

## Esfera pública y Panopticismo: consideraciones sobre la vigilancia en la vida cotidiana

Hélder Rocha Prior, LabCom - University of Beira Interior/ University of Brasilia (PNPD-CAPES)  
[helder.prior@gmail.com](mailto:helder.prior@gmail.com)

Recibido: 22/06/2014 • Aceptado: 21/07/2014 • Publicado: 31/07/2014

**Cómo citar este artículo:** Rocha Prior, H. (2014). Public sphere and Panopticism: Considerations about surveillance in everyday life. *Sphera Publica*, 1, (14), 23-38

### Resumen

En la actualidad, no es posible discutir cuestiones relacionadas con el espacio público sin mencionar las estructuras tecnológicas que potencian el debate y el ejercicio de la ciudadanía. En el modelo actual de la auto-comunicación de masas, los ciudadanos ya no son sólo espectadores en las arenas de la discusión pública, sino participantes activos en un proceso que rompe con el paradigma tradicional de difusión (medio) - receptor (audiencia). Las nuevas tecnologías de la comunicación ofrecen enormes beneficios, pero siempre hay un precio que pagar. Irónicamente, las tecnologías que aumentan la ciudadanía son las mismas que intensifican el ojo electrónico y la sociedad de la vigilancia. Este artículo retoma el concepto de Foucault de panopticismo y la adaptación del diseño arquitectónico de Jeremy Bentham a las relaciones de poder. El presente manuscrito construye, de forma teórica, un acercamiento entre la sociedad de la información y los aspectos modernos de vigilancia en la vida cotidiana.

### Palabras clave

*Sociedad vigilante; panóptico, Sociedades de Control*

# Public Sphere and Panopticism: Considerations about surveillance in Everyday Life

Hélder Rocha Prior, LabCom - University of Beira Interior/ University of Brasilia (PNPD-CAPES)  
[helder.prior@gmail.com](mailto:helder.prior@gmail.com)

Received: 22/06/2014 • Accepted: 21/07/2014 • Published: 31/07/2014

**How to reference this paper:** Rocha Prior, H. (2014). Public sphere and Panopticism: Considerations about surveillance in everyday life. *Sphera Publica*, 1, (14), 23-38

## Abstract

At the present time, is not possible to discuss questions about Information Society and communication policy without mentioning the technological structures that enhance the public debate. Indeed, it is important to include the Internet and the social media in the set of stages which contribute to give the public sphere a higher coverage. In the current model of mass self- communication, the citizens are no longer only spectators in the arenas of public discussion, but active participants in a process that breaks with the traditional paradigm broadcast (*media*) – receiver (audience). New information technology offers huge benefits but there is always a price to pay. Ironically, the technologies increasing that citizenship are the same that intensify the electronic eye and the *panopticon* surveillance society. We believe that our societies need more ethics and politics discussion in an era of a certain vulgarization of surveillance practices. This article revisits Foucault's concept of panopticism and the adaptation of the architectural design to power relationships. The paper in hand constructs, theoretically, an approach between information society and modern surveillance aspects in everyday life.

## Key words

*Surveillance Society, Panopticon, Societies of Control*

## **1. Introduction**

Jeremy Benthan's panopticon project is one of the main metaphors of a society in which surveillance has become a routine and regular activity. In fact, these days, thinking in terms of a surveillance society brings to light the daily encounters with bureaucratic activity and the desire for efficiency, control and coordination of technological systems that support the contemporary world. Currently, surveillance is a daily practice that occurs unbeknownst to individuals. Throughout the world, surveillance is a pervasive phenomenon, present in physical spaces and, also, in virtual spaces that characterize network society. In this work, we seek to understand how web platforms process, store and analyze personal data without forgetting the theoretical foundations of surveillance studies.

