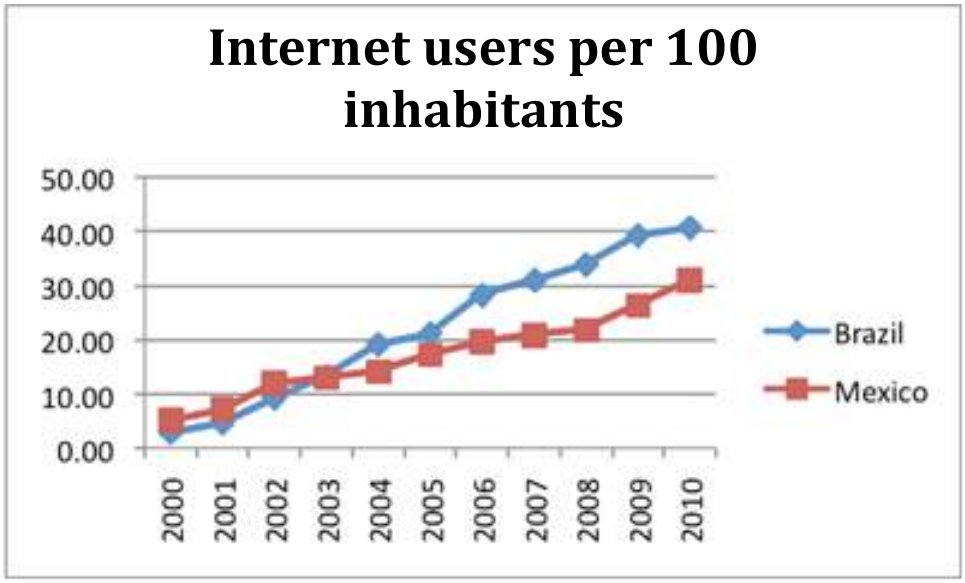
5. SECTION ON PERSONAL DATA ON THE INTERNET

5.1 Introduction: The context of conditions of access to Information and Communication Technologies (ICT) in Latin America

The conditions of access to and use of information and communication technology (ICT) differ substantially in developed countries and in the developing world. While the former are concerned with issues related to network use, for the latter, universal access continues to be a challenge present on the agenda of their public policies and governments.[40]

Historically, the use of the Internet in Latin America begins in 1996 and evolves slowly: in 1998, less than 1% of the population was connected (Hilbert, 2001,) a figure that represented the highest-income individuals. As of that year, the percentage of the Latin American population on the Internet began to expand and rapidly evolve, reaching 9.9 million in 2000, a number that jumped to 60.5 million in 2005[41]. Graph 13 shows the evolution of the number of Brazilian and Mexican Internet users from 2000 to 2010:

Graph 13: Number of Internet users per 100 inhabitants



[40] A research project of the UNCTAD performed in 2002 in 51 countries shows the differences between these two groups of countries with regard to the strategies used to develop their information society. A concern with awareness, training and education appear repeatedly in both groups. However, the developed countries tend to prioritize regulatory and legal aspects, while the developing countries prioritize the development of infrastructure and the universalization of access (UNCTAD, 2002).

[41] E-Marketer data available at: www.emarketer.com/Reports/All?Latam_aug06.aspx.

This development was accompanied by government initiatives and digital inclusion policies for developing an information society. In Brazil, these initiatives were assigned to the Ministry of Science and Technology or the Ministry of Communications, as is the case of the "Information Society Program", established in 1999, and the "National Broadband Plan" that commenced in 2010.

Based on the information obtained by the International Telecommunication Union in 2008 (UIT, 2010), in recent years, Brazil and Mexico have reached high levels of access with the use of new technologies reaching most of their inhabitants. However, the positioning of these countries in the worldwide scale of information technology and communication development[42] shows that there is still much to do: Brazil is only ranked in 60th place and is the fourth best positioned country of Latin America, behind Argentina, Uruguay and Chile (which appear in 49th, 50th and 54th position, respectively) and ahead of Mexico, which is ranked at 77th. With regard to universal access[43], Brazil is ranked 65th; in use[44] it is ranked 54th, and in ability to use new technologies[45], it is ranked 61st.

One of the most immediate consequences of this situation is the level of discussion surrounding the regulation of the network in these countries. In general, these discussions are incipient and unconsolidated, as is the case of the debate on the privacy, collection and treatment of personal data in Latin America.

i. Brazilians online

As per data provided by the Internet Management Committee of Brazil (CGI.br, 2010), currently, 35% of Brazilian homes have a computer and 27% have Internet access. The data shows that the speed of the Internet connections in Brazilian homes has increased in the past three years and that the main reason for accessing the network is communication (94%), followed by searches for information and leisure (87% each), education (66%), and financial services (17%). E-mail was the main activity performed (80%), followed by instant messaging services (74%) and social networks, such as Orkut (70%).

[42]To perform this measurement, the report is based on an indicator called IDI (ICT Technological Development) that includes various indicators related to the access, use and ability to handle information and communication technologies. The first and second groups appear with a weight of 40 years, and the last with a weight of 20.

[43] The access index is the result of five indicators: the proportion of homes with computers, the proportion of homes with Internet access, access to broadband for Internet users, penetration of land telephone lines and penetration of cellular telephone access (ITU, 2010).

[44] The use index is calculated based on the number of Internet users per each one hundred inhabitants, the number of broadband subscribers per each one hundred inhabitants and the number of mobile broadband Internet subscribers per each one hundred inhabitants (ITU, 2010).

[45] The ability index is the result of the adult literacy rate and the GER (gross enrollment ratio) in secondary and tertiary education (ITU, 2010).

Home is the primary location of Internet access in the country: 57% of Internet users access the network from their homes, while 34% use public access locations such as cybercafés. It is interesting to note that, in 2007 and 2008, the use of these establishments exceeded access from homes, which shows the important role played by public access centers in the process of digital inclusion of the country. At date, 77% of those who use these locations do so because they do not have a computer at home and 72% because they do not have an Internet connection. Fun, social interaction and online games also appear as reasons for using cybercafés, representing 40%, 25% and 20%, respectively, of Brazilian Internet users.

Some statistics are related to security practices and access to personal data. Of the total number of Internet users in an urban area, 20% identified the security devices such as passwords, registration, usernames and anti-spam tests as a difficulty in managing Internet use. Of those who have used the Internet but have never purchased products online, 29% indicated that one of the reasons they did not do so was a concern regarding the privacy or security of these transactions and a resistance to supplying personal data or information, such as credit card information, over the Internet. Fifteen percent of the population that uses the Internet mentioned a concern for protection of the security of their information as a reason for not using the electronic government services.

ii. Mexicans online

Based on the information available in the studies performed by the IWS Corporation on Latin America and the Caribbean that cover 20 countries, Brazil is the most populated country of the region (201,103,300 inhabitants) and has the highest number of Internet users in the area (75,943,600). The penetration of the Internet in Brazil (37.8%) was higher than the world average (28.7%) and the average of the region (34.5%).

Mexico, the second most populated country of Latin America (112, 468,855 inhabitants), is the nation with the second highest number of Internet users in the area (30,600,000). However, Internet access in Mexico (27.2%) was below the world average (-1.5%) and the average of the region (-7.3%).

With regard to population Internet access, the highest level of access was found in Argentina (64.4%), followed by Uruguay (52.8%), Chile (50%), Colombia (48.7%), Costa Rica (44.3%), Brazil (37.8%), Venezuela (34.2%), the Dominican Republic (30.5%) and Panama (28.1%). Mexico was ranked tenth in the region in this regard.

However, Mexico is the country with the most Facebook users in Latin America (15,037,020). Its penetration was established by the IWS to be 13.4%. This is based on the fact that, in 2010, there were considered to be 112,468,855 inhabitants in Mexico. The IWS did not present the “Facebook index” in Mexico, which is estimated at 49.14%. This means that, for every 10 Internet users, 5 are Facebook users. The IWS estimated the “Facebook index” to be 35% for the region.

Based on the results obtained in *The Global Information Technology Report 2009-2010* (World Economic Forum), Mexico was ranked 78th of the 133 countries analyzed. In the study corresponding to the period from 2008-2009, it was ranked at 67th. In the period from 2007-2008, it was ranked 58th of the 127 countries analyzed. Based on the results of the studies performed by the World Economic Forum, in the period from 2007-2010, Mexico dropped 20 places with regard to technological competitiveness. The results obtained for certain indicators included in *The Global Information Technology Report 2009-2010 study are very revealing.* For example, in "availability of new technologies" Mexico was ranked 79th; in laws governing new technologies, it was ranked 67th; in number of telephone lines, 67th; in security of Internet services, 60th; accessibility of digital content, 87th; broadband, 80th; home telephones, 108th; broadband rates, 73rd; mobile phone rates, 79th; landline phone rates, 100th; priority of information and communication technology (ICT) for the government, 96th; public contracting of advanced technology products, 93rd; importance of ICT to the government's vision for the future, 74th; mobile telephone subscriptions, 91st; Internet users, 79th; Internet access at schools, 77th; capacity for innovation, 80th; level of use of Internet by businesses, 78th; success of government in promoting the use of ICT, 100th. In the quality of teaching of mathematics and sciences, Mexico was ranked in 123rd position.

In view of the above and based on the results of the *Global E- Government Survey 2010, which is an annual report prepared by the United Nations Public Administration Network (a United Nations organization) to evaluate the effectiveness of the strategies and actions implemented by governments with regard to e-government, Mexico was ranked at 56. In the 2008 edition of this study, it was ranked at 37. It is necessary to determine why in a period of two years Mexico dropped 19 positions in the world ranking.*

It is necessary to mention that the principal studies on Internet users in Mexico agree that there is an important gender gap in Internet access. Based on the AMIPCI study, 55% of Internet users are men and 45% are women. However, the results of the WIP study shown in the chapter on Mexico indicate the gender distribution to be 58% men and 42% women. Also, in Mexico, most Internet users are young: 61% of users are under 25 years old, a figure that does not include those younger than 12. Also, 76% are under 32 years old.

5.1.1. ICT and protection of personal data in Latin America

The situation of development of new information and communication technologies, particularity the Internet, gives rise to a new paradigm for the protection of personal data. On the one hand, there is the ease with which information is transported, stored and processed, which increases astronomically with the evolution of ICTs. On the other hand are the specific characteristics of the functioning and architecture of the Internet which consist firstly of the transfer of files between computers shared by the entire world and whose use is closely related to registration practices. On the Internet, everything can be traced, stored and coded, and many of these practices are interrelated, even the network maintenance and operation protocols.

