and have gained increasingly more ground. In any case, it should be positively determined that, thanks to the approval of the new GDPR, less spam is being received.

2. Installation and use of banned electronic behavioral monitoring techniques. In this sense, we note two instruments out of many that are relevant to social networks. First, the use of cookies by a platform will allow certain user data to be known while the user is connected to it. With these, one can know, among other things, the place from which the user accesses the web (fixed or mobile), the operating system being used, the most visited sites, the number of clicks performed, etc. Second, web bugs involve unconscious actions whose repercussions could go unnoticed. For example, to record and track the opening of a document - e.g., an email - over the Internet, an image that is linked to a server other than the one that hosts the page that we are visiting is included. These are one pixel by one-pixel graphics that install a program on the hard drive to read all cookies on it. When the page is opened, the server will be asked for that file, and the Internet Protocol (IP) address of the requestor will be registered. Requesting the linked image will allow the gathering of the IP address of the computer, the date and time that the page with the image was accessed, the browser type and browser version that are used by the consumer or user, the operating system, the default language, and cookie values, among other things. In this way, large amounts of statistical data are collected, and users are tracked. Preventing the use of the aforementioned devices or, at least, creating certain limits that guarantee privacy has been a recent priority for the EU and, of course, for Spain. Directive 2002/58/EC has addressed these issues by considering, for example, that using cookies is a legitimate

technique as long as the data owner is informed and, in turn, his or her consent regarding the use of cookies for a legitimate purpose is obtained. It is also worth noting Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications services and networks, Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation in the electronic communications sector. Regarding the new obligations that are imposed by the community and national regulations, they require obtaining consent and providing timely information to users to ensure that they are aware of the use of their personal data and the purposes. Specifically assessing the need to install persistent cookies is necessary because privacy risks could be reduced through the use of session cookies. In the case of installing persistent cookies, their duration should be reduced to the minimum based on their purpose.

3. Being a victim of manifesting criminal practices such as phishing and pharming. This type of scam aims to obtain personal information, especially access to financial services, by spoofing the appearance or the name of a particular bank. This phenomenon is often spread through spam. Paradoxical as it may be, it is common for users to use the same passwords across sensitive sites and to participate as members of various virtual communities, which means that if there is a security breach in any of these sites, the consequences could be extended to users' other portals because the same password accesses all portals. The issue is aggravated even more so when users employ the same passwords for financial operations.
4. The indexing of profiles by electronic search engines. On many occasions, social networks allow search engines to index user profiles, personal information and other linked contacts in searches, which poses a significant privacy risk and hinders the process of eliminating user information from the Internet.
5. Identity violations. There is the possibility of concurrent identity theft for certain users, who, without having previously registered on the platform, discover that their digital network identities already existed on the social network.

Considerations with regard to Minors and the Disabled

At the national level in Spain, with respect to the data protection regulations (Organic Law on Data Protection 3/2018, and Spanish Regulation 1720/2007 and the direct impact of the GDPR), we must distinguish two large groups for which there are regulations regarding obtaining consent. On the one hand, those over 13 years of age may give their consent regarding personal data protection except in cases in which, by legal imperative, such consent requires the assistance of legal representatives. On the other hand, minors under 13 years of age generally require the consent of their parents or guardians for processing personal data.

It also prohibits exploiting the incredulity and special vulnerability of minors, including those who have not yet become adults, in order to obtain various kinds of family information. This includes, for example, their professional, economic, sociological or other characteristics that require the prior consent of their owners.

In the case that data for minors is intended, the language that is used to collect such consent is applicable only to those over 13 years of age since, for minors below the age, the exclusive consent of their legal guardians is required. In addition, the language must be clear and sufficiently understandable for a minor according to the provisions of article 13 of the Development Regulation LOPD. This requirement implies the use of simple terminology and excludes technical terms, ambiguous terms or expressions whose effective understanding is arduous for a minor. Naturally, the comprehension and vocabulary that is considered intelligible for a 13-year-old child will not be equal to that for a child who is approaching adulthood. In any case, according to the spirit of the precept, we must consider that the intentions of the legislators are not to make distinctions with regard to the maturity of a minor throughout his or her natural evolution. Hence, the language that is used to seek authorization and consent to process the personal data of a minor should be clear and simple enough so that it can be perfectly understandable both for a person older than 13 years of age and for a child about to reach adulthood.