## **2. Public Sphere, Mass Self Communication and Surveillance**

It seems appropriate to initiate the reflection on communication processes and electronic surveillance, specifically regarding the intensification of the surveillance practices in modern societies, assuming that currently it is not possible to discuss questions related to citizenship and processes of political communication and participation, without making reference to the technological structures that strengthen the public debate about public affairs. Actually, the rhetoric that surrounds the News Media embodies, as Dennis McQuail has pointed out, a decentralisation of the communication processes that break with the paradigm of broadcast (media) – receiver (audience) (McQuail, 2003:140). In the past decades, the public sphere was exclusively controlled by the agents of the Media system, specifically journalists and opinion makers, that selected the themes of public discussion, proceeding to a rigorous selection about what should come to public and what they should retain. Nevertheless, the current "Mass Self Communication" breaks with the traditional paradigm named "Gatekeeping", mainly because it allows citizens to have access to new ways of communicating and debating in a mobilisation and participation process around common causes. More recently, technological developments gave new opportunities to participate in society in alternative ways of mainstream media, ways based on information and communication technologies as e-democracy or social media, for example. According to the sociologist Manuel Castells, the Mass Self Communication or the individual communication of masses refers to the individual

assertion in the middle of a certain mass, that is, it is a sort of communication that “produces itself inside the brain of individual consumers who interact socially” (Castells, 2009:108). It is a new communication realm whose language are digital and whose senders are globally distributed and globally interactive. Castells argues that ordinary citizens are appropriating new means of horizontal communication to interact on networked communities (smartphones, videostreaming, blogs, digital and social media...). It is mass communication because potentially it can reach a global audience: it is individual communication because it is the subject himself that selects the concrete content of the message, escaping from the control purpose exerted by the gatekeepers or media agents. So, the Mass Self Communication offers alternative information or perspectives in the new media spaces.

But, by breaking with the communication processes of mainstream media, the Mass Self Communication has the advantage of defining, in a precise way, the implications of a communication in network. Now, dismissing the journalistic mediation, each individual can have access to the public sphere, limit the media agendas and the discussion themes and interact in the local and global networks of digital communication that characterizes society in a network. As the notion of cyberdemocracy presupposes a direct and unlimited access to knowledge and to public discussion, whether the individual subject or the political system in itself have found a way of communicating directly with the public avoiding, in fact, the journalistic reading when the time comes to (re)produce the content that has to be transmitted. At this point, we see a transformation in the institutional structure of communication and of the traditional media, mainly because the Mass Self Communication” literally refers to the individual assertion inside a certain mass.

In fact, the digital communication which characterises the society in network, supported by the communication model described by Castells (2009), a model in which the interpersonal communication, the mass communication and the individual communication of masses interact and complement each other, ended by changing the political communication processes and strategies. Thereof Castells himself has claimed that the “mass self communication” played a crucial role in Barack Obama’s victory in the United States Presidential Election of 2008 or, more recently, in the large protests against austerity measures that took place in Portugal and Spain organized on Facebook and Twitter. With the decentralisation of the communication processes, the political actors can now interact with the attentive public and the latter can show his opinions and dispositions about the republic management to the political sphere, or the formal sphere. By interacting

with political bodies programmed to deliberate, these new arenas of discussion and debates can result in the rational formation of opinions about issues that need to be regulated. However, and as the democratic discussion in network should not drain away in the virtual debates and in the individualisation of a public linked with technology, the power communicatively produced must be transformed in real actions or in reusable power.

### **3. From mass self communication to mass self surveillance**

However, there is one point that cannot be forgotten. The transformations, that we have been analysing, change not only the social relationships, but also the relationships of power which are inherent in the evolution of the own communication system. While citizens use new technological devices to participate in the public sphere, privacy yields to a system of digital exchange that easily transforms itself in power control. Therefore, it is suitable to analyse the inherent repercussions of the advances of new technologies, even if such analysis invites us to speculate on the return of a certain ubiquity of power. At this point, the panopticon image of Bentham can be used as a metaphor. From the generic point of view, surveillance is defined as a purposeful, routine, systematic and focused activity (Murakami, 2006, p. 5), used to manage people and populations. Currently, the society of surveillance is a paradigmatic case of interaction between technology and society, not so much referring to the struggle between work and capital, as Karl Marx has analysed it, but referring to the storage and recovery of data in archives – praxis of the bureaucracy highlighted by Max Weber-, and also regarding the specific dimensions of social life shaped by the adaption of technologies of information. Nowadays, surveillance capacities have quickly being extended and their capacities are implicated in basic questions of everyday life. As the functioning of new technologies rises, considerably, the “individual transparency”, the computers activity and the telecommunication activity allow a considerable development of the capacities of surveillance (Lyon, 1995:81-82). Actually, the electronic devices make easier either the knowledge acquisition, or, mainly, the storage and processing of data. By means of a cumulative process, such data processing allows to cross information stored with new data implicated in a development process of knowledge that seems to feed itself. In fact, data bases present themselves as a crucial element of operation of the intelligence services, since the bigger and more detailed a data base is, the bigger it is its capacity of information extraction, increasing the possibilities of

