How Social Networks and Data Brokers trade with Private Data

Cómo comercian con la información privada las redes sociales y empresas de datos

DOI

Germán Llorca-Abad, Lorena Cano-Orón

ABSTRACT

The so called social networks and data brokers have become the iconic players of the thriving Big Data economy. The aim of our research is to unveil the details of their tactics, which mainly are founded on the boundaries of the current legal framework. For this purpose we use a triple methodological approach: antecedents' bibliography review, an in-depth interview, and text analysis. The results can be summarized in three main conclusions: social networks and data brokers; a) hide their users how they gather their personal data; b) do not inform their users the purposes for which they have gathered their personal data, and c) take advantage of the weaknesses of the current legal framework to carry on with their activities.

KEYWORDS: BIG DATA, DATA MINING, DATA BROKERS, SNS COMPANIES, PRIVACY.

RESUMEN

Las así llamadas empresas de datos y redes sociales se han convertido en protagonistas icónicas de la economía del Big Data. El objetivo de esta investigación es desvelar los detalles de sus estrategias, que se asientan principalmente en las flaquezas del marco legal vigente. Para ello empleamos una triple aproximación metodológica: revisión bibliográfica de antecedentes, entrevista en profundidad y análisis de texto. Los resultados se resumen en tres conclusiones principales: las redes sociales y las empresas de datos; a) esconden a sus usuarios el modo en el que capturan sus datos personales; b) no informan la finalidad del uso de dichos datos; y c) se aprovechan de las lagunas del sistema legal vigente.

PALABRAS CLAVE: BIG DATA, DATA MINING, DATA BROKERS, EMPRESAS SNS, PRIVACIDAD.

1. INTRODUCTION AND STATE OF THE QUESTION

The progressive digitalization of personal and professional communication processes has caused an exponential growth of data. This explosion has originated in the field of investigation in communication concepts such as *big data*, or *data mining*. It also has turned researchers' attention to old problems, such as the digital divide, or privacy protection, but from a digital scope. On the one hand, this phenomenon describes the increasing interest of companies and governments in converting information into knowledge. On the other hand, it also means that they seek to collect and make sense of some of the exabytes of information generated daily by users.

Thus, data have become a sort of *commodity* to be traded with. The technology needed to exploit information and make a benefit of it already exists and continues to develop. This has major outcomes for personal privacy in the digital sphere. The lack of training in the way we use the network implies that sometimes we do not manage correctly our privacy in the Internet. Our personal data is captured, screened out and classified by entities that might not have our explicit permission to do so.

Not just devices such as smartphones, computers, tablets or smart watches, but also common equipment like our water, gas, or light meter gather enough information to create accurate knowledge about us. Even our public transport

pass stores data about our routines (Galdón 2012). In other words, techniques of data collection and monitoring are already integrated in regular webs and technological tools. We can be watched and followed by the net. People can intrude on our private life and analyse our data without we realizing it (Morozov 2012).

People are vulnerable in three ways. First of all, the Internet DNA: the code. Network architecture is not neutral or unique. It has its own ideology and its structure conditions the kind of practices that we can do online (Lessig 2006). Because of it, everything we do online is traceable and storable. This code allows the creation of specific software programs whose main goal is to collect data from users, the installation of the cookies and similar technologies on computers. This activity was being done silently since a few months ago, when legislation bound companies to announce users the installation of cookies. However, their disclaimer does not specify which data is being collected and for how long.

It is possible to apply filters to users by default. These filters are based on users' data and turn the user experience into a *filter bubble* (Pariser 2011). This customization could be practical in some ways, but it could also be dangerous for users' minds, because it affects people's public opinion concept (Sunstein 2001; Han 2014). A common example of this is what Facebook does in their News Feed[1], which currently considers the time a user takes to read friends' posts. Its algorithm filters news from friends you are interested in, and they know who they are because of your interaction on the platform and your silence watching the news (Yu & Tas 2015).

Current EU privacy and data protection policies do not cover the new needs of citizens that have arisen as a result of technological developments, particularly in the progress of data mining. A new legal framework should be fit for protecting users' activity in the digital sphere. The main EU Directives on data protection and on e-privacy were approved in 1995 (EU 1995) and 2002 (EU 2002). There have been subsequent modifications but the bases are still from the old ones (2014).

The European Commission noticed this situation after several years of reports done ad hoc to evaluate the protection of citizens, and prepared a proposal for a legislative reform that will replace the current Directive 95/46/EC. This proposal considers the characteristics of the current digital sphere and

1 A comprehensive research carried out by Kramer, Guillory & Hancock (2014) explains how Facebook made experiments with its users through the manipulation of their News Feed. The conclusion was that the social network succeeded in creating positive and/or negative emotional contagion in a massive scale.

extends the protection of internet users, in order to cover all their guarantees and rights. Although this renewal was proposed in 2012, it was not approved until June 2015 by the Council. Now the final redaction is left to the new legislation until it takes effect. One of the main innovations of the reform is the implementation of the right to be forgotten, which had to be imposed and regulated by a judgment of the European Court of Justice (ECJ), due to the delay that is leading the process of adoption of the reform.