When an individual is less than 13 years old, the authenticity of the consent that is provided by legal guardians must be guaranteed. The person that is responsible for processing will be in charge of verifying that consent has been granted by the parents or guardians.

In any case, the social networks themselves have obligations to have technological means to guarantee users' ages. This issue arises in practice with relative frequency. In fact, the Spanish Data Protection Agency (AEPD, in Spanish) has condemned the lack of diligence in verifying the identification of a

child who was registered on a certain website whose data were used for advertising.

As a complementary matter, we should refer to article 84 LOPD, which establishes that parents, guardians, stewards or legal representatives of minors must ensure that minors have "balanced and responsible" use of digital devices and services within the information society to ensure the adequate development of their personalities and preserve their dignity and fundamental rights. This mandate, in fact, continues to be a reflection of what is established in article 154 of the Civil Code, which states that "parental authority shall always be exercised for the benefit of the children, according to their personality and respect for their physical and psychological integrity."

The Public Prosecutor must advocate the precautionary and protective measures that are outlined Organic Law 1/1996, of 15 January, on the Legal Protection of Minors when the use or dissemination of images or personal information of minors in social networks and information society services "may imply" an illegitimate intrusion into their fundamental rights.

The legal provisions that have been approved in Spain to ultimately ensure the privacy of minors are enforceable only at the national level. In contrast, the application of Spanish law cannot be demanded either in the community or in the international space because the law will not be applicable there. One of the greatest obstacles that arises when effectively guaranteeing and protecting privacy is the lack of legal instruments that affirm the extraterritoriality of the illicit behaviors of computerized information processing in relation to the physical territory. Some of the instruments have been used in the past. This last detail is especially relevant in the field of social networks.

ETHICAL NORMS AS A SUITABLE COMPLEMENTS TO NETWORK ACTIVITIES

Self-regulation in general and codes of conduct, in particular, are rarely addressed in legal studies. They have barely been addressed by doctrine and jurisprudence, although the legislature uses them to precisely promote and consolidate its validity in various fields that, in our case, are both electronic commerce and social networks.

It should be noted that self-regulation is strongly suggested by the legislator in different normative texts. One of the areas in which we aspire to achieve the full and effective use of the regulatory formula we analyze is in social networks.

Autoregulation is the action and the effect of self-regulation, with the latter being the act of regulating oneself. In other words, this option involves the

organization of a particular subject—in our case, social networks—by the agents who participate in it.

The formula that disciplines the social relations that take place in a given sector, such as self-discipline, has always existed in some form since, naturally, all organizations self-regulate. Self-regulation supposes the observance of some behavioral patterns, principles and ethical norms whose fulfillment has been previously set as objectives.

The legally relevant self-regulation is intelligible and acceptable to the system of rights and is sometimes incorporated as if it were its own reference. With this consideration, we must include the foresight of the legislator to promote self-regulation in highly technical and complex sectors, such as social networks. The nonbinding or voluntary right is the set of instruments that, although they do not reflect the imperative nature that characterizes legal norms, can significantly affect the legislative landscape and promote the legal standardization of certain practices (ESPINOSA CALABUIG, 2001).

Codes of conduct cannot establish norms whose application is more permissive than the minimum that is required by law nor be openly contrary to the imperative law. A reduction in the legal norms that are established by legislators is not admissible as imperative law or, in its case, semioperative in favor of the consumer. They do, however, significantly improve the protective framework that is applicable to the potential consumer and/or user - the weak part of the contract - in terms of electronic commerce.

The norms that are contained in these codes tend to be much more adapted to the specific problem that they want to solve because their development has been precisely carried out by the people who are closely related to the problem that needs to be solved (Margulis, 2003; BENNET and RAAB, 2006; Ruotsalainen, 2017).