reaching new data or new signs (Whitaker, 1999:151-152). In fact, surveillance grows continually and the fast developing of the information and communication technologies are, also, a question of power. Power relations are inherent to modern surveillance processes focused on data and personal information. Facebook, for example, collects a lot of data from people and admits it. The IRS, and also the FBI, uses a variety of social media sites like Facebook, twitter, Myspace and Second Life to investigate people. Recently, the FBI decided to explore developing a web application that would monitor uses updates on social media sites. "On Facebook and other commercial web 2.0 platforms, mass self-communication is used for the purpose of mass self-surveillance" (Fuchs, 2011:139). Generally, the logic of functioning of data bases obey to the trading principle and collection of information in a relatively open and consented way by consumers, but that does not involve that there is not a certain resemblance between the functioning of data bases of private or public companies and the parallel functioning of the intelligence services. Actually, as well a process as the other allow the access to a certain sort of personal information about citizens that was collected according to a specific use; as well a process as the other are based in the prerequisite that such information is valuable and "constitutes a certain power". As Reg Whitaker explains this point:

The centralised and secret model has in some way been replaced by the decentralised and commercial model, although both work in parallel, using the same technologies, but in a different way. Nevertheless, there are important resemblances. Either public or private, governmental or organisational, data bases, in general, comprise information that can be interpreted by machines and that is connected to a network, being that such data have been collected according to one or both of these general aims: a) risk assessment and exclusion; and b) consumer identification and his inclusion (1999: 153).

Nevertheless, as we have seen, the concentration and processing of information collected and stored in databases increasingly wide correspond to a transverse characteristic either to companies, or to the political system itself. Thus, although currently the surveillance corresponds to multi-directional and decentralized dynamic, databases, by allowing the collection and the crossing of information organized in network, form a functional system more or less unified. It is worth noticing that in most cases, citizens provide information in a consented way by filling out commercial questionnaires that allow

to identify consumer's preferences and lifestyle. By managing business risks, such market researches facilitate the selection of the target audience. However, some information acquires a compulsory nature, as is in the case of the information provided to the tax system to the point that they can be proven in government databases. Whether in a case or in another elimination of risk is presented as crucial objective and it is commonly shared.

It is undeniable that new technologies (mobile communication, digital and social media and a variety of another social tools) have allowed the creation of platforms for interaction and debate that enhance our capabilities and increase, exponentially, the access to participate in the public sphere. But it is precisely what allows the establishment of a communication without spatial barriers and the easy access to knowledge, services and trade, which makes us more vulnerable to electronic surveillance. "The two aspects are inseparable. (...) Browsing the network allows us to contact with people from all over the world, but it can also mean that our communications might be intercepted by others that, at the same time, locate and identify us" (Whitaker,1999:199). Regarding this conceptual framework for action-oriented surveillance, it is important to include the operation of electronic mail (e-mail) throughout the systemic mechanisms of data interception. The junk mail, a term used when computers started generating mailing lists, is an example that shows the surveillance exerted over consumers. The customized ads that get daily into our e-mail box result from a variety of technological tools that companies have in order to direct themselves to potential consumers. As today societies are in an advanced stage of consumer capitalism, the social order remains stimulating and directing consumers to forms of integration that are articulated with the market. Marketing companies such as CCN, a British company dedicated to the intersection of data based on e-mail, stores the data of more than 43 million people and over 30 million units of financial information. The commercial surveillance is clearly one of the strategies of business enterprises and at the same time, an extension of capitalist surveillance that currently goes beyond the surveillance in the workplace. The power of capital is, thus, associated with the control of the consumer in a position of power where consumers' knowledge is transformed into power and capital. This industry of commercial data collects information that, in spite of not having an apparent relationship between them, allow to cross personal information including names, addresses, phone numbers, consumer preferences and even individuals and families remunerations that are crossed through mainframes of on-line access. Indeed, the more and more complex functioning of databases increases the