Thirdly, the factor that puts users in a vulnerable position is the *information divide*. Due to the lack of digital literacy and the quiet operation with which information is collected, regular users do not realize the loss of control over their data. In fact, Internet companies may have easy access to their sensitive information, as they are not aware on what they are revealing. Users tend to trust their service providers, and the law should protect them (Wauters et al. 2014).

These collecting practices are legal. Users sign a digital contract when, for instance, they create a digital profile in a social network. Privacy policies and terms and conditions texts explain what the company does with their data, how they are gathered and for how long. When users "accept the terms and conditions", they are giving their consent to companies to execute all they have written on these long but vague texts.

Andrejevic has described the internet as a huge scenario for the "interactive economy" based on "predictive analytics" (2011, 279-281). This new field in the economics pathways is based on "user-generated activity" (Andrejevic 2011). Every day millions of users work, share content, buy, and surf the web in a wide variety of forms. All this traffic generates what it is so called big data, at a rate of an estimated 2.3 trillion gigabytes per day (IBM 2015), and it grows around 40% every year (Thakur & Mann 2014, 469). As Andrejevic points out, all this "user generated data" is "collected by interactive platforms about users, usually invisibly as they go about the course of their wired lives, or at least that portion of their lives that involve digital, networked devices" (2011, 279).

Big data enthusiasm can be considered one of the most relevant outcomes of wired life. All the information spreading the Internet is classified in two general categories: (i) structured data, which are numbers and words that can be "easily categorized and analyzed" (Thakur & Mann 2014, 469). In this group information inputs are generated by things "like network sensors embedded in electronic devices, smartphones, and global positioning system (GPS) devices" (Thakur & Mann 2014, 469), and things like transaction data or account balances. (ii) unstructured data, which includes more complex information. Unstructured big data is the things that humans are saying

through logging data actions, transactions, social media interaction, images, video and audio loading, e-mails and events.

This information contains an inestimable value for companies and governments, so all the efforts are being put into data mining analytics. "Data mining (sometimes called data or knowledge discovery) is the process of analyzing data from different perspectives and summarizing it into useful information -information that can be used to increase revenue, cuts costs, or both. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases" (Thakur & Mann 2014, 471).

As Thakur & Mann (2014) indicate, Doug Laney (2001) was the first one talking about 3V's in Big Data Management, as a key-issue in its understanding: volume, velocity and variety. In recent investigations, some have pointed out the need for adding more V's: variability, value, and veracity. As all forms of online activity contribute to the creation of this data, "they are all implicated in the account of exploitation developed here" (Andrejevic 2011, 279). Although scrutinizing big data for relevant information does not seem easy, companies are making their way through[2].

This fact is becoming crucial to understand the Internet functioning. While big data prophets claim to have reached a sort of happy *arcadia*, some questions should be raised on the issue. It is undoubtedly true that information generated by users in the internet can be handled in beneficial applications. The discoveries in this respect could apply for a wide range of decision-making in many strategic fields, as Chen, Mao and Liu (2014) have described: national security, environment, bio-medical purposes, or industrial solutions. That shall be the reason why public and private organizations are investing huge economical resources on big data policies. For this respect, as Kashmir points out (2012), police services have become data mining fans, as big data analysis could help in their investigation procedures.

However, a hypothetical global benefit derived from this should not be taken for granted, as it seems that only economical and individual reasons prevail. Within this context, users are simply considered *commodities* in an exchange market (Andrejevic 2011) and it should worry politicians, analysts, and academics. "An emerging commercial model for the interactive economy has become reliant on the prospect that information-based target marketing

2 Evgeny Morozov (2012) stresses out the fact that the amount of data generated in our daily activity as users pose serious hazard to get intelligible and useful information from data mining. Although his skeptical view on the issue, companies and governments do not hesitate in investing their resources in finding it.

and data mining will be increasingly effective in manipulating and channelling consumer desire" (Andrejevic 2011).

We find quite significant that Andrejevic (2011) links the behaviour of the Internet companies to the notion of surveillance, as well as bringing in the debate the notion of exploitation in online contexts. These two questions are by far the most relevant in the actual debates being held around this issue. Big data managers face enormous safety and privacy challenges, as traditional data protection methods have already been shown not applicable. Chen, Mao &Yunhao (2014, 203) have identified two main concerns on the privacy field: "(i) Protection of personal privacy during data acquisition: personal interests, habits, and body properties, etc. of users may be more easily acquired, and users may not be aware. (ii) Personal privacy data may also be leaked during storage, transmission, and usage, even if acquired with the permission of users".