Law 34/2002, of 11 June, of the Society Services of Information and Electronic Commerce (LSSI-EC) justifies the use of codes of conduct in the aforementioned subject by virtue of their usefulness as a self-regulation tool that is especially suited to adapt the articles of the law to the specific characteristics of each sector. It is for this reason that knowing the particularities of the codes of conduct determines that it corresponds to the public sector to promote the creation and application of such instruments through coordination and advice.

We must mention that, due to the relevance of their effects, the existence of the European code of conduct of the Federation of European Direct and Interactive Marketing on the use of personal data in direct marketing whose content complies with Directive 95/46/EC on privacy provides sufficient added value to this Directive since it is properly focused on the specific issues and

problems of data protection in the direct marketing sector and offers sufficiently clear solutions for these issues and problems.

Companies that adhere to systems of self-regulation should show their potential customers that they know the system that protects the rights and interests of the user who has chosen their service. It is necessary, therefore, for there to be an accreditation mechanism for the adherence to a system of self-discipline so that companies that are actively committed to its sustainability and development are identified (Listokin, 2015). This will be evidenced by the display of the corresponding seal of trust accrediting the company's compliance with it on a visible place on the website of the company that verifies the code of conduct (KROEBER-RIEL and WEINBERG, 2003).

As for the possible content that the codes of conduct may present, with respect to electronic commerce, it is worth insisting that they may well contain comprehensive regulations of electronic commerce, including questions related to privacy and well-being that are entirely dedicated to the data protection in that area. In any case, the code of ethics will contain measures with varying details that aimed at guaranteeing personal data protection for both adults and minors. For all that we have seen so far, awareness can be raised as a result of the eventual damage that could potentially result from the imperative need to ensure high levels of privacy protection on social networks. Although we are faced with platforms that are subject to legislation on personal data protection, we must not lose sight of the fact that laws are, by nature, limited from the outset, and as a general rule, their implementation is only effective in the territorial space for which they were conceived. On the Internet, as is well known, there are no territorial borders, and although national laws are applicable, the virtuality of the practice is extremely limited.

As a consequence of the assessments that were previously made, it is wise at all times, as has been suggested by the community, to first promote the creation of a code of conduct regulating social networks whose scope will initially be the community space. Nevertheless, a code of conduct with an international scope is most desirable. In any case, the importance of the step that is taken should not be underestimated because such a decision does not at all represent an obstacle for a global code of conduct to be formed in the future.

At present, no code of conduct has been developed in the public space; however, as we have determined on several occasions, this presumably will take place. It should not be forgotten that such a code of conduct will be voluntary. Indeed, its articles will become a reference for data protection in the field of social networks and will therefore not be mandatory for platforms, unless it has been previously stated. Social networks wishing to adhere to the code and adopt such an attitude will publicly demonstrate that their behavior is more protective of the

user than the legislation itself. In other words, in certain cases, the legal provisions in favor of the user will be improved, while in others, legal loopholes will be filled. It should be noted, in this sense, that we are faced with an environment that is so dynamic that national laws are not able to adequately and fundamentally regulate the issue due to the speed with which things change and the different natures of society, information, and knowledge. In any case, we are not faced with a new problem because, traditionally, the legislation has solved problems in the application of technologies, although with a certain delay. These problems have been creating new difficulties for legislative bodies. Such a drawback, which is inherent to the procedure for the elaboration of norms, could be avoided (or at least relativized) by referring to the codes of conduct regulating social networks. This is because such conventional norms are the result of self-regulation, have dramatically shorter and less formalistic preparation periods than do legal norms and have the ability to more quickly adapt to technological changes.

Regarding the issues that, in our opinion, should be addressed in such a document, by revealing the best practices for privacy in social networks, we will highlight some but not all of them that can reflect the exhaustive actual possibilities. Note, therefore, that what we will point out is only a minimal example of the content. In this sense, we will insist on questions of substance and form.

With respect to the latter, it is fundamental that the articles of the deontological code establish an obligation by social networks to present all the information related to their services in a clear and simple manner. The language that is used in their privacy policies should be understandable by any user and allow them to know their rights and obligations.

Plausible codes of conduct should come from the various agents who subscribe to social network content and should be driven by the need to promote the codes through different media, information and education sources. In summation, the promotion of codes of good practice by communities in a social network can significantly contribute to the training and awareness of users. It would be desirable, in this sense, to establish the need for social networks to institute a specific section aimed at informing users of the conditions of the service and the effects of each action that is performed on their respective home pages.