transparency of the subject. Citizens, workers and consumers are now more visible to the invisible watchmen that submit them to a control increasingly steady and imperceptible. The surveillance societies of contemporary days are a product of the so-called “information society”. Facebook’s chief security admits, for example, that the company uses technology to spy on private chats. Using smart software, this “social media” uses a computer program to scan chats and messages sent between users.

On the other hand, e-mail is one of the most used tools in interpersonal communication, but this does not mean that instantaneous access to mediated communication is proportional to guarantee the security of the established communications. As the e-mail servers have the ability to archive all incoming and outgoing e-mails, in case of interception, both the sender and the receiver of the message can be easily located through the e-mail address, and this increases the vulnerability of the system. However, nowadays this process is vastly magnified, such that all manner of everyday activities are recorded, checked, traced and monitored for a variety of purposes (Lyon, 2009: 7). If, as suggested by Whitaker, “it seems inevitable that governments, businessmen and other public and private organisations intercept and control e-mail” (1999:134), which will be the way to ensure a greater secrecy and privacy in communications at distance? The answer necessarily leads to the use of the field of cryptography and cryptanalysis. The name comes from the Greek *kryptós*, meaning “hidden”, and *gráphein*, meaning “writing”, and refers to the application of mathematical techniques that allow the content of a message to become legible only to the recipient. Little wonder, then, that the concept is very familiar to intelligence services of the States, mainly because it is one of the most advanced techniques of espionage. As Wayne Madsen adds about this:

The National Security Agency of the United States of America (NSA) has maintained for years a secret agreement with Crypto AG, a Swiss company that sells encryption technology to various countries and business organizations, allowing the NSA and intelligence services that collaborate with it full access to allegedly secret communications (Madsen, 1998:63).

On the whole, two forms of encryption can be identified, one symmetrical and the other one asymmetrical. In the case of symmetric cryptography there is only one cipher, that is, both the sender and the receiver of the message use the same password to



decode the message. In the case of asymmetric cryptography, it resorts to a combination of two keywords which are related; one public and the other one private, only allowing the receiver of the encrypted message to decode its content. The public key can be disseminated among many but the encrypted information can only be decoded by the holder of the private key. The private key, as its name suggests, is only known by the entity that generated it, and the cipher is never distributed. Both function as mathematical algorithms used to encrypt information, since any data encrypted by the public key can only be decrypted by the corresponding private key. Currently, there are some programs on the market that have allowed a sort of democratization of encryption. According to Whitaker, the best known is Pretty Good Privacy, a 128-bit system, extremely complex, which ensures the privacy of communications and which falls into the group of new techniques for counter-espionage and counter-surveillance.

#### 4. Living in a Society of Control: Foucault and Deleuze

It was precisely this digitisation logic that fits the reading proposed by Gilles Deleuze (2003) about the functioning of the “societies of control”. The Old Subjects, which had in the “major means of confinement” the concentration of power, were gradually replaced by logic of *wave* which has its most perfect analogy in the figure of the *snake*. While disciplinary societies are regulated by Watchwords, especially by the *signature* that indicates the *individual*, and by the *number* or registration indicating his position in a given *mass*, “in societies of control, by contrast, the main point is no longer a signature or a number but a code: the code is a password, while disciplinary societies are regulated by *watchwords* (not only from the point of view of integration but also of resistance)” (Deleuze, 2003:242).

Indeed, Michel Foucault (2009) set disciplinary societies as the succeeding model of Societies of Sovereignty, those societies that generate more than life they centred their power in decision criteria of death. Disciplinary societies, in fact, refer to the great confinement, following a hierarchical model where “all the coercive technologies of behaviour are concentrated” and intensified (Foucault, 2009: 300). They comply with a multiplicity of processes and meticulous techniques resulting in a Political Anatomy, of widespread location, and in a certain Microphysics of Power. According to Foucault, the body is monitored, from a social control that imposes coercion, prohibitions and

obligations, complying with an effectiveness and economy of movement and the activity processes. In the author's words: "these methods that allow a detailed control of the body operations and which ensure the constant subjection of its forces, thus imposing a relation of docility-utility, it is what might be called *disciplines*" (Foucault, 2009:141).