We owe the definition of users as mere commodities to Fuchs and Sevignani (2013). These authors consider that the activity of people in the web serve as alienated work for the benefit of the internet companies. This would show a total disrespect for user's privacy protection on the companies' side. We can trace the deepest roots of this theoretical approach in older audience and framing studies. "Dallas Smythe (1981) [...] held that the reception activity of audiences constitutes a form of unpaid labour. [In the internet] the central task of value production is 'out/crowdsourced' to the users" (Krüger and Johanssen 2015, 637). Researchers also have discovered that this is not something companies explicitly hide, but even when these facts are publicly know, people react with passiveness. Krüger and Johanssen show how users, even when feeling betrayed, continue "the relation with the deceiving partner [...] on the basis of a fundamental injury that has been derealised" (2014, 644).

From time to time these companies change their algorithms in order to capture a "broader spectrum of information [...] in order to market to us more effectively" (Andrejevic 2011, 278-281). This happens because as individuals "we have been party to the aggressive privatization of what started as a publicly funded communication network" (Andrejevic 2011). While people think they move freely in their wired activities, the fact is that every neither single action nor decision they are taking is being registered an incorporated to a big data repository. Due to the nature of the World Wide Web, the laws of privacy protection do not apply well, and companies risk at their ultimate limit to acquire relevant information. "There is more at stake in interactive forms of surveillance than violations of traditional privacy norms: specifically the concentration of new forms of predictive power in the hands of commercial interests" (Andrejevic 2011, 282).

"Rejoinders to critiques of exploitation in such contexts typically invoke both the lack of coercion and the pleasures of participation" (Andrejevic 2011, 283). In fact, some authors argue that we are living in a "privacy paradox" (Wittes& Liu 2015). In this article their authors claim that privacy debate is biased "towards overstating the negative privacy impacts of new technologies relative to their privacy benefits" (2015, 2). On this behalf, we could pose a simple question: are we not considering the benefits of a daily privacy such as accessing porn sites or looking for information about embarrassing illnesses? The idea is quite tempting, as it suggests a concept linked to immediate privacy that would allow users to carry on a digital life only for themselves. However, why should we give up on long term outcomes when relying on these companies our personal data? Wittes and Liu shall reply that "consumers choose whether or not to use these technologies based, in part, on whether they value more the privacy given or the privacy taken away" (2015, 3). We will completely agree this assertion when companies provide consumers with full and clear detail on how they use our personal data.

2. METHODOLOGY

This work is within structure and policies of communication theory, as we believe that is the perspective from which we can raise a better analytical study of the policies that protect individuals on digital security and control of privacy. The specific methodology used to undertake the research is based on relevant and interdisciplinary documentary analysis, the text analysis of four of the most popular social networks' legal advices, and the interpretation of the data obtained in an in-depth interview with the responsible of a relevant Europe's based data broker company.

All the information analysis is displayed in section 3. Firstly, subsection 3.1 evidences the techniques data brokers use in order to obtain and trade with personal data. The details come, mainly, from the in-depth interview carried out and the results obtained in previous investigations. Secondly, subsection 3.2 shows the results of text analysis of Social Network companies (SNS) Facebook, Whatsapp, Youtube, and Twitter's legal advices. These two types of enterprises make business by different strategies, but mainly trading with users' personal data. The main hypothesis proposed is that for this purpose these companies rely their activity in playing with the limits of legal frameworks, digital divide when linked to users, and how the deep World Wide Web code is structured.

On the one hand, pros of this proposal could be summarized as for the emphasis put on user's perspective, the use of multidisciplinary bibliography, and the discovery of secondary sources such as Just and Puppis (2012) for interpreting legal advices' texts metadiscourses. On the other hand, cons must be considered from the point of view that companies lack in transparency when asked on their activities. The companies sample analyzed could also be broader. Our aim is to foster debate and a more profound knowledge of how some internet companies base their business.

3. RESULTS AND DISCUSSION

In this section we describe two different types of companies devoted to trade with our personal data. Information collecting and data selling can be considered the core of their business. Although the final strategies implemented by both sorts of companies may differ, the general outcomes of their activity are the same. In fact, as we previously mentioned in the introduction, both of them benefit of a weak legal framework, a strong digital divide when considering users' abilities to manage their privacy on the internet, and how the deep World Wide Web code is structured. We will try to define them and describe some of the main tactics they use to achieve their mission.

3.1. DATA BROKERS

It all starts with an ordinary action. We access our favourite social network profile and suddenly an ad with an attractive message pops up: "Congratulations, you've won a car", or something similar. Sometimes the prize is a worldwide tour, or money. When we click on the ad, we are brought a little bit deeper in the trap. There we discover it is all about a contest in which we could end up winning the announced prize. Getting into the contest is quite easy. The proponents only demand to provide few personal data with, such as our e-mail address, full name, age, gender and, sometimes, profession, telephone number, or so. It is when we accept the legal advice before getting the right to participate in the contest that we are part of the business. This is one of the most popular modus operandi that some internet companies use to collect information. From then on, we become part of a trading kind of game.