This new reality leads us to the necessity of regulating the practices and flow of communications in this new environment. However, in the Latin American region, only certain countries are nearing a debate on the protection of personal data in either the academic or legal field. Chile was the first

Latin American country to have a consolidated law on this issue (19.628), followed by Argentina (25.326), which stands out as the only country in the group whose legislation is recognized as adequate by the standards of the European Union. In Uruguay, a new specific law on the issue was enacted in 2004 and abolished with the publication of the new law in 2008 (18.331). In Colombia, the debate on the issue is more recent, although this country already has a law for the protection of personal data (Nougrères et al., 2008).

In Mexico, it was in 2010 that the Federal Law for the Protection of Personal Data Held by Individuals or Corporate Entities (LFPDPPP, Spanish acronym) was issued. This law governs the legitimate, controlled and informed treatment of this information. As indicated in the sections on CCTV and identification cards, in a context of development of information and communication technologies, the LFPDPPP has been presented as necessary and several sectors of society and the government indicated the need to develop these regulations as a result of the absence of governance in this regard.

Therefore, this law strengthens the emerging standards that govern access to information and the protection of data by the authorities and recognizes individuals and private corporate entities, etc., as the parties governed by this law; however, it exempts its application to credit bureaus in view of the provisions already established in the Law for Governing Credit Bureaus and other applicable provisions, and also exempts its application to individuals who collect and store personal data that is exclusively for personal use without any intent for commercial disclosure or use.

The above is due to the fact that the Law for Governing Credit Bureaus establishes a specific legal procedure for the protection of the information of individuals and corporate entities as a result of the gathering, handling and delivery or sending of information related to their credit history, credit transactions and other similar transactions.

From a legal standpoint, the LFPDPPP is focused on:
- Guaranteeing the privacy of the individuals; that is, it must protect the individual's own specific information so that it is seen by few.
- Create a right for the individual to auto-determine whether to inform, which consists of recognizing the freedom of individuals to know that their information has been noted, filed, used or transferred by any method; to who, when and for what purpose.

In other words, it establishes a channel for individuals to enjoy legal protection with regard to the treatment of their personal information, since the automation and computerization of such, in addition to placing their private life at risk, involves the use, disclosure and storage of personal data by any means.

The use of this law covers any action of access, handling, use, transfer or disposal of personal data.

Finally, the law establishes a series of principles and rights, for which the limits of observance and exercise are: the protection of national security, order, public security and safety and the rights of third parties.

Through this Law, the Mexican federal government has attempted to govern several of the principal actions that are being taken with regard to security, such as the proliferation of video surveillance and the implementation of a sole individual identification card. The Law also represents progress with regard to computer regulation, although, as discussed below, its governance in this regard is inconsistent due, to some extent, to the wide range of problems that derive from the issue of the Internet.

Of the countries of the most economic importance in Latin America, Brazil is the only one that does not yet have a law to protect personal data. There are currently three primary legal frameworks in the country in this regard: the one referring to privacy that appears as a fundamental guarantee in the Federal Constitution; the action of *habeas data* that recognizes the individual's right to control his/her own information; and the protection of consumer data, which refers to cases related to information processing initiatives. Currently, the consolidation of a comprehensive regime is under discussion in the country through a bill for the protection of personal data that would protect citizens in virtual space[46]. This bill seeks to govern common online practices, such as data processing for addresses for advertising campaigns and relevant content or the transfer of this information between various companies, which are issues of particular concern with regard to the issue of the protection of personal data in Brazil.

5.2 Personal data on the Internet in Brazil

5.2.1 How the Internet mapping was performed in Brazil

The purpose of the mapping was to identify the relevant players in the processing of surveillance and control of personal data on the Brazilian Internet. Six areas were proposed in the mapping: legislation, academic studies, technology, corporations/institutions, civil society and events, and the specific methodologies described below were applied to each of such areas:

i. Legislation

General Objective:

Review Brazilian legislation at the national and state level to identify laws, bills and regulatory frameworks related to the treatment of personal data on the Internet in Brazil.

[46] The bill for the protection of personal data was inspired by Directive 95/46/CE of the European Union and went through a period of public consultation and is now awaiting presentation to National Congress.

Specific Objectives:

a) Identify laws in force and bills at the national level and in three Brazilian states: Rio de Janeiro, São Paulo and Paraná;

b) Identify the legislators, their political parties and the regions of the country they represent;

c) Identify the year the law or bill was proposed;

d) Identify the most recurring issues related to the regulation of personal data on the Internet in Brazil;

e) Identify the players responsible for the regulation of personal data on the Internet in Brazil.

Databases consulted:

a) Online search systems of the Federal Senate website (http://www.senado.gov.br)

b) Online search systems of the Chamber of Deputies website (http://www.camara.gov.br)

c) Online search systems of the Legislative Assemblies of the states of Rio de Janeiro (http://www.alerj.rj.gov.br), São Paulo (http://www.al.sp.gov.br) and Paraná (http://www.alep.pr.gov.br)

Methodology:

We analyzed the bills and legislation in force at the national level and in three Brazilian states: Rio de Janeiro, São Paulo and Paraná. The states selected were those shown to have some level of progress in the regulation of cyberspace, in order to evaluate whether the issue of personal data was also addressed in this context.

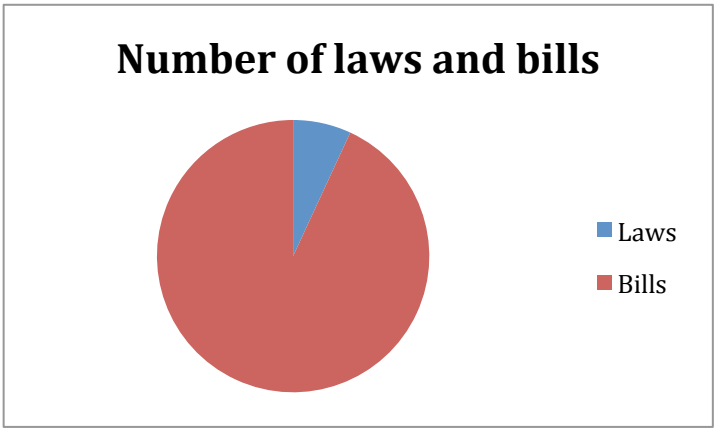
The methodology adopted is based on visiting websites where the bills and legislation in force are found in the Chamber of Deputies, Federal Senate and the Legislative Assemblies of the three selected state, searching for the term "Internet" on each site[47]. The results pages were explored from

[47] Since the search functions of these sites were not very effective, we managed without the specific terms included in the dictionary of keywords of this investigation and decided to search only on the Internet, reviewing all of the results found. There were 832 Chamber bills, 113 Senate bills, 116 cases of federal legislation in force, 493 bills of the Legislative Assembly of the State of São Paulo, 124 cases of legislation in force for that state, 493 bills of the Legislative Assembly of the State of Río de Janeiro, 49 cases of legislation in force for that state, 30 bills of the Legislative Assembly of Paraná and 11 cases of legislation in force for that state.

November 2010 to February 2011 and all of the bills or laws related to the subject were recorded for subsequent analysis.

In total, 8 laws and 108 bills were analyzed, representing a total of 116 records. Graph 14 shows the number of pertinent projects for this item.

Graph 14: Number of laws and bills



The analysis of the material began with the creation of a dictionary of subjects[48] and the manual classification of the most recurring issues. For each law or bill, three types of indexes were used: a principal index showing the relationship of the project to the research; a thematic index for measuring the recurrence of issues, players and actions; and indexes for the justification of the bills, based on the reading of the section of such where the authors argue their objectives and the importance of the issue.

Results:

a) General Description: recurring issues

We identified that, in general, the types of bills and laws in force were repeated with significant frequency, both at the federal and at the state level. We have listed below the most recurring issues in the results found:

- Responsibility of cybercafés, requesting **user registration and identified** (which at times includes the use of surveillance cameras in these establishments), in an attempt to impede

[48] See Exhibit X of the dictionary of subjects used in the classification of Laws and Bills, as well as their frequency in absolute values and percentages.

crime and/or protect children and adolescents

- Adoption of measures to guarantee Internet security that create classifications and sanctions for crimes carried out through the Internet, such as fraud, falsification, invasions, interception and/or violation of data, propagation of malicious software, pornography and pedophilia, etc.
- Projects to **prohibit anonymity** and create **registration and identification** mechanisms, whether for **Internet access** (through access providers) or for **offering and using various services**, such as website publication, blogs, interaction in forums, use of e-mail addresses and records of domains. Many of these projects also include the **storage of communications and user access logs.**
- **Discipline of user accesses,** through the adoption of **indicative classification** mechanisms for the control of access to adult sites/content; creation of education programs in schools and proposals for the installation of **content filters** in learning institutions; public distributions or even offering of such by access providers to the general public.
- **Receipt of unsolicited commercial messages** (considering this action at times to be an invasion of privacy, which generates debate regarding the obtention of the recipient's e-mail address).
- **Regulation of the validity of the digital signature**, through prior registration and the electronic document (frequently as a means of regulation for electronic commerce).
- **Regulation of the concession of data for police investigations and espionage** through the Internet, of both a domestic and international nature, as well as the creation of organizations specialized in computer crimes.

b) Players:

The following players were identified:

- Providers of Internet access, hosting, e-mail or other services (chat rooms, discussion lists, forums, websites with adult content and portals)
- Authors (of sites and blogs)
- Participants/users of these sites and services
- Owners of cybercafés and electronic gaming establishments
- Learning and research institutions (schools, universities, etc)
- Public administration bodies and entities

The most recurring players were the providers, who appear in 34% of the bills/laws analyzed, and for participants/users, children and adolescents both appear in 15% of the bills/laws.

c) Levels of responsibility

Most of the bills seek to make the network administrators, providers and users responsible for practices that involve the identification and handling of personal data. The following levels of responsibility were observed for the players identified:

- The service providers or site owners as responsible for the content published by the participants: the individual responsible for the site must moderate it and remove inappropriate content and identify illicit practices or their authors
- The authors of e-mails or comments and publications on websites as responsible for the content published
- The providers, institutions and site owners as responsible for disciplining access and use by creating codes of conduct/security to which the users are to be subject
- The providers of access and services, including the owners of cybercafés, as responsible for the identification of users by keeping logs and registration data for a certain period of time (set or not)
- Providers of access and services as responsible for the security and functioning of the systems offered to the public
- Providers of access and services as responsible for protection of the data stored (registration information, logs or contents of user communications)

d) Classification of the bills/laws based on their implications for the treatment and regulation of personal data on the Internet

We were able to classify almost all of the bills/laws into six broad categories, based on the target issues/practices and their consequences for the treatment and regulation of personal data on the Internet.