Foucault believes that the historical moment of the emergence of *disciplines* coincides with the birth of an art of the human body which does not focus only, neither in raising their skills, nor in raising the processes of subjection, but rather the establishment of a proportional relationship between obedience and usefulness. The *policy of coercion* is based in a working process related to the body. The process is aimed at controlling its movements by mechanical procedures of organic extraction. "The human body gets into a mechanism of power to be explored, dismantled and reassembled" (*Ibidem*). More than imprisoning the body, this *political anatomy* seeks a greater speed and effectiveness of the operating processes not only for the body to do what you want, but also to operate as intended. Consider the explanation of Foucault:

The discipline produces subjected and exercised bodies, "docile" bodies. Discipline increases the body strength (in terms of economic utility) and diminishes these same forces (in political terms of obedience.) In a word: separates the power from the body: on one hand, it turns that power into a "skill", which it seeks to increase, on the other hand it exchanges the energy, the power that could result from it and converts it into a relationship of strict subjection. If economic exploitation separates the force and the working product, we can say that the coercion of discipline establishes in the body a coercion link between an increased aptitude and an added domination (Foucault, 2009:142).

In his analysis related to the means of confinement, Foucault considered the discipline as a political anatomy of detail. It is a meticulous practise that has in the analysis of little things an elementary procedure in men's control and use. In the major means of confinement, individuals are distributed in a space in order to extract the maximum benefit from them, to know where and how to find them, to interrupt counterproductive contacts, to watch every moment, and watch any conduct to be appreciated or sanctioned. These techniques allow us to learn to master and to master to use, extracting the maximum benefit from them. Here too, the recovery time is crucial. The correlation between body and gesture is a condition of effectiveness and speed in a

process where the proper use of the body allows a better use of time. As Deleuze explains in this point:

Foucault has brilliantly analysed the ideal project of the means of confinement which is particularly visible in the factory: to concentrate, to allocate in space, to order in time, to set in space-time a productive force whose effect should be greater than the sum of elementary forces (Deleuze, 2003:239).

According to Foucault, the technique of confinement is visible in institutions such as school, factory or hospital. However, it is the prison that, particularly, represents the confinement model for excellence. In the large means of confinement, a perfect correlation between surveillance and architectural techniques that enable that same surveillance are witnessed. The Panopticon of Jeremy Bentham is, in fact, the architectural figure that allows this correlation. This metaphor can be applied to schools, hospitals, factories or even places of correction. It follows a very simple architectural design: in the periphery, there is a ring-shaped building, in the centre, a central tower with large windows opening onto the inside of the ring. The peripheral construction is divided into cells that cross the entire width of the building. Each cell has two windows, one facing the interior of the building, corresponding to the windows of the central tower, and another one to the exterior, and that allows light to pass through the cell from side to side. You just have to put a vigilant in the central tower and close in each cell a madman, a patient, a convict, a worker or a student. Due to light effect, any gesture made in the cells of the periphery can be controlled from the central tower. In this way, the warder can see without being seen, however. Like this, visibility becomes a trap. Therefore, the panoptic machine makes possible a state of permanent visibility, ensuring, in a sense, the automatic operation of power. As the prisoner never knows if he is being spied upon, he must presume that he may be being spied on, mainly because he experiences a state of continual visibility.

Control is attained by the constant sense of presence of an invisible eye. Through a simple architectural idea, the morals were reformed, the health preserved, the instruction diffused, the public burdens lightened. The more individuals who should be inspected are at the mercy of the eyes of individuals who must inspect, or, at least, the better such an impression can be caused, the easier the model gets closer to the ubiquity of God. The Panopticon, or “the place where you can see everything”, manufactures, in that way,

homogeneous effects of power. Actually, Foucault is a foundational thinker on Surveillance Studies.