Names like Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf, or Recorded Future say nothing to average people. Nevertheless, these sorts of companies, the so called data brokers, really

handle the internet data market. Their general purpose is to collect users' personal data (big data), classify it in different categories (data mining), and sell it to other companies. Those other companies will use the purchased information in order to market people, who usually will never know they have been targeted. Data brokers use the win-game strategy described lines above to gather the information, but sometimes it is not the only way it is used. They also use cookies dropped into pc systems, trace internet users' interaction in their wired activity, or simply buy it from other sources, such as credit card networks operators.

In 2014 the *Federal Trade Commission* of the United States made a report analysing those nine companies, as they represent the majority of the data brokers sector. The administration took the decision due to the lack of transparency in the law, which virtually gave (gives) them the freedom to do whatever they want with no monitoring. At first glance, why should we be suspicious? Quite easy: according to the Fed's report (El Comercio 2014), "data brokers can, for example, *typecast* someone as a consumer with a bad credit record, or as a person with health problems that could affect in job performance; even if the information on which they are based is incorrect".

The X data broker (XDB[3], from now on) started its activity in 2005. This company's turnover rises more than 12 million euro per year (Bureau van Dijk 2015), and most of the information gathered in their servers got there through the win-game strategy. "We start asking for simple data such as name, age, and gender. If the user decides staying in the game, then we can get the e-mail address, a full name, and a postal address. Once the user clicks 'I agree' on the legal advice, we keep stimulating him or her through positive incentives. Then we get it all: which is their mobile company, name of the car insurance company, interests, hobbies, profession, etc." (XDB 2015). Everything is perfectly lawful, but within the process, the acceptance of the legal advice and the game conditions may look confusing "as users have to mark two different check boxes nearly at the same time".

As Jason Koebler (2015) stressed out in a press article, "we are gaining one type of privacy while sacrificing another, and the type of privacy we gain is often more valuable and more immediate to the layperson than the type of privacy we're giving up by entrusting it with companies who want to use our

3 *XDB* is a fake name used to refer a Europe's based data broker company. We conducted an in-depth interview the 1 March 2015 with one of its principal managers. In order to use the information we were provided with, we had to sign a confidentiality agreement, by which we cannot unveil the company's name, or any other personal detail. All the information regarding it was classified as secret.

data to make money". However, Koebler follows, "just because we search for something online does not mean it should be stored in a database forever, in perpetuity", which usually happens. "The information is stored and commercialized until the contact data provided by the user does not work any longer. This means we keep the information virtually forever" (XDB 2015).

As mentioned above, all the business is perfectly lawful. "The win-game players must give us their informed consent by marking a check box that contains a link to the legal advice piece. This document describes all the uses we will give the information" (XDB 2015). When asked if it was common among the users not to read the legal advice, the interviewed pointed out "not having trustful evidence on that" (XDB 2015). On the one hand, this procedure shows how weak privacy protection laws can be. On the other hand, it confirms how easy is to skip a truly full informed consent verification. The company is not breaking the law, but the strategy used to get the data is roundly controversial.

This could be explained due to the fact that despite all regulations, national law disposals, and international provisions, protecting information privacy is also becoming a lucrative business. We find an emblematic example in one of the furthest borders of Europe. The government of Iceland (Berejano 2015) has been reinforcing the country legislation in order to implement security around digital information stored in the country. As for technical and technological trust, the Icelandic administration is also creating an appropriate infrastructure. This protective environment will be offered to companies and any sort of organizations in order to keep secret their sensitive data. Unfortunately, unless there is a real effort put in creating an international strong legal framework, data brokers will keep *skirting* the law.

XDB uses a back-office department ruled by lawyers, designers, computer scientists, communication specialists, and publicists in order to "organize, classify, and package information in attractive *bundles*. Then, these bundles are sold, mainly, to e-commerce, insurance, or phone companies. Each bundle contains, at least, information of fifty thousand different people" (XDB 2015). One of the most important tasks after getting the information from one user the first time is keeping it updated. "That is why our duty follows by targeting him or her, via marketing actions, in order to keep our databases permanently refreshed. We have a specific department in charge to carry out this purpose" (XDB 2015).

In fact, the win-game player never gets to know that some of the marketing operations he gets involved with afterwards come from the company that got his personal data in the first place. "Sometimes the tactic is different. We simply improve the win-game webs, so that the users come over again and

again. This strategy optimizes our inscription ratio and keeps our storage data up to date" (XDB 2015). It must be said that all the process endures for a whole year. "After the win-game is launched we keep developing it for whole year. The idea is simple: once the player is fully engaged, he or she will keep on playing a *little bit more* in order not to waste the time they have invested. At this stage we can get any information we want" (XDB 2015).