- 34% institutionalize registration routines and seek to prohibit anonymity
- 24% propose the adoption of practices that imply the identification of site owners, participants, infractions and/or infractors

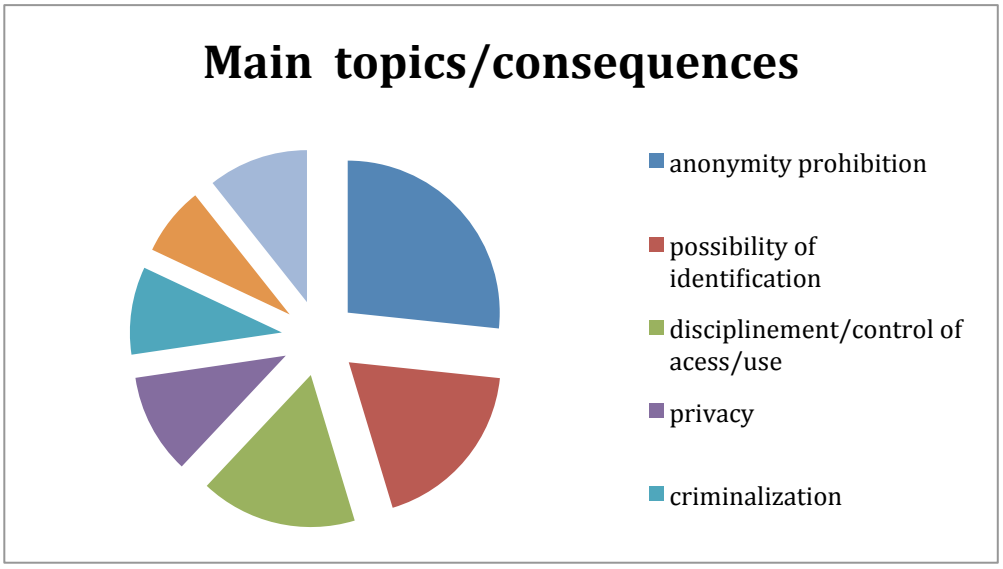
- 22% involve disciplining/controlling access and/or use of the network and propose the adoption of content filters and mechanisms/codes of conduct that regulate access to sites considered to be inappropriate (especially for minors)

- 14% include privacy defense mechanisms

- 12% are focused on defining the crimes committed through the worldwide computer network

- 9% are aimed at data protection, with the adoption of practices to improve the security of web transactions

Graph 15: Main topics/consequences



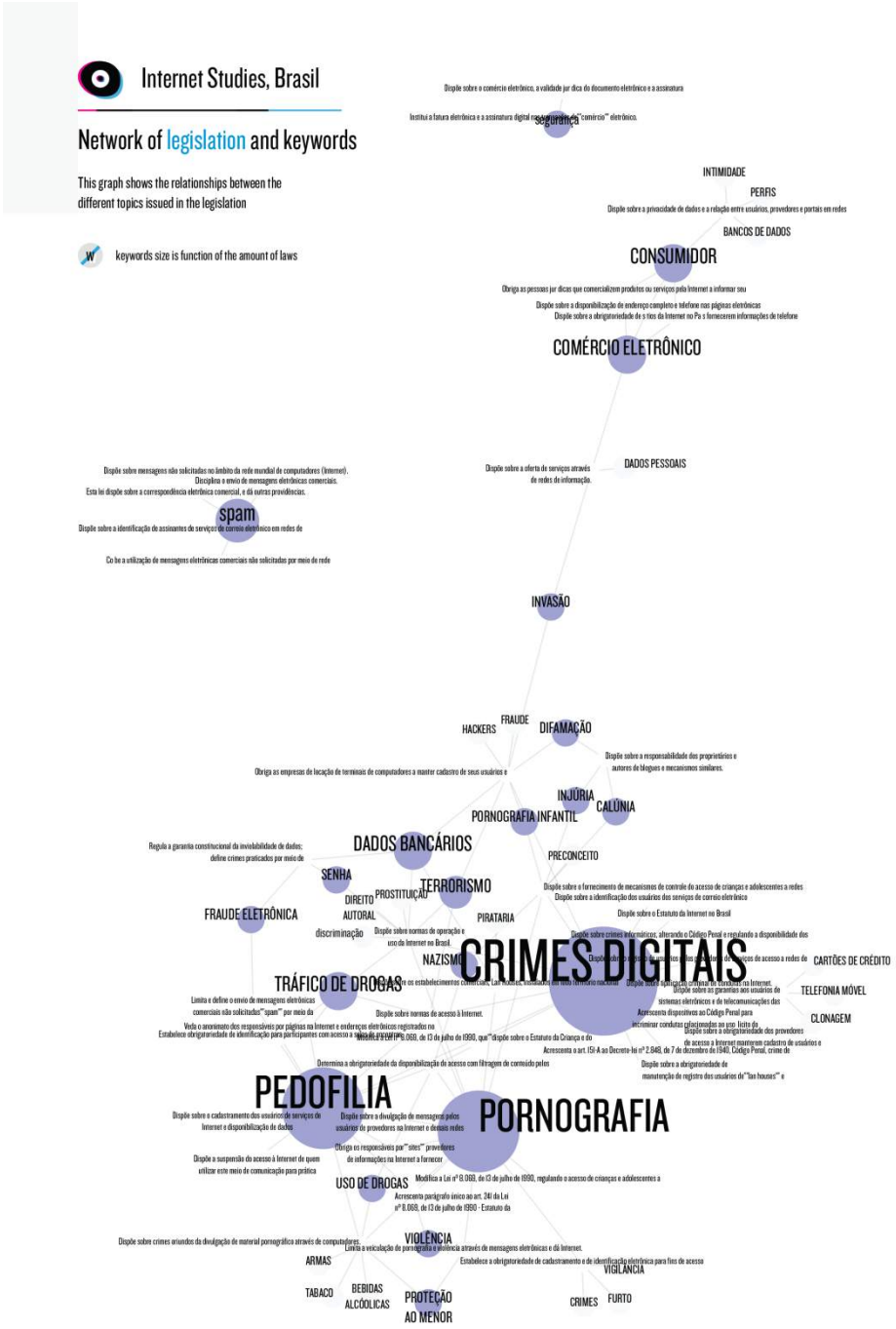
e) Trends observed

Based on the classification made in the previous point, the following trends are present:

- Privacy: Security privilege that results in the effort of classifying crimes and vetoing anonymity

A fundamental conflict reoccurs in the bills and laws analyzed: the intention of protecting privacy is confused with security premises and appears almost side by side with the intention of vetoing anonymity for the purpose of guaranteeing online security and fighting crime. This statement can be supported by the significant percentage of bills that include registration (47% of the total) and the equally important number of bills for criminal classification or that mention in the text that their justification is to attempt to impede the use of the network for performing illicit acts (67% of the total).

Graph 16: Network of laws and bills and keywords



The crimes that are focused on the most are sex crimes: the crime most referred to is pedophilia, which appears in 19% of the bills/laws, followed by pornography and child pornography, which appear in 18% and 6% of the bills/laws analyzed. Next come data violation crimes: electronic fraud (16%), invasions (9%), interference in data systems (6%) and attacks and forgery (3% each).

Recurring reference was also made to the use/trafficking of drugs (9%), terrorism (6%) and Nazism (3%). Crimes such as slander, defamation, calumny and slander are among those with the fewest references (each appears in 3% of the bills/laws analyzed).

In the bills that include registration, we observed that 16% include the provision of maintaining an access log. Another constant was the institutionalization of the need to link civil identity to a terminal or IP, which deeply hurts the right to open networks.

It is important to mention, in this context, the addition of the Senate to Chamber Bill 89/2003, known as PL Azerdo. Already approved by the Senate and being processed by the Chamber of Deputies, this bill seeks to halt the increase in virtual crimes, especially pedophilia. However, its text contains inconsistencies that allow consequences to arise that threaten the fundamental practices of cyber culture, criminalizing even actions such as shared use and access to P2P networks based on principles of intellectual property. The bill establishes the need of maintaining access records, which could delay initiatives of digital inclusion even more, as well as the criminalization of common practices such as the transfer of data or information available on a computer network, communication device or information system without authorization from its legitimate owner.

- **Cybercafés and prohibition of anonymity**

In the bills/laws that include practices for prohibiting anonymity in Internet access, one of the most recurring issues is the regulation of the use of cybercafés for purposes of prohibiting anonymity in the access obtained through these establishments. 18% of the bills analyzed address this issue and almost all of these laws/bills institute the collection of registration and surfing data for the use of the computers, while some even include the implementation of security cameras in these environments. Some of these laws/bills aimed at ensuring the wellbeing and protection of minors adopt disciplinary measures for use, such as the prohibition of access to those under 12 years of age, regulatory conditions for access to those under 18, prohibition of the sale of cigarettes and alcoholic beverages, and the adoption of measures to guarantee the health of the users of these establishments (adequate lighting and volume of the computers, as well as limit to the number of hours of permitted use). The three states under analysis already have laws of this kind[49].

- **Protection of children and adolescents and content filters**

The protection of children and adolescents appeared as the second most recurring objective/justification and was included in the intent of 19% of the laws/bills. In addition to the regulation of cybercafés and the definition of computer crimes, the implementation of obligatory content filters also appears as a recurring subject with regard to this sector of the public. In an attempt to impede undue access to sites at homes, schools and public administration, filters were

[49] In Sao Paulo they have Law 12.228/2006, in Rio de Janeiro, Law 5.132/2007 and in Paraná, Law 16.241/2009.

cited in 13% of the bills/laws, both at the federal and at the state level, often accompanied by the idea of installing code classification mechanisms, which was mentioned in 11% of the bills analyzed.