Despite the genius of the analysis proposed by Foucault, the author was aware of the brevity of the model of the major means for confinement. The disciplines, before the appearance of machinery of a third kind, would undergo a crisis which resulted in the advent of a new kind of society. As Deleuze says on this point:

We are in a general crisis of all means of confinement, prison, hospital, factory, school, family. Family is an interior, in crisis as well as other interiors, educational, professional, etc. The responsible ministers have been announcing supposedly necessary reforms. Reforming school, reforming the industry, hospital, the armed forces, prison, but everyone knows that these institutions are disappearing, at a longer or shorter term. It is just about managing their distress and keeping people employed until the installation of the new forces that are already knocking at the door. These are the societies of control that are in the process of replacing disciplinary societies (Deleuze, 2003:240).

In societies of control, we are no longer in the presence of the pair mass-individual. It is no longer the number or registration that indicates the position of the individual in a given mass, because individuals have transformed themselves in divisible beings, divisible into elements, and on the other hand, the masses into data or samples that, as we have seen, allow the management and elimination of risk. According to Deleuze (2009), it is a mutation of capitalism, a capitalism that no longer focuses on the pursuit of capital gains by the consequent logic of the maximization of sales and decrease of the costs of production, but in marketing. In this dispersed system where factory ceded its place to the company, marketing becomes a control tool whose numerical language is the cipher. The same cipher that refers to the position of each individual, his tastes, his preferences, his virtual tours, his wavy state or even his own state of mind. The location of individuals in space and time, as well as the coordination of their activities depends on the interaction of humans with machines that, paradoxically, are becoming more and more autonomous. In Marx's words: "The new surveillance is there, without coups d'Etat or revolutions" (Marx, 1985, cited in Lyon, 1995:82).

In this new framework of capitalism, where intelligent marketing has gained more and more strength, the undifferentiated mass of individuals has led to consumer groups with specific characteristics. That is why the key to the new intelligent marketing is based in

information and in the data accumulation about the consumer's characteristics. Through a selection of informative profiles, the databases exclude groups considered at risk and include informative profiles whose characteristics are close to the audience of potential consumers. Thus, cyberspace acts as a parallel world where we all have an invisible profile to the real world and that is a sort of reply regarding what we actually are. A profile becomes visible through the look allowed by the electronic eye. The surveillance made possible by the advent of new technology makes, in effect, individuals visible in a way that Bentham could not conceive. The inspector of the central tower was gradually replaced by a multiplicity of inspectors, in a surveillance process that is now decentralized and consensual. According to Whitaker:

Every time we make a purchase or financial transaction, every time we buy shares, somewhere (and the record of these activities is more and more complete) we are briefly illuminated by the now ubiquitous and decentralized *panopticon*. This momentary transparency, along with all the other moments that are registered by an electronic data processing, sets up a unified model. It is known that new technologies have wiped away many jobs, what is not known is that the first unemployed of this new era is the inspector / Big Brother. (...) The strength of this new *panopticon* lies in the voluntary participation of people thanks to the benefits and advantages it offers, since people are less likely to perceive the harm and threats (Whitaker, 1999: 171-175).

Credit cards and / or payment cards, for example, offer a high degree of convenience in financial transactions, but the fact remains that the magnetic tape let know what we have bought, where we have done it, where we have been and in some cases where we go. The operation of ATM systems can identify personal preferences and physical movements and add this data to the consumer profile. The American company AT & T, the telecommunications giant was responsible for creating a card that combines the functions of credit card, bank identification card and phone card. In Portugal, cardmobili is a service that allows to store in the mobile phone loyalty cards inherent in consumption. The consumer only has to sign in the company website with a valid e-mail address, and install the application on the phone. Since then, nearly 200 cards which are now available for download are transferred to the mobile phone and they can be shown in the corresponding stores. This dematerialization of cards is, indeed, convenient for the customer but we must not forget that it opens space for the combination of data that were previously dispersed.

Consumption compensates for the consented participation in the new electronic panopticon. Whitaker points out that: "Currently, when the panoptic surveillance challenges the subject, it makes it by understanding his needs and fulfilling his desires" (Whitaker, 1999:177). If Bentham's Panopticon allowed the isolation of individuals through a centralized and hierarchical architectural construction, technology in the service of intelligent marketing is oriented towards the differentiation of the consumer, individualizing his tastes and needs. As we see, at this point the similarity is structural.