At the technical level, the obligation to implement certain actions should be arbitrated, such as establishing security applications that are aimed at guaranteeing or, where appropriate, mitigating the possibility of receiving unwanted commercial messages through social networks; establishing technological measures that allow for knowing the ages of the users, which is especially important for restricting the entry of minors; and creating tools for reducing identity theft within the network. In addition, they should eliminate

obsolete data that may exist in different servers and the encryption of those data that are in use, thus minimizing the damages that could be caused by outside attacks by malicious third parties. Furthermore, the applications should create analysis mechanisms for the strength of passwords so that only those that are sufficiently secure for the user and, therefore, not easily decipherable by third parties are allowed. Also included are dissociating the data that exist in a user profile so that unauthorized users cannot access user data for malicious purposes, devising different categories for profiles to control the volume of personal data that the user allows other users to see, and establishing different categories of authorizations that are set by the users themselves so that they can decide who can view their profiles and what type of data others can access.

Likewise, media should be made available to users through which they can report situations that affect their personal or third-party data or that constitute inappropriate, offensive or illegal material. To this end, within social networks, a system could be created to automatically block such content that could later be examined by individuals.

It is very important to reinforce the idea that the code of conduct that is adopted should limit a relatively common practice by social networks: unilaterally modifying privacy policies without prior notice to previously registered users who initially accepted them. With the assumption that the modifications were necessary, they should be communicated so that the users can read them, accept them (if wanted) and unsubscribe from the service if desired.

CONCLUSION

The Internet is a global and open network that allows the exchange of information. Currently, the World Wide Web is configured as a social relationship that is based, to a great extent, on the growing participation of users. Social networks and, in general, collaborative websites are the primary means of promoting interaction with other network users. Such platforms are based on the creation of profiles in which the respective users provide significant amounts of personal data. However, it is necessary to strike a balance between the open nature of the Internet and the protection of the personal data of internet users.

The number of social network users is growing worldwide. Despite the significant growth and the notoriety of such social spaces, personal data are subject to numerous risks. There are certain measures that can be taken to eliminate or mitigate those risks to the maximum possible extent. Among these, legal regulations and the promotion of self-discipline by agents in the sector can have a combined effect.

The value of self-regulation is especially relevant in an area such as the one that we are analyzing that does not seem to recognize territorial borders. In fact, the platforms on which social networks are based are often located outside the European Union and mainly in the United States. Therefore, at the time of registration, the data will be transferred to servers and offices that are located in that country. Therefore, it is necessary and plausible that the privacy policies of social networks that exist in the global territorial space guarantee high levels of privacy protection for users. Given that, as we have anticipated, the Internet has no territorial borders. A means by which privacy protection can be successfully achieved is through self-regulation, and its most paradigmatic manifestation is codes of conduct. These tools are highly efficient in the partially connected fields that we have examined of social networks, electronic procurement, and interactive advertising.

Regarding the content that the codes of conduct regulating social networks should address, the codes are broad with respect to the privacy protection of users. One of the purposes of such documents is that they will improve the prevailing legal norms by responding to questions that the legislators have not addressed.

It is recommended that a code of conduct regulating social network privacy be approved by the community or international bodies. We must not lose sight of the fact that one of the characteristics of the codes of conduct there is that they are voluntary; therefore, for users demanding compliance with them, the codes will have to be previously adopted by the platform in question. Notably, adopting codes of conduct will have numerous advantages for social networks that are committed to fully adhering to the codes given that its differentiated attitude will be able to accredit the observance of best practices in the field of user data protection.

REFERENCES

ADAMS, M. Big Data and Individual Privacy in the Age of the Internet of Things. **Technology Innovation Management Review**, v. 7, n. 4, p. 12-24, 2017.

BALLESTEROS MOFFA, L.A. **La Privacidad Electrónica. Internet en el centro de protección**. Valencia: Tirant lo Blanch, 2005.

BARBANELL, J. Needing a new approach to address employee data breaches in the american workplace. **Journal of Law and Cyber Warfare**, v. 4, n. 3, p. 49-51, 2015.