- **Spam and Opt-Out**

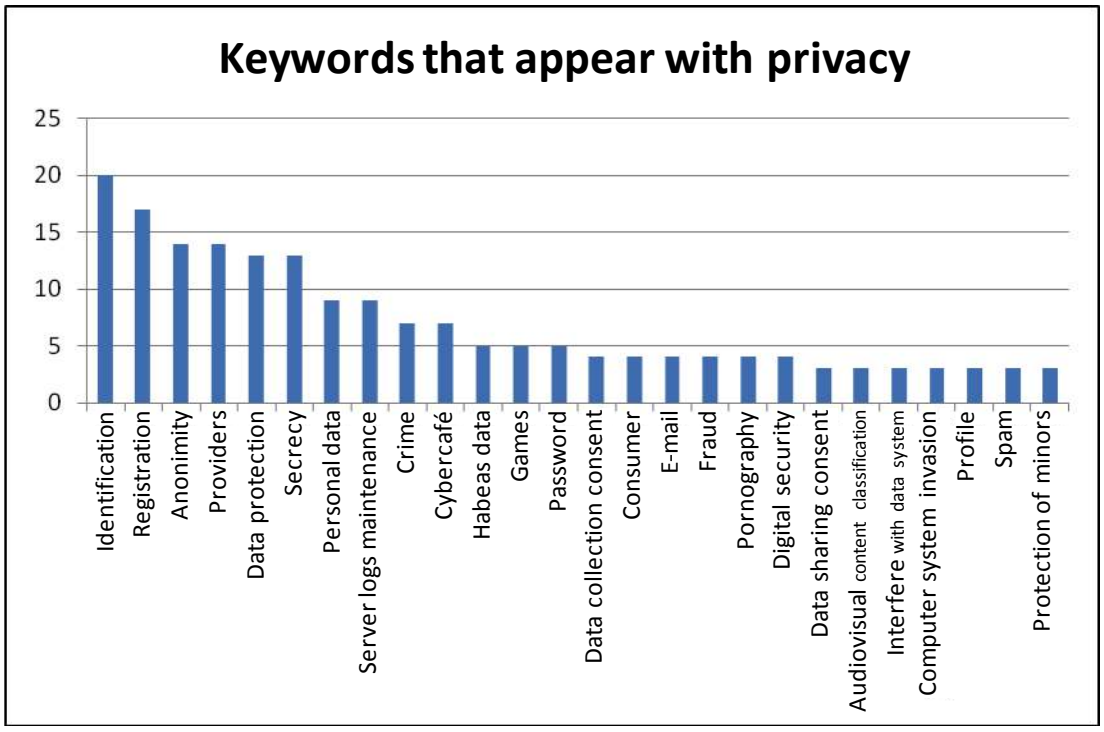
The fight against spam is the fourth most frequent objective/justification and is included in 10% of the bills. In addition to spam, the term opt-out was also recurring, both appearing in 9% of the bills/laws analyzed. Often, these bills are related to the intent of impeding the distribution of viruses and malicious programs and, consequently, avoiding crime. In some cases, concern is expressed with regard to user privacy and the methods of obtaining their e-mail addresses.

- **Protection of personal data and privacy: a "minor" concern**

The number of bills/laws whose principal objective was to guarantee the principles of data protection and privacy was 5%. Issues such as user consent for the collection/processing/distribution of data were mentioned in 6%, 2% and 5%, respectively, of the bills and laws analyzed. Notification for data collection appeared in 2% and the right to consent to, be aware of and/or correct the information stored in these databases was mentioned in 4%. In general, these bills also included the defense of the inviolability of electronic communications (except with a court order) and the protection of delicate information, such as sexual orientation, religion, political views, heath information, among others.

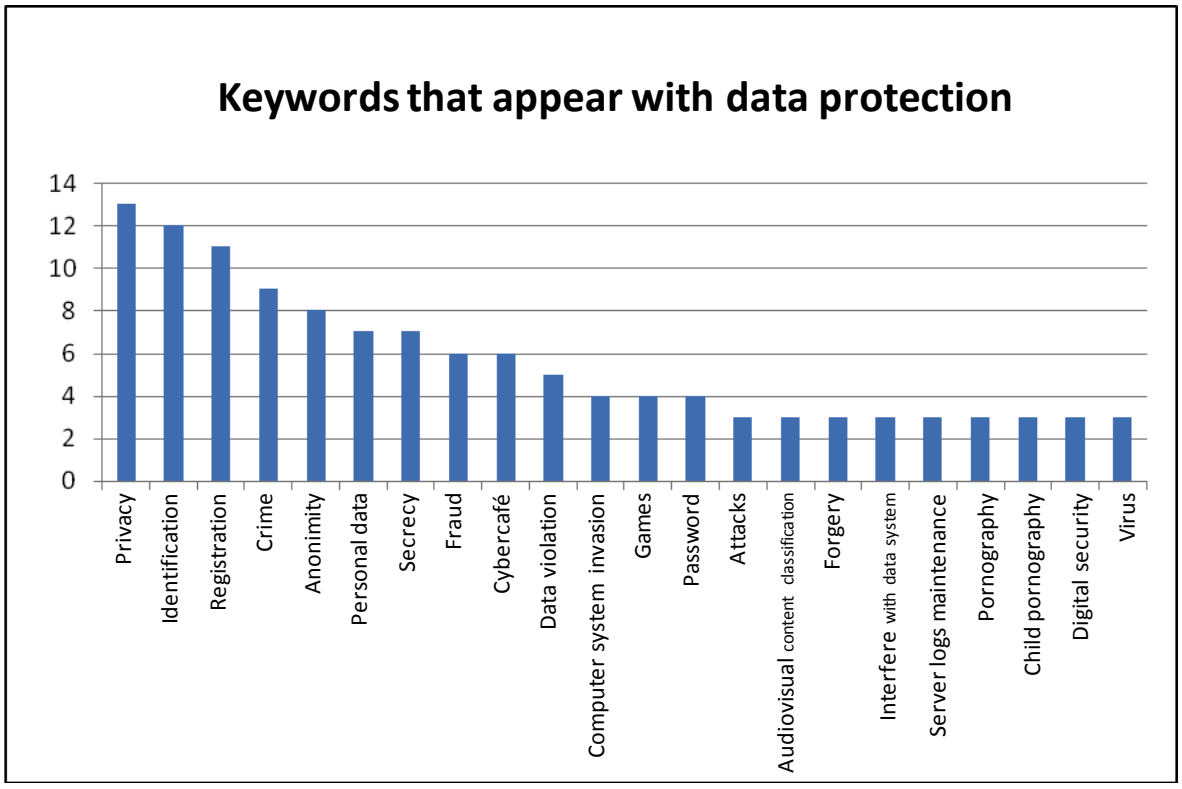
When we consider the bills that do address the issue of privacy but do not have it as their main purpose, the index of recurrence increases to 26%. In these cases, the guarantee of privacy often appears in bills focused on prohibiting anonymity, indentifying the need for a record and the link of such record to data protection. Graph 17 shows the distribution of the elements that appeared the most often along with the term privacy:

Graph 17: keywords linked to privacy



The context of the bills linked to data protection is in turn related to privacy and the sphere of crime (and, consequently, the relationship between anonymity and registration practices) and data security. Graph 18 shows the frequency of the items that appear in relation to this term. The presence of terms such as fraud, invasion, passwords, attacks, data system interference and viruses can be observed:

Graph 18: Keywords linked to data protection



In many cases, the only idea associated with the protection of personal data presented in the projects analyzed was to make the party required to keep the record responsible for maintaining an access log and/or storing messages and keeping them confidential, seeking to ensure the privacy of the users. Although these bills address the need for governing the formation of the databases kept, in many cases, by service providers, their purpose, in most cases, is to prevent crimes carried out through the Internet. This situation was observed in 22% of the bills/laws analyzed. In addition, it is important to mention the problems of considering this regulation to be sufficient to ensure the privacy of the users and the right to freedom of expression on the Internet.

- **Conflicting context: Civil framework of the Internet and the law for the protection of personal data**

At the federal level, two bills open to public consultation by the Ministry of Justice stand out due to their relevance and their conflict with this dominant context. One of these is the Civil Framework for the Internet in Brazil, which attempts to establish legislation that determines the rights and responsibilities for the use of digital means, with a focus on guaranteeing the rights and not restricting freedoms. The bill presented to society for discussion by the Ministry of Legislative Affairs of the Ministry of Justice, in cooperation with the Rio de Janeiro School of Law of the

Gegulio Vargas Foundation, received more than two thousand contributions during the period of public consultation on the issue. It was sent to National Congress on August 24, 2011 and will now be discussed by the Chamber of Deputies and the Federal Senate.

The bill inverts the trend of proposals for criminalization initiatives and attempts to first define a set of rights rather than prioritizing efforts for criminal classification. This bill defines the responsibilities and rights for users and access providers and seeks to ensure online privacy and freedom of expression. It also establishes that the safeguarding of the records of access to Internet services shall depend on the authorization of the user, as well as respect for standards and guidelines related to the protection of personal data. This means that the user must be clearly informed of the reason for the registration of his/her data. It also seeks to establish that practices involving the treatment, distribution and access of third parties to their data shall depend on their authorization. The bill also guarantees users the right to access and correct their information and that their identification shall only be related to the records kept through court authorization, which doubtlessly is a significant evolution from the PL Azerdo and other similar bills.

Another relevant and central initiative for this report, which is also open to public consultation, seeks to create a law for the protection of personal data in the country. The bill on the issue was also proposed by the Ministry of Justice, this time in cooperation with the Brazilian Observatory of Digital Policies of the Technology and Society Center of the Getulio Vargas Foundation of Rio de Janeiro. It seeks to establish the right to privacy guaranteed in the country's constitution, and the proposal is primarily focused on the recent scenario of proliferation of personal data on digital communication networks, as well as the ease with which this information can be accessed, distributed and used. In this context, the bill defends the position that the use of this information should be defined based on the choices of the owner of such and not based on the will of those who access and/or store such data. To guarantee its operation, it establishes the creation of a Guarantee Authority responsible for, among other aspects, the tax application of the law, and the application of sanctions and dialogue with the various sectors of society.

The bill defines "personal data" as "any information related to an individual who is either identified or identifiable, whether directly or indirectly, including the addresses or identification numbers of a terminal used to connect to a computer network". It establishes that individuals must be informed that their data is being collected at the time this occurs and that it cannot be used without the prior authorization of the owner of such. The bill also establishes that users must be informed of the possible consequences of their refusal to allow the use of their data and seeks to establish conditions for this to occur in a precise and legal manner, in good faith, within the purposes foreseen. The owner of the information is guaranteed the right to review, correct or cancel such information and, similarly, he/she is guaranteed the right to not be subjected to decisions affecting him/her in a significant manner made merely as a result of the automated treatment of personal data for purposes

of defining his/her profile or personality. In this point, the bill even establishes that citizens can request an explanation of the parameters used in decisions of this kind.

ii. Academic studies

General Objective:

Perform a preliminary mapping of the academic production related to the problem of personal data on the Internet in Brazil

Specific Objectives:

a) Identify researchers on the issue in Brazil, as well as the institutions to which they belong.

b) Identify the development, by year, of the academic production on the issue.

c) Identify the issues related to the problem of the treatment and regulation of personal data on the Internet in Brazilian academic production

Databases consulted:

a) Capes Publications Portal

b) Redalyc

Methodology:

In order to build a panorama of academic and scientific production related to the protection of personal data on the Internet in Brazil, we analyzed 56 national journals included in the Capes Publications Portal and the Latin America Redalyc Index. In each of these databases, we searched for the following keywords, analyzing the results obtained and registering the pertinent articles:

- Data protection + Internet
- Personal data + Internet
- Surveillance + Internet
- Monitoring + Internet
- Privacy + Internet
- Freedom of expression + Internet
- Copyright

- Copyright + Internet
- Cybercrimes
- Digital crimes
- Digital security
- Data security + Internet
- Regulation + Internet

The searches were performed from February to April. In the Capes Portal, the search was restricted to the national publications aimed at the following areas: Law, Communication, Information Science and Computer Science. In Redalyc, the search was performed for the keywords in Portuguese and in Spanish and the content considered included both articles by national researchers and those by foreign researchers on the context of Brazil.