One of the great strengths of the data brokers companies is the ability they develop to anticipate what consumers will wish or not worldwide. These companies get to know users' movements on the internet and in real life through the information they collect from them. As we have seen, analysts of these companies create multi-level classifications in which could fit any consumer in the world. This system allows them to guess which products they may or may not want in order to sell them. Thus, personal data and private information become a gold mine to data brokers.

3.2. SOCIAL NETWORK SERVICES

When we use Social Network Services we must be aware of two facts: 1) we are dealing with a private enterprise whose main interest is to get benefits; and 2) if we are not paying for the service with money, we are paying for it with our data. The main difference between money and data is that the first is not traceable, while data represents us, marks us and also can dominate us. Personal data has become an emerging commodity, it is conveyed as a currency used by users to pay for many free services on the network. Morozov (2015a) cautions that users are deceived twice because they do not notice about this data transactionand are not conscious of the adequacy of the digital space made from them, "in a way that is neither transparent nor desirable".

Privacy policies and terms and conditions of a SNS are a legal contract between the user and the company. These texts have to expose in deep what the company is going to do with users' data. Every user has to accept this contract to finish the registration on a SNS. However, to get the user's consent this way is not legal in the EU because it does not collect enough characteristics to be informed, free and specific (Van Alsenoy et al. 2015). The most popular SNS are American companies that offer their services in Europe and thus have to accomplish the EU legislation, which is more protectionist than the American one.

At the present research we have selected four popular SNS (Facebook, WhatsApp, YouTube and Twitter) and we have examined three aspects of their Data Policy: 1) How they use users' data; 2) How long they gather these data; 3) What would happen if the company is merged with another one or is

involved in a bankruptcy. How these powerful companies deal with our data is public for everyone but not known by every user.

3.2.1. FACEBOOK

This company use the users' data with four main objectives (Facebook 2015a): 1) Provide, improve and develop Services, such us tailoring the experience for each user or doing a research (Facebook 2015b); 2) Communicate with the user; 3) Show and measure ads and services; 4) Promote safety and security. It does not specify how indeed this information is processed and how the user could be affected.

The collected data is stored "for as long as it is necessary". "Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services." In case the company had a new owner, the dataset would be transferred without the need of users' consent, because users have accepted these conditions already.

A research carried out at KU Leuven University by Van Alsenoy et al. (2015) that analyses Facebook terms and conditions and data policy, showed that this company could be not respecting several EU regulations on privacy. This report has had a considerable media impact and Facebook has spoken about it. The company has admitted some infractions shown by the research (Gibbs 2015a) but also it has exposed its disagreement with the 'European right to be forgotten" (Gibbs 2015b).

3.2.2. WHATSAPP

This SNS uses the users' data to operate, maintain and provide its service (WhatsApp 2012). Also they are employed to communicate with the user, to improve the quality and design of its platform, to create new services "by storing, tracking, and analysing user preferences and trends". Moreover, WhatsApp may share "non-personally-identifiable information (such as anonymous User usage data, referring / exit pages and URLs, platform types, asset views, number of clicks, etc.) with interested third-parties to assist them in understanding the usage patterns for certain content, services, advertisements, promotions, and/or functionality on the WhatsApp Site". So, data gathered by this company, as the other ones, is used basically to profit.

WhatsApp stores personal data 30 days after the user deletes its account. In other words, during the period of time that a person is user of this SNS, all personal data will be collected and analysed. And in case of bankruptcy, insol-

vency or similar situation, they are not liable about how personal information is treated, transferred, or used. Indeed, they "reserve the right to transfer or assign the information we have collected from our users as part of such merger, acquisition, sale, or other change of control".

Actually, Facebook absorbed this company recently (Facebook 2014). So, despite the fact that WhatsApp exposes that Facebook will respect WhatsApp users' privacy (Koum 2014)[4], according to its privacy policy and Facebook's one (2015a) is not what is expected to happen. In fact, it is also remarkable that the German data protection commissioner dissuades Germans to use WhatsApp after be merged with Facebook because of its weak privacy (Eadicicco 2014).

Current WhatsApp privacy policy is dated from 2012. According to Morell Ramos (2015), a specialist lawyer on privacy policies, WhatsApp terms and conditions now present errors, contradictions, gaps or legal loopholes about everything that has changed in these three years, like new services and the new company owner.

3.2.3. YOUTUBE

YouTube was sold to Google in 2006. And as a part of Google platform, YouTube is ruled by Google's privacy policy and terms and conditions (Google 2015). So what we are showing it is applicable to all family services of this company.

This enterprise draws upon users' data to provide, maintain, protect and improve all their services and develop new ones and to communicate with the user. Also, Google combines and analyses personal data to tailor content (search results and ads) and improve user experience. All users' data from all its services are stored for a period of time, which is not specified, after user removes its data. In its terms and conditions document, Google (2015) exposes that users have given to the company "a worldwide license to use, host, store, reproduce, modify, create derivative works [...] communicate, publish, publicly perform, publicly display and distribute such content. [...] This license continues even if you stop using our Services".