BECHMANN, A. y BOWKER, G. Unsupervised by any other name: Hidden layers of knowledge production in artificial intelligence on social media. **Big Data & Society**, v. 1, n. 11, p. 1-11, 2019.

BENNET, C. y RAAB, C. **The governance of privacy. Policy instruments in global perspective**. Cambridge: The MIT Press, 2006.

BERROCAL LANZAROT, A. La protección de los derechos de los menores de edad en internet. **Revista Crítica de Derecho Inmobiliario**, n. 739, p. 3371-3422, 2013.

BORGOHAIN, T. KUMAN, U. y SANYAL, S. Survey of Security and Privacy Issues of Internet of Things. **International Journal of Advanced Networking and Applications**, v. 9, n. 11, p. 20-26, 2015.

CARPENTER, D. Privacy and biometrics: An empirical examination of employee concerns. **Information Systems Frontiers**, v. 20, n. 1, p. 91–110, 2016.

CASTILLO JIMÉNEZ, C. La sociedad de la información y los derechos fundamentales. Ley 34/2002 de servicios de la Sociedad de la Información y del comercio electrónico. **Derecho y Conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento**, n. 2, p. 21-37, 2002.

COOLEY, T. **A Treatise on the Law of Torts or the Wrongs which arise independent of contract**. Chicago: Callaghan, 1888.

DÍAZ ARIAS, J.M. **Guía práctica sobre normativa de protección de datos y publicidad comercial**. Barcelona: Ediciones Deusto, 2008.

ESPINOSA CALABUIG, R. **La publicidad transfronteriza**. Valencia: Tirant lo Blanch, 2001.

GUERRERO PICÓ, M.C. **El impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal**. Madrid: Thomson Civitas, 2006.

KROEBER-RIEL, W. y WEINBERG, P. **Konsumentenverhalten**. Munich: Vahlen, 2003.

LISTOKIN, S. Industry Self-Regulation of Consumer Data Privacy and Security. **John Marshall Journal of Information Technology and Privacy Law**, v. 32, 15–32, 2015.

MARGULIS, S.T. Privacy as a social issue and behavioral concept. **The Journal of Social Issues**, v. 59, n. 2, p. 243-261, 2003.

MAROTTA-WURGLER, F. Self-Regulation and Competition in Privacy Policies. **The Journal of Legal Studies**, v. 45, n. 2, p. 13-39, 2016.

MCDERMOTT, Y. Conceptualising the right to data protection in an era of Big Data. **Big Data & Society**, v. 4, n. 1, p. 1-7, 2017.

OLIVIER LALANA, A.D. El derecho fundamental "virtual" a la protección de datos. Tecnología transparente y normas privadas. **La Ley**, n. 5, p. 1539-1546, 2002.

PETRUCCO, F. The Right to privacy and new technologies: between evolution and decay, **Rivista di Diritto dei Media**, v.1, p. 1-35, 2019.

PRIETO ANDRÉS, A. La nueva Directiva europea sobre el tratamiento de datos personales y la protección de la intimidad en el sector de las telecomunicaciones. **La Ley**, n. 5, p. 1710-1713, 2002.

REBOLLO DELGADO, L. **Vida privada y protección de datos en la Unión Europea**. Madrid: Dykinson, 2008.

ROSSNAGEL, A. **Handbuch Datenschutrecht**. München: Verlag C.H. Beck, 2003.

RUOTSALAINEN, P. Privacy, Trust and Security in Two-Sided Markets. In ***E*-Health Two-Sided Markets**. Holland: Academic Press, 2017.

SPIEKERMANN, S. *The challenges of personal data markets and privacy.* **Electronic Markets**, v. 25 n. 2, p. 161–167, 2015.

TOLCHINSKY, D. McCuddy, K. Adams, J., Ganster, D. y Fromkin, H. Employee perception of invasion of privacy: A Field Simulation Experiment. **Journal of Applied Psychology**, n. 66, p. 308-313, 1981.

ZARSKY, T. Transparent Predictions. **University of Illinois Law Review**, v. 4, p. 1503-1569, 2013.