Although much of the surveillance is, in fact, commercial, the issues mentioned above do not exempt a sociological, ontological and political analysis of a particular dimension of social life that has been accelerated by the development of information technologies. We can characterize web 2.0 as mass self-surveillance where a group or population is monitored in order to detect and store their personal data and individual differences (Fuchs, 2011, 138). Social media companies aggregate, collect and storage personal data provided by users, a process sometimes called participatory surveillance or dataveillance. Facebook, in fact, stores, associate and sells the personal data and the preferences of more 500 million users. The behaviour of each user, their personal likes and dislikes are collected and have economic purposes. On the other hand, social media sites like Facebook, Twitter or Foursquare are designed for users investigate, continually, digital behaviour and digital traces left by their friends. As Marwick says on this point:

In communities where social technology use is prominent, a single person may have a Facebook profile, a Twitter account, a Tumblr blog, a Foursquare account and an Instagram photo stream, each transmitting personal information to an audience. This information is broadcast to be looked at, and as such, people can look closely. The constellation of practices framed variously as stalking, watching, creeping, gazing or looking are characteristic of social media use, but this social surveillance creates panoptic-type effects (Marwick, 378-379).

## **5. Conclusions**

Like all arts, With web 2.0, users are producers of information (prosumers), but the collection of personal data and the interconnection of these data across multiple platforms converts web 2.0 into a social or participatory panopticon that exerts power and domination. If, as we advocate in this paper, surveillance has an institutional dimension as

a generator of power, it might be interesting to consider, not only the potential of the new, more comprehensive public sphere, but also the implications this wider scope, which have to do with a certain contraction of private space. As there cannot be changes in the public sphere that do not simultaneously affect the private sphere, the distinction between public life and private life is dissolved as states and corporations collect personal data, ignoring the old boundaries. Indeed, while we participate and benefit from the processes of the current communication network, privacy is lost in cookies and strategies for the recovery of personal data.

## 6. Bibliography

Castells, M. (2009). *Comunicación y Poder*. Madrid: Alianza Editorial.

Deleuze, G. (2003). "Post-scriptum sobre as sociedades de controlo". In *Conversações*, Lisboa: Fim de Século Edições.

Foucault, M. (2009). *Vigilar y Castigar; Nacimiento de la prisión*. Madrid: Siglo XXI Editores.

Fuchs, C. (2011). New Media, Web 2.0 and Surveillance. *Sociology Compass* 5/2, 134-147.

Habermas, J. (1989). *Teoría de la Acción Comunicativa: complementos y estudios previos*. Madrid: Catedra.

Kant, I. (1995). *A Paz Perpétua e Outros Opúsculos*. Lisboa: Edições 70.

Lyon, D. (1995). *El ojo electrónico; El auge de la sociedad de la vigilancia*. Madrid: Alianza Editorial.

Lyon, D. (2009). Surveillance, Power and Everyday Life. En R. Mansell, C. Avgerou, D. Quah, and R. Silverstone (eds.). *The Oxford Handbook of Information and Communication Technologies*. Oxford: Oxford University Press.

Madsen, W. (1998). Crypto AG: the NSA'S Trojan Horse?. *Covert Action Quarterly* (<http://mediafilter.org/caq/cryptogate/>).

Mattelart, A. (2009). *Un Mundo Vigilado*. Barcelona: Paidós.

Marwick, A. E. (2012). The Public Domain: Social Surveillance in Everyday Life, *Surveillance & Society* 9(4), 378-393.

Marx, G. T. (1985). The Surveillance Society: the threat of 1984-style techniques. *The Futurist June*, 21-6.

Mcquail, D. (2003). *Teoria da Comunicação de Massas*. Lisboa: Fundação Calouste Gulbenkian.

Murakami, D., Ball, K., Lyon, D., Norris, C. (2006). *A Report on the Surveillance Society*. For the Information Commissioner by the Surveillance Studies Network.

Whitaker, R. (1999). *El fin de la privacidad; como la vigilancia total se está convirtiendo en realidad*. Barcelona: Paidós.