In the cases in which the publication site did not have a search function, the analysis was performed manually, except in certain rare cases where the volume of articles was extremely high. Before performing the search, we evaluated the operation of the search function, opting to use only the word Internet in the cases in which the use of specific terms did not bring back any results.

Basic data was stored on the articles considered to be pertinent and their authors. In this stage, the articles were also evaluated with regard to their link to the issue (A for those most related to the issue and B for those less related). At the end, all of the material recorded passed through a process of classification by subject, which was automated due to the very large number of articles.

To show the subjects that were addressed the most, we created a dictionary of 201 terms based on the manual analysis of the body of 50 articles. Later, a script was produced that searched for each of the terms in all of the articles and recorded the number of times they appeared. Finally, each article was classified based on the elements that appeared three or more times, ordered by relevance (from the one that occurred the most to the one that occurred the least).

Results:

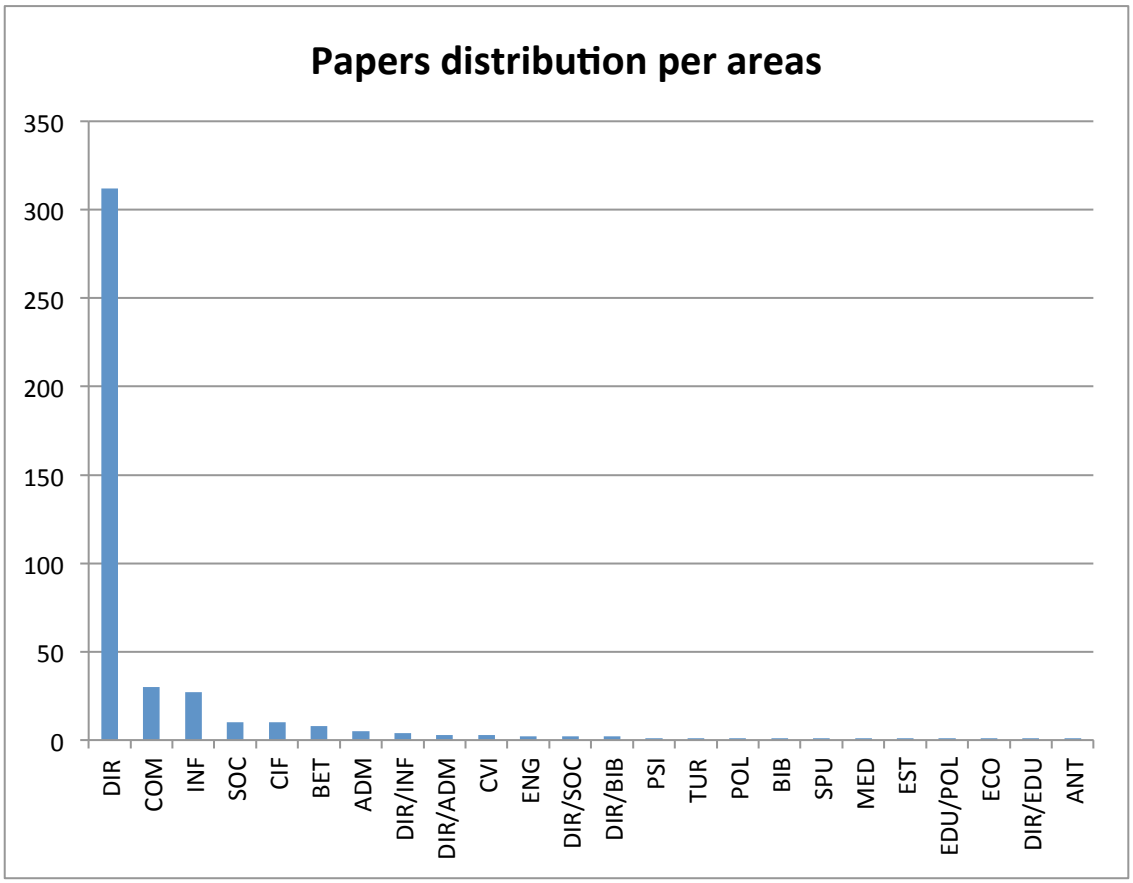
a) General Information

The searches performed resulted in a total of 5,358 articles. Of these, 429 were related to the issue, with 342 having an A-level relationship and 87 having a B-level relationship.

The data collected shows an obvious prominence of discussions on the area of Law: 73% of the articles found belong to this area of knowledge. The next most prominent was the area of Communication, with 7%, followed by Computer Sciences with 6%. Sociology, Information

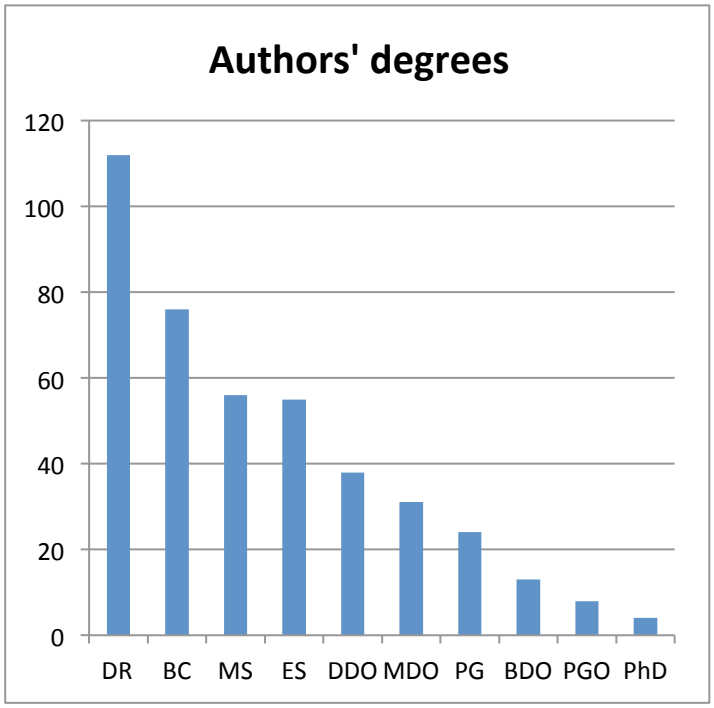
Sciences and Bioethics appeared lower in the ranking with 2% each. Graph 19 shows the distribution of the number of articles by area of knowledge.

Graph 19: Distribution of articles by area of knowledge



With regard to the academic level of the authors, we observed that most of them have Doctorates. Next are those with Bachelor's degrees, with 32% less. The number of authors with Master's degrees and specializations did not vary significantly. Most of the authors are from the area of Law, followed by researchers from the areas of Information Sciences, Engineering and Communication. Graph 20 shows the distribution of authors by their degrees:

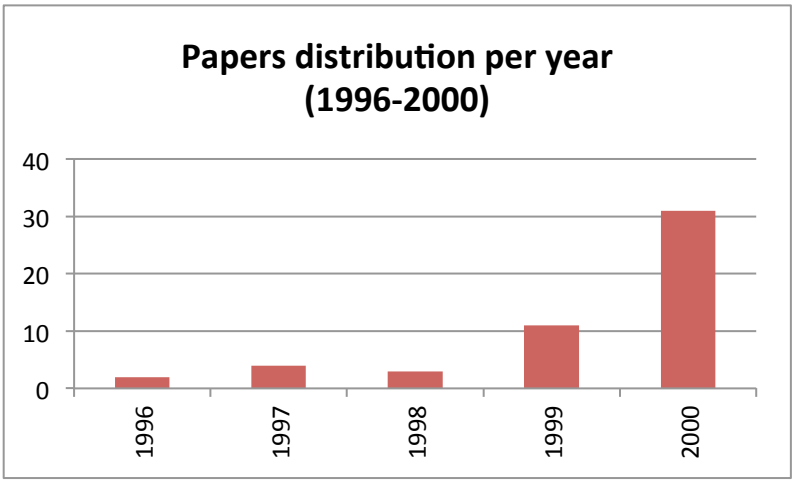
Graph 20: Level of education of the authors



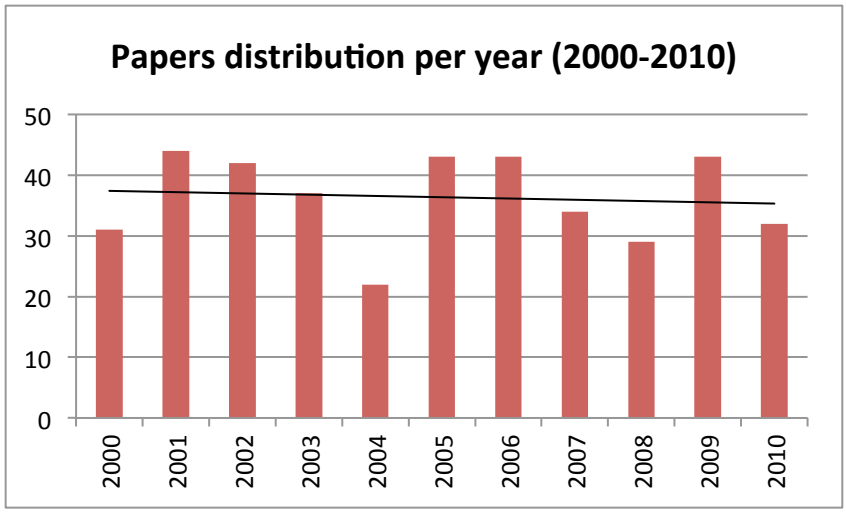
The publication that had the most results on the issue was Jus Navegandi, a legal publication, where we found 252 articles. It is important to highlight that the public site also includes content that is not strictly academic, with the character of opinions, and scientific articles in the standard format, which contributes to the significant number of results observed.

With regard to the distribution of articles over a timeline, we verified that the first works on the subject began to appear in 1996. The number of articles remained practically stable until 1998, as of which time we observed a trend of rapid and marked growth that extends until 2000. As of this date, the number of articles related to this issue stabilized at a new level, which was maintained throughout the entire decade of 2000. Graphs 21 and 22 show the number of studies per year. It can be observed in graph 22, which covers the past decade, that the trend, adjusted to recognize the least square method, is a line parallel to the axis, which represents the stabilization of the number of annual research projects.