In case Google was involved in a merger or similar situation, this company agrees "to ensure the confidentiality of any personal information and give affected users notice before personal information is transferred or becomes

4 Besides it is noteworthy that this WhatsApp blog post is translated on 43 languages, while its policy privacy is only available in English.

subject to a different privacy policy".

Google privacy policy has been deeply supervised by UK Information Commissioner Office (2015) and Article 29 Working Party (2012), who have bound Google to incorporate the changes suggested by them at the new privacy policy. Our research considers that the changes made by this company are not enough specific to users. An example of this is the absence of the exact period of time that users' data will be kept in Google servers in the current privacy policy.

3.2.4. TWITTER

This company employs users' data to communicate with them, to make inferences (such as what topics the user is interested in and tailor the content), to improve its services and its security and to be able to show click statistics (Twitter 2015). The period of time that data is stored depends on the way that it is obtained; it could be a minimum of 10 days and a maximum of 30 days after deactivation of user account. In case Twitter was involved in a bankruptcy, acquisition or sale of assets, users' data would be "sold or transferred as part of that transaction". This latest statement perfectly reflects how data is the real value of this kind of companies. After knowing the purchase of WhatsApp by Facebook, the Google omnipresence on internet and the agreement between Twitter and Google that allows Google to index Twitter public information, we can appreciate that the digital communication market is controlled by a few companies.

4. CONCLUSIONS

In his latest work Andrew Blum (2012) showed how the internet is, in fact, depending on a very complex but fragile technological infrastructure. All the hidden wires, hubs, and connexions that give us access to the web create the illusion of a virtual almighty world. We will not deny this argument, nor either try to push it forward. We just realize that the internet, with all its implications, has become a central piece of everybody's life. In an extremely short period of time, we all have become dependents on it.

We buy, work, socialize; but also, share, play and communicate daily through very different ways due to app's, SNS, and web sites. The wired activity of millions of people generates an immense amount of potentially exploitable data. Companies and governments have begun a sort of race in order to

collect, interpret, and use it for a wide range of applications. This could be all positive, as information becomes knowledge. However, reality shows that companies and governments' interest is guided only by economical and control purposes. No humanistic achievements considered.

When we surf the web, does not matter for how long or how intense our experience is, we are sharing our personal data with the service providers. All of a sudden, we become part of a huge business being carried out by data brokers firms. These companies gather our data and sell it so the products and services market can target us. This could pose no problem, as long as we grant our personal data with no previous intimidations. Nevertheless, as we have stressed out, some of the strategies used by these companies borderline illegal behaviours. Protecting internet users' privacy and intimacy rights has become a major issue in these days. Some different reasons explain the critical situation we are facing and we will have to meet in the next decades.

Firstly, there is not a general legal framework fostered by any competent worldwide authority. International and local regulations can easily be overcome by data brokers. Secondly, users are not properly trained in the use of new technologies. This is the reason why, sometimes, we do not know how to manage our private data in the web. And it is the reason why we do not fully understand the implications of giving away our privacy rights. Finally, the privatization of the digital space gives all the power to an uncontrolled bunch of companies that will not hesitate in using the power we are providing them with.

Users' privacy is shown "as a barrier to economic growth" (Morozov 2015b). Data market is growing and its users do not read the rules established by companies. Moreover, even if users read all regulation texts, they would found difficult to achieve a proper understanding and interpretation of them. Mainly by the complexity of the language presented, the technicalities, the small fountain, length and amount of information that is given, etc. (Wauters et al. 2014). Perhaps one reason why users do not read privacy policy texts is the time it would take them to completely read these texts. As McDonald and Cranor (2008) note in their study, it would take 201 hours on average per year to read all the conditions of the websites we surf. And this contrasts with the average of 8 seconds that employs half the population surveyed in the study of Böhme&Köpsell (2010) to accept the terms and conditions. A recent study by the Pew Research Center (PRC 2014) notes that 91% of its respondents say they have lost control over how companies use and store their personal information. This study also remarks that 64% of the sample thinks that the government should regulate what advertisers do with their personal data.

To conclude, data market is closely related to a loss of users' privacy. The current legislation is not protective enough to assure citizens rights. So, we consider that the key element is the digital literacy. If people are concerned about its privacy and the value of its data, they will achieve a better control of its personal information and the information divide will be reduced.

5. REFERENCES

All URLs but DOI addresses in this article have been abbreviated using neither Google nor Bitly online shortening tools. All URLs where successfully accessed on 2/07/2016.

ANDREJEVIC, Mark (2011). *Surveillance and alienation in the online economy*. Surveillance & Society 8 (3): 278-287. Dirección: http://goo.gl/Zi4Zgw (Última consulta: 10 abril de 2016).