Graph 21: Distribution articles/year (1996-2000)



Graph 22: Distribution articles/year (2000-2010)



b) Players

The following players were identified in the academic production on the subject of the treatment and regulation of information on the Internet in Brazil:

- Researchers (mostly with Doctorates, as can be seen in Graph 20). This can also be observed in the graph of authors who stand out in the journals as having produced the most articles.
- Research and learning institutions
- Vehicles of academic publication. A classification of the publications by the number of articles on the issue can be seen in Graph 23.

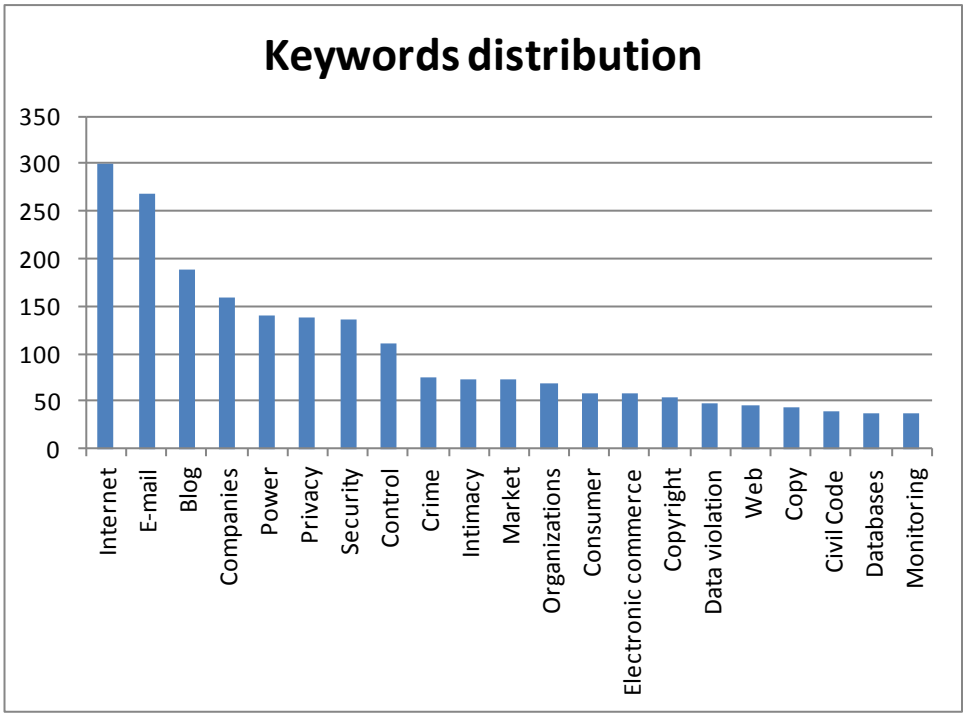
Graph 23: Publications and authors

c) Trends

- Recurrence and relationship between subjects

The analysis of the most frequent indicators show a law of potential, which indicates that a few subjects appeared many times and many varied subjects had a very low level of recurrence: they appeared very few times. See graph 21 below with the most frequent aspects. The term Internet appeared 300 times and leads the list, followed by the terms e-mail (269), blog (189), companies (160), power (141), privacy (138), security (135), control (110), crime (74), market (72) and intimacy (72). It is important to highlight the recurrence of the terms “copyright” and “copy” and the pair of terms of “data violation” and “monitoring”, which are associated with the field of security, appear in the top 20 terms of the classification. This analysis considered as keywords the dictionary words that appeared at least five times in a specific article.

Graph 24: frequency of indicators by article



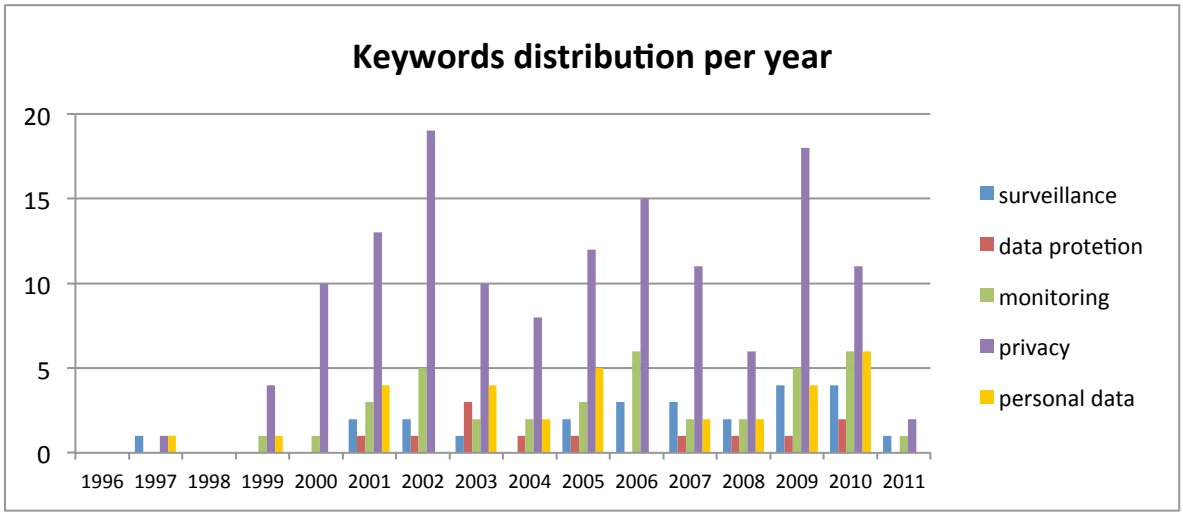
The recurrence of the indicators by area of knowledge shows that in the Legal field, the discussions regarding the issues of “privacy” and “intimacy” are more common than in other areas of knowledge. The term “surveillance” was the most frequent in the Communication and Sociology works, while in the security field, which was ranked fifth in the classification of the areas of Law, Information and Sociology, was the least recurring in Information Sciences and Communication. These last two areas include more discussions on intelligent agents and personalization, while Law more frequently addressed the issue of copyrights. In Bioethics, the issues of health, violation of information, biopower and discrimination were more frequent that in the other areas.

It was also possible to identify, in the journals with the highest number of pertinent articles, the most frequent subjects, as shown in graph 25.

Graph 25: Keywords by journal

Finally, we observed the distribution of the number of articles that contain the keywords "surveillance", "data protection", "monitoring", "privacy" and "personal data". There was no significant variance over the years and the same curve of distribution tended to reproduce itself in the articles over the timeline. In general, the dominance of the term "privacy" maintained strong, as well as the comparatively lower frequency with which the terms "surveillance", "personal data" and "data protection" occurred.

Graph 26: Distribution of keywords by year



iii. Events

General Objective:

Investigate events related to the regulation/protection of personal data on the Internet in Brazil.

Specific Objectives:

a) Identify the type and year of the event

b) Identify the organizing institutions

c) Identify the principal issues discussed

Databases consulted:

Electronic sites for news and organizations

Methodology:

We researched at the electronic sites of organizations and electronic news sites, events related to the regulation and protection of personal data on the Internet in Brazil. The pertinent results were registered in a table that contains: the name of the event, the date it was held, the organizing institutions, type (workshop, seminar, etc) and the issues discussed. The searches were performed in the months from October to December 2010.

Results:

a) General Information

A total of 22 events were identified that were held in 2009 and 2010 in the format of seminars, debates, conferences and meetings (Exhibit V). With regard to the most relevant issues, four events were focused on the central issue of the protection of personal data, three of which were organized by government ministries (Public Ministry and Ministry of Justice), in cooperation with the UERJ, FGV, and the Internet Management Committee of Brazil, and one by the Latin American Network Habeas Data. The issue of the establishment of the civil framework of the Internet in Brazil also stands out as a priority at six events, two of which were organized by the International Free Software Forum – PUC RS, and the other four events on the civil framework were organized by the Instituto CONIP, the ALERJ, the Ministry of Justice and FGV and by the FEDERASUL. The Latin American context consisted of five events and the specific Brazilian context consisted of 9 events.

b) Players

The following relevant players were identified among the organizing institutions of the events:

- Ministries: Ministry of Justice and Federal Public Ministry
- Academic research institutions: FGV, National School of Consumer Defense, UERJ, Unibrasil, UFSC, PUC RS, FAPEAL, University Blas Pascal, PUC PR
- Federations: FEBRABAN, FECOMERCIO, FEDERASUL
- Associations, Councils, NGOs, Networks: Carta Maior, International Free Software Forum, OAB-SP, Institute CONIP, ALERJ, Brazilian Association of Computer and Telecommunications Law, Latin American Network of Habeas Data, SEBRAE/AL.
- Companies: OWASP, Now Digital

c) Trends

It is important to note the investment made by the Brazilian government (through the Public Ministry and the Ministry of Justice) in the last five years in the promotion of events in cooperation with civil society with the objective of discussion regulatory civil frameworks with direct implications on the treatment of personal data in the country, specifically taking into account the digital networks of distributed communication like the Internet. This trend is corroborated by the presence of the two referred ministries among the most recurring organizers of events related to the protection of personal data.

iv. Institutions and Government

General Objective: Identify the institutions and organizations with programs and practices that have implications for the treatment, regulation and/or governance of personal data on the Internet in Brazil.

Specific Objectives:

a) Map the areas of action of the institutions identified

b) Identify, in the environment of the institutions identified, the recent practices and actions so as to pinpoint their implications for the treatment and regulation of personal data on the Internet in Brazil.

Databases consulted:

Journalism sites, news sites and sites of organizations.

Methodology:

The databases mentioned above were used to research information, documentation and materials that allowed for the identification of national institutions and organizations with programs and practices that have implications for the treatment and regulation of personal data on the Internet in Brazil. The pertinent results were recorded in a table for subsequent analysis, using the following categories: name of the institution and/or organization, area of action, practices, recent actions and link to the website of the institution and/or organization. The searches were performed in the months from October to December 2010.

Results:

a) General Description:
Four relevant institutions were identified with regard to the treatment, regulation and/or governance of personal data on the Internet in Brazil: Civil Framework Observatory; Digital Culture Program; Internet Management Committee; Public Debate on the Protection of Personal Data (Exhibitive).

b) Players
The players identified consist basically of the institutions identified:

- Civil Framework Observatory;
- Digital Culture Program;
- Internet Management Committee;
- Public Debate on the Protection of Personal Data

It is important to point out that these institutions are characterized as having a "hybrid" composition that involves government bodies, non-government corporations, technological devices and the participation of civil society. This composition could be seen in the practices of these institutions, as described in Exhibit VI.

c) Trends
Based on that established in the previous point, we perceived that the institutions identified had a composition of a hybrid nature that sought to link different players (governmental, non-governmental, technological and civil) in the discussion on digital networks of distributed communication and their impact on Brazilian society. All of the institutions identified strongly encourage the participation of civil society in this debate, using as one of the key tools the Internet itself. The issue of the treatment of personal data on the Internet is focused on most directly by the Public Debate on the Protection of Personal Data, which maintains a clear position of promoting regulatory frameworks for the protection of personal data. The question of personal data on the Internet is also present in the other three institutions, in these cases as linked to the broader contexts of regulation and governance of the Internet and the practices that characterize the digital culture.

v. Civil society movements, actions and organizations

General Objective: Identify the movements, actions and organizations whose practices contribute to the promotion of public debate and the participation of society in the reflection on the treatment and regulation of personal data on the Internet in Brazil.

Specific Objectives:

a) Map the areas of action of the movements and organizations identified

b) Identify the recent practices and actions with implications for the promotion of public debate and the participation of society in the reflection on the treatment and regulation of personal data on the Internet in Brazil.

Databases consulted:

Websites for newspapers with national coverage, news sites and sites of organizations.

Methodology:

The referred databases were consulted for information, documents and materials that allowed for the identification of national movements and organizations with practices that have implications for the participation of civil society in the public debate on the treatment and regulation of personal data on the Internet in Brazil. The pertinent results were recorded in a table for subsequent analysis, using the following categories: name of the movement and/or organization, area of action, practices, recent actions and link to the website of the movement and/or organization. The searches were performed in the months from October to December 2010.

Results:

a) General Description:

Nine civil society movements and organizations were identified whose practices and actions favored, to a lesser or greater degree, the participation of Brazilian society in the public debate on the regulation and treatment of personal data on the Internet. (EXHIBIT VII). These movements and organizations are distributed among different areas of action: human rights, consumer rights, right to communication, production of knowledge and innovation in communication technologies, political activism on the Internet, defense of freedom of expression on the Internet, protection of personal data and defense of the right of privacy on digital communication networks.

b) Players:

The following players were identified:

- Habeasdata
- Pirate Party
- Consumer Forum
- Personal Data

- Instituto NUPEF (Nucleus of Research, Studies and Formation)
- Intervozes
- Instituto CONIP (IT Knowledge, Innovation and Practices in Public Administration)
- Mega Não
- Cyberactivism

The areas of action and recent practices of each player can be seen in Exhibit VII

c) Trends

Although the number of relevant actors in Brazilian civil society is small, we noted their progressive growth in recent years. We also noted that the issue of regulation and the treatment of personal data on the Internet, when it is not the direct aim (as in the case of the Habeas Data organization, that acts in favor of a policy of protection of this data), goes hand in hand with the debate of militancy in the sense of guaranteeing fundamental rights (privacy, freedom of expression, among others), in the context of digital networks of distributed communication.

vi. Technologies

General Objective:

Identify the principal technologies used to capture, treat or protect personal data on the Internet. These technologies are usually called trackers.

Specific Objectives:

a) Trace and identify the three principal mechanisms for monitoring and capturing personal data (cookies, flash cookies and web beacons) in use in five of the 15 most accessed sites in Brazil and the two most popular Internet social networks in Brazil

b) Identify the function of the cookies and beacons used and classify them by type, measuring the variety of different types present on the social networks and sites analyzed

c) Identify the companies responsible for the cookies and web beacons used on the social networks and sites listed, as well as their principal practices

d) Analyze the privacy policies of the social networks and sites listed to verify the level of transparency with regard to the use of the identified mechanisms for collecting and monitoring personal data

Databases consulted:

a) Five sites included in the 15 most accessed sited by Brazilians: Terra, UOL, Globo.com, Yahoo.com and YouTube[50].
b) Two of the most popular social networking sites in Brazil: Orkut and Facebook[51] .

Methodology:
In the investigation of the sites, we identified and analyzed the HTML cookies, Flash cookies[52] and beacons[53] present in four portals (Terra, UOL, Globo.com and Yahoo.com) and a video sharing site (YouTube). This research was complemented by the analysis of the privacy policies of these sites to observe whether they correspond to the practices and technologies used, as well as the level of transparency of the information provided to the user with regard to these practices and technologies.

With regard to social networking sites, an extraordinarily popular phenomenon in the country, we identified and analyzed the html cookies and web beacons associated with the five most used applications in Orkut and Facebook[54]. This selection was based on the popularity ratings offered by the sites themselves. In this way, the use of the applications by all users and not only the Brazilian public was taken into consideration.[55]

[50] Based on the Alexa classification, available at http://www.alexa.com/topsites/countries/BR. This measurement is performed based on the combination of the daily average number of visitors and the number of viewings throughout the past month.

[51] The use of social networks in the country is specific to Brazil in the Latin American context. It began with the popularity of Orkut, launched by Google in 2004. The Portuguese version of the site became available in 2005 and its operations were transferred from California to Brazil in 2008 due to the massive adhesion to the site in the country. Today, Brazilians represent 50.6% of the site's users, according to data provided by Orkut itself (available at http://www.orkut.com/MembersAll). It is visited by 73% of the active Internet users in the country at March 2010, according to data from IbopeNetRating (Rodrigues: 2010, online).
The growth of Facebook in the country is a more recent phenomenon that accelerated in 2009. From August 2009 to August 2010, the site grew from 1.5 million visitors to 9 million, according to data from comScore. Nevertheless, Orkut continues to be more popular. In August 2010, for example, Orkut received 29,411 million visitors and Facebook received 8,887 million visits. In the month analyzed, 36,059 million users over 15 years old visited a social networking site in the country.

[52] Cookies are small files saves on the user's computer. They can be sent by the site seen or by third party servers and they allow an identifier to be assigned to a user. This information is saved on the user's computer and it can be used to monitor the user's navigation and obtain data on the access made, such as the IP address, operating system used, etc.
Flash cookies work in the same manner as html cookies but they can only be used with flash applications. The management and identification of these files by users is less transparent than for html cookies and is carried out through the user's own browser and with an open un-owned protocol.

[53] Web beacons allow for user monitoring without locating a file on the browser, as cookies do, which decreases the user's level of control and makes tracking more complex. Although they also use a request from a server to send a file, this technique does not save an identifier on the user's computer. Rather, the monitoring is performed through the complementation of the variables of the subsequent requests for this file. An example of this technique is the use of web bugs; i.e., one pixel images that are transparent, and therefore invisible, that are used for tracking.

[54] As the users of social networks are identified through a registration system, the companies that offer these services do not need to use trackers to gather personal data or a user profile. Therefore, we focused on the analysis of the social applications developed by the associated companies that operate in these platforms, the use of which does not require a specific session to be initiated.

[55] Orkut and Facebook measure the popularity of their applications by types or categories. For our analysis, we considered the first place of the five most-visited categories. The analyzed applications were: Orkut - Secretos del Mar, Buddy Poke, Feliz cosecha, Baby Adopter and Música; in Facebook - Causas, Texas Hold'em, frases, Badoo, and Quiz Planet.

The methodology for identification and analysis of the trackers, inspired by a measurement of the use of trackers on U.S. sites performed by The Wall Street Journal (Valentino-Devries. 2010, online), consisted of visiting the analyzed sites and reviewing the cookies registered in the browser before and after each visit. In each site, nearly 30 pages were visited randomly in an attempt to diversify the navigation, taking care to avoid access to external links[56].

The flash cookies were analyzed in a similar manner, using the Website Storage Settings Panel, a mechanism of Adobe that makes it possible to see this type of tracker[57]. For the analysis of the web beacons, we had the assistance of the Ghostery[58] software, which identified the company responsible for the tracker. In the case of the cookies (html and flash), we used the domain used to host the tracker for this identification.

The searchers were performed in the months from January to March 2010. The last stage of the investigation consisted of analyzing in the site of the companies responsible for the trackers found, the privacy policies, opt-out mechanisms and information provided to the users on the services offered and the personal data capturing technologies used. Based on this data, the cookies and beacons were classified to show the trends, practices and predominant players.

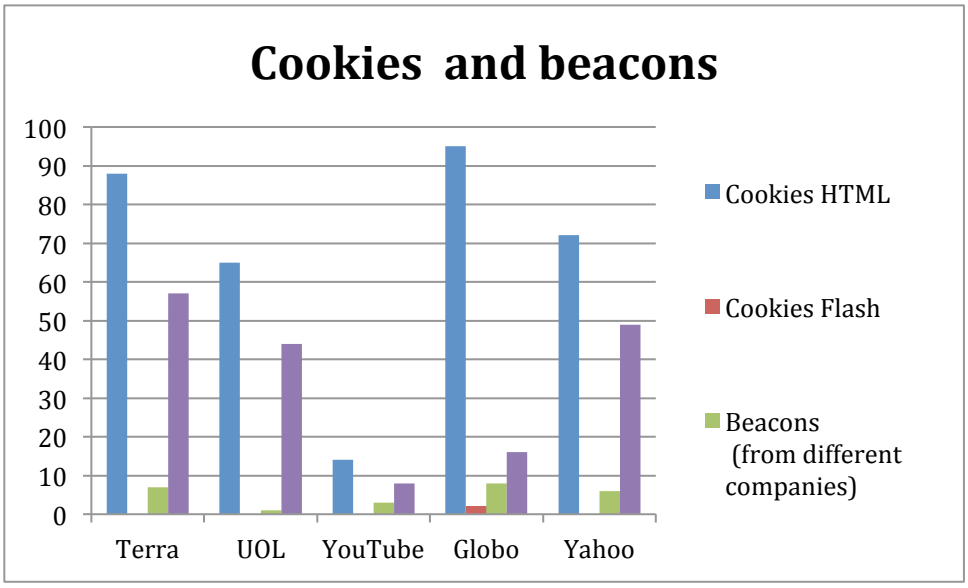
Results:

a) General Information

A total of 334 html cookie files were found in the five sites analyzed, of which 174 were from third party servers. Considering only the non-repeated cookies, there are 53. We identified only 2 flash cookies, placed by the site visited itself, and 25 web beacons, excluding the repetitions. Graph 27 shows the distribution of these trackers by site analyzed.

[56] We surfed without logging in, since this procedure would identify the user for the company and open up the possibility of other forms of user monitoring being used.
[57] Available at http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html.
[58] The software is an expansion available for the primary browsers on the market that identifies web beacons and the companies responsible for them. Available at http://www.ghostery.com/.

Graph 27: cookies and beacons by site analyzed



We observed that the Terra, UOL and Yahoo sites use, on average, 3.2 times more cookies from external servers than the Globo.com portal and YouTube. With regard to the number of beacons, UOL and YouTube are the sites where this technique is the least used (one and three times, respectively), while Yahoo, Terra and Globo.com had six, seven, and eight beacons, respectively.