ARTICLE 29 WORKING PARTY (2012). *Letter from the Article 29 Working Party to Google Privacy Policy*, 16 October. Dirección: http://bit.ly/1IUUkz1 (Última consulta: 9 abril de 2016).

BEJERANO, Pablo G. (2015). *Islandia quiere ser la Suiza de los datos*. El Diario.es, 9 January. Dirección: http://goo.gl/utC8Cu (Última consulta: 10 abril de 2016).

BERG, Martin (2014). *Participatory trouble: Towards an understanding of algorithmic structures on Facebook*. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 8 (3): 2. DOI: http://dx.doi.org/10.5817/CP2014-3-2.

BLUM, Andrew (2012). *Tubes*. New York: Viking.

BÖHME, Rainer y KÖSPELL, Stefan (2010). T*rained to accept: a field experiment on consent dialogs*. Actas de la SIGCHI Conference on Human Factors in Computing System, USA: 2403-2406. Dirección: http://bit.ly/1CzTS8j (Última consulta: 12 abril de 2016).

BUREAU VAN DIJK (2015). *Orbis Database*. Dirección: http://goo.gl/RnyIRj (Última consulta: 10 abril de 2016).

CHEN, Min, Mao, Shiwen y Liu Yunhao (2014). *Big data: a survey*. Mobile Networks and Applications, 19 (2): 171-209. DOI: http://dx.doi.org/10.1007/s11036-013-0489-0.

COMERCIO, El (2014). *Las nueve empresas que saben más de ti que Google o Facebook*. ElComercio.pe , 28May. Dirección: http://bit.ly/1gsJMMq (Última consulta: 15 abril de 2016).

EADICICCO, Lisa (2014). *Whatsapp CEO responds: nothing is more important to me than protecting private, secure communication*. Business Insider Australia, 18 March. Dirección: http://bit.ly/1NZ7lXG (Última consulta: 15 abril de 2016).

EU (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

EU (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

FACEBOOK (2014). *Facebook to Acquire WhatsApp*. www.newsroom.fb.com, 19 February. Dirección: http://bit.ly/1ilEw9w (Última consulta: 20 abril de 2016).

FACEBOOK (2015a). *Facebook data policy.* www.facebook.com, 30 January. Dirección: http://on.fb.me/1Dwr7Vp (Última consulta: 20 abril de 2016).

FACEBOOK (2015b). *Research at Facebook*. www.facebook.com, 30 January. Dirección: http://bit.ly/1rNNfYf (Última consulta: 20 abril de 2016).

FUCHS, Christian y SEVIGNANI, Sebastian (2013). *What is digital labour? What is digital work? What's their difference? And why do these questions matter for understanding social media?* Triple C: Journal for a Global Sustainable Information Society 11 (2): 237-293. Dirección: http://goo.gl/JumLpV (Última consulta: 18 abril de 2016).

GALDÓN, Gemma (2012). *¿Qué hacen con nuestros datos en internet?* El Pais.es, 12 June. Dirección: http://goo.gl/5CVrZ2 (Última consulta: 20 abril de 2016).

GIBBS, Samuel (2015a). *Facebook admits it tracks non-users, but denies claims it breaches EU privacy law*. TheGuardian.com, 10 April. Dirección: http://bit.ly/1PrWhox (Última consulta: 17 abril de 2016).

GIBBS, Samuel (2015b). F*acebook questions use of 'right to be forgotten' ruling*'. TheGuardian.com, 7July. Dirección: http://bit.ly/1HdzYPc (Última consulta: 17 abril de 2016).

GOOGLE (2015). *YouTube's privacy policy*. Google.com, 30 June. Dirección: http://bit.ly/1e3kr3y (Última consulta: 17 abril de 2016).

HAN, Byung-Chul (2014). *Psicopolítica*. Barcelona: Herder.

IBM (2015). *The four v's of Big Data*. IBM Big Data and Analytics Hub. Dirección: http://goo.gl/vZtL1c (Última consulta: 19 abril de 2016).

ICO (2015). G*oogle to change privacy policy after ICO investigation*. Information Commissioner's Office, 30 January. Dirección: http://bit.ly/15PuSKD (Última consulta: 17 abril de 2016).

JUST, Natascha y PUPPIS, Manuel (Eds.) (2012). *Trends in Communication Policy Research: New Theories, Methods and Subjects*. Bristol: Intellect Books.

KASHMIR, Hill (2012). *Using Twitter to identify psychopaths*. Forbes.com, 20 July. Dirección: http://goo.gl/FLMIPZ (Última consulta: 17 abril de 2016).

KOEBLER, Jason (2015). *Counterpoint: the Internet has given us more privacy than ever before*. Motherboard.vice.com, 27 May. Dirección: http://goo.gl/DqRMcx (Última consulta: 8 abril de 2016).