With the exception of UOL, the five sites analyzed indicated the possibility that third parties could use trackers on their site. UOL had the most simplified privacy policy and was the only one that did not speak of the relationship between cookies and advertising and service personalization. It also stated that its cookies are not used to control the preferences of its Internet users, although it did admit their use for internal control of navigation. UOL and Globo.com were the only ones that did not directly refer to the use of web beacons.

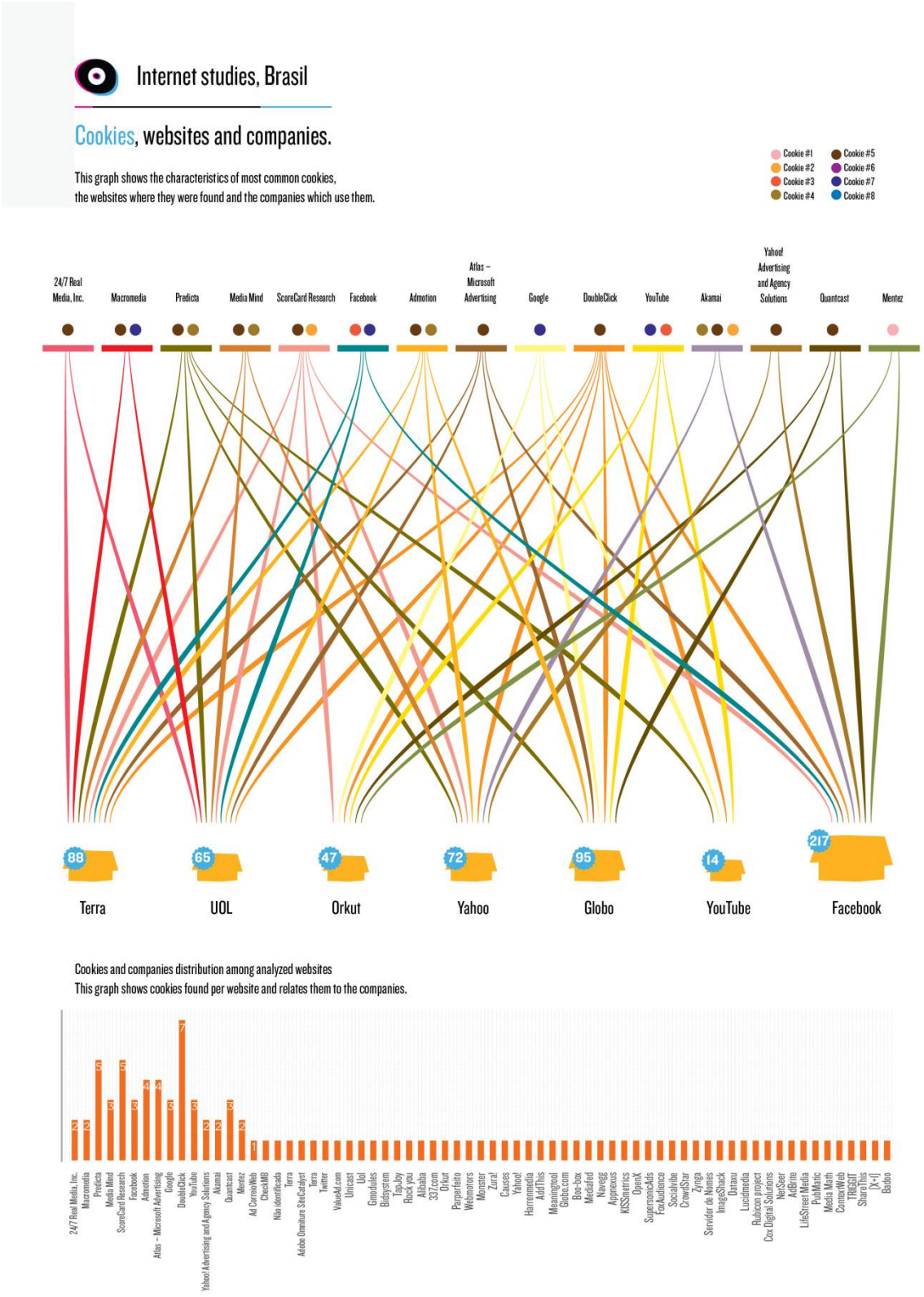
In the two social networks analyzed, we found a significant disparity in the number of html cookies found; In Orkut, the analysis of five of the most popular applications gave back 47 cookies, while in Facebook we found 217. Considering only non-repeated cookies, these numbers drop to 13 and 38, respectively. The number of web beacons, however, did not very significantly: there were 18 unrepeated trackers of this kind on Orkut and 15 on Facebook.

We identified 69 companies, domestic and foreign, responsible for the cookies found on the seven sites analyzed. In the case of the web beacons, there are 23 companies. The most recurring cookie[59] and the second most recurring beacon are from the company DoubleClick, a subsidiary of Google specialized in providing advertisements and giving support in the administration of advertising campaigns. Two other services of the company are high on the list: the beacon of Google Analytics was the most recurring and the Google AdSense was ranked third on the list.

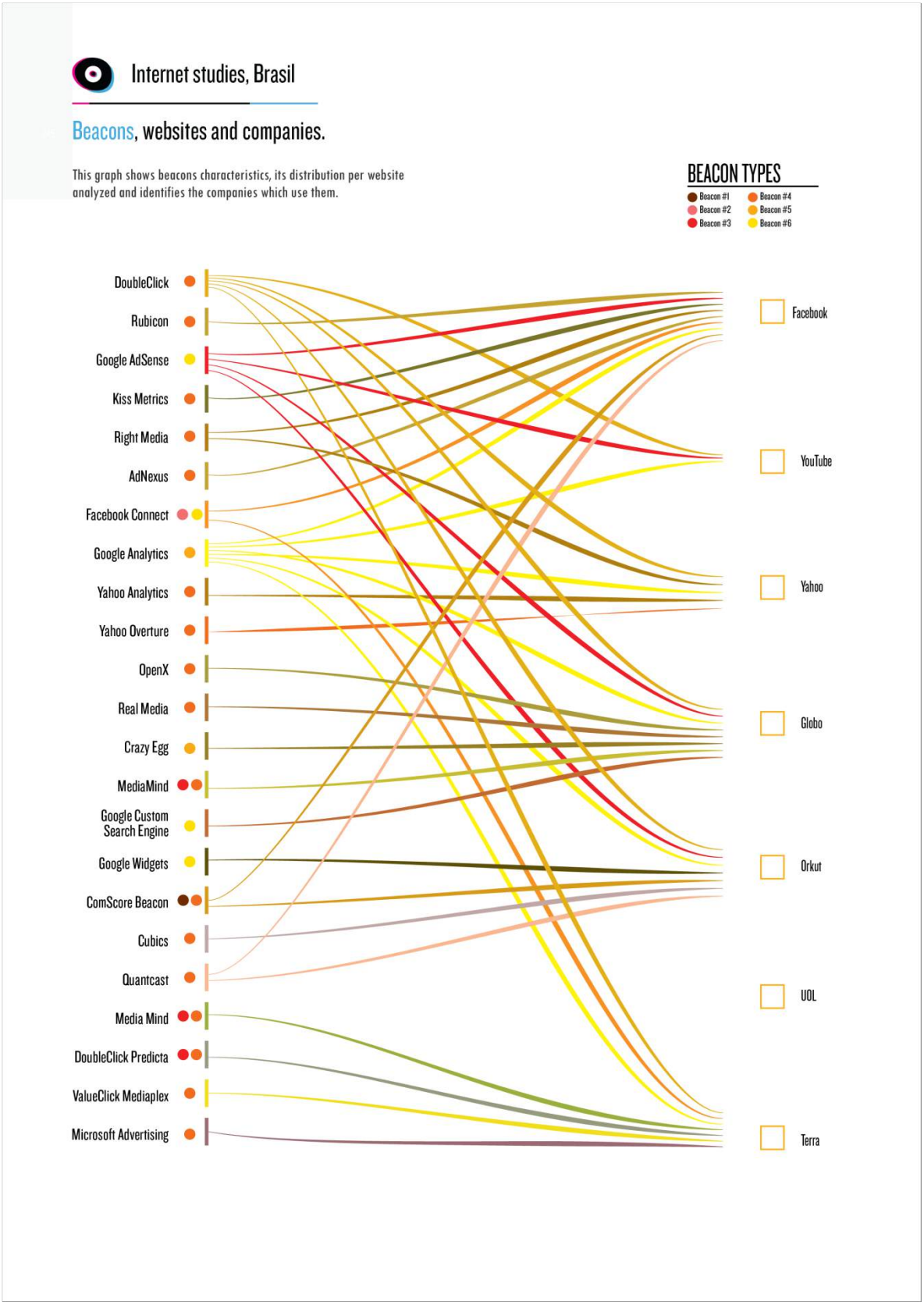
Graphs 28 and 29 show the number of cookies and beacons found on all of the sites analyzed and the companies that produced them.

[59] The classification of recurrence was performed based on the number of sites at which the cookie or beacon appeared in the seven sites analyzed (Globo.com, YouTube, Terra, Yahoo, Uol, Orkut and Facebook) and not the total number of times the tracker in question appeared. The complete list is available in Exhibit VIII.

Graph 28: Cookies, websites and companies



Graph 29: Beacons, websites and companies



b) Players

- Companies responsible for producing and supplying the cookies and beacons
- Sites that host and use the cookies and beacons
- Different types of cookies and beacons that involve different practices for the use and operation of personal data
- Advertising companies contracted by third parties
- Opt-out mechanisms
- Organizations, corporations and/or agreements aimed at reconciling commercial interests and respecting the privacy of the consumer and/or user. These players provide stamps and/or certificates that indicate the respect of the codes of conduct by the companies, usually with regard to the treatment of personal data.
- Internet browsers, which allow a certain level of visibility for the use of cookies and options to deactivate them
- Internet user[60]

c) Trends observed

- In search of more clicks: The dispute for the attention of Internet users

62% of the companies responsible for the cookies found and 68% of those responsible for the web beacons offer technologies for the publication of advertisements and their business is to promote the monitoring, analysis and optimization of advertisements or social applications.

- Monitoring: In a market full of options

In only seven sites, we identified a significant number of companies. Of the 69 that operate cookies and the 23 that operate beacons we found, respectively, 45 and 19 companies whose business is closely associated with Internet monitoring practices. These companies offer services such as audience measurement, provision of usage maps, access analysis and navigation flow and services related to marketing, as described above.

- Predicta, Navegg, Zura! and Boo-Box: Domestic companies

Of the companies identified, we found four domestic companies: Predicata, Navegg, Zura