KOUM, Jan (2014). *Setting the record straight*. Blog.whatsapp.com, 17 March. Dirección: http://bit.ly/1Ggr5Am (Última consulta: 17 abril de 2016).

KRAMER, Adam D.I., GUILLORY, Jamie E., HANCOCK y JEFFREY T. (2014). *Experimental evidence of massive-scale emotional contagion through social networks*. Actas de la National Academy of Sciences 111 (24): 8788–8790. DOI: http://dx.doi.org/10.1073/pnas.1320040111.

KRÜGER, Steffan y JOHANSSEN, Jacob (2014). *Alienation and digital labour-a depth-hermeneutic inquiry into online commodification and the unconscious*. Triple C: Journal for a sustainable information society 12 (2): 632-647. Dirección: http://goo.gl/pExXds (Última consulta: 8 abril de 2016).

LANEY, Doug (2001). *3D Data management: controlling data volume, velocity and variety*. Meta Delta Application Delivery Strategies. Dirección: http://goo.gl/t6oLnL (Última consulta: 25 abril de 2016).

LESSIG, Lawrence (2006). *The Code version 2.0*. Cambridge: Basic Books.

MCDONALD, Aleecia M. y CRANOR, Lorrie Faith (2008). *The Cost of Reading Privacy Policies*. I/S: A Journal of Law and Policy for the Information Society 4: 541-565. Dirección: http://goo.gl/BFcGrD (Última consulta: 23 abril de 2016).

MORELL, Jorge (2015). *5 puntos que WhatsApp sigue sin actualizar en sus términos y condiciones*. Terminosycondiciones.es, 30 April. Dirección: http://bit.ly/1TvmEex (Última consulta: 21 abril de 2016).

MOROZOV, Evgeny (2012). *The net delusion*. New York: Public Affairs.

MOROZOV, Evgeny (2015a). *Facebook isn't a charity. The poor will pay by surrendering their data*. TheGuardian.com, 26 April. Dirección: http://goo.gl/oRvn6L (Última consulta: 20 abril de 2016).

MOROZOV, Evgeny (2015b). *What happens when policy is made by corporations? Your privacy is seen as a barrier to economic growth*. TheGuardian.com, 12 July. Dirección: http://bit.ly/1HXCCKl (Última consulta: 21 abril de 2016).

PARISER, Eli (2011). *The filter bubble: What the Internet is hiding from you*. New York: The Penguin Press.

PRC (2014). *Public Perceptions of Privacy and Security in the Post-Snowden Era*. Pew Research Center. Dirección: http://goo.gl/HIuoPi (Última consulta: 2 abril de 2016).

RYBAS, Natalia y GAJJLA, Radhika (2008). *Developing cyberethnographic research methods for understanding digitally mediated identities*. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research 8 (3): 35. Dirección: http://goo.gl/9W2Cfj (Última consulta: 29 abril de 2016).

SMYTHE, Dallas Walker (1981). *Dependency Road*. Norwood New Jersey: Ablex.

SUNSTEIN, Cass (2001). *Republic.com*. New Jersey: Princeton University Press.

THAKUR, Bharti y MANN, Manish (2014). *Data mining for big data: a review*. International Journal of Advanced Research in Computer Science and Software Engineering 4 (5): 469-473. Dirección: http://goo.gl/PNFZfd (Última consulta: 22 abril de 2016).

TWITTER (2015). *Twitter privacy policy*. 18 May. Dirección: http://bit.ly/1MoUeyu (Última consulta: 1 abril de 2016).

VAN ALSENOY, Brendant, VERDOODT, Valerie, HEYMAN, Rob, AUSLOOS, Jef y WAUTERS, Ellen (2015). *From social media service to advertising network: A critical analysis of Facebook's Revised Policies and Terms*. Dirección: https://goo.gl/NMsIjt (Última consulta: 2 abril de 2016).

WAUTERS, Ellen, DONOSO, Verónica, LIEVENS, Eva y VALCKE, Peggy (2014). *Re-designing & re-modeling social network terms, policies, community guidelines and charters: Towards a user-centric approach*. EMSOC.be Report. Dirección: http://goo.gl/Bo6XES (Última consulta: 22 abril de 2016).

WHATSAPP (2012). *WhatsApp legal info*. WhatsApp.com,7 July Dirección: http://bit.ly/1fAUxfo (Última consulta: 22 abril de 2016).

WITTES, Benjamin y LIU, Jodie C. (2015). *The privacy paradox: The privacy benefits of privacy threats*. Center for Technology Innovation, 7 July. Dirección: http://goo.gl/XsgHev (Última consulta: 23 abril de 2016).

YU, Ansha y TAS, Sami (2015). *News Feed FYI: Taking Into Account Time Spent on Stories*. Facebook newsroom, 12 June. Dirección: http://bit.ly/1L5IkMy (Última consulta: 5 abril de 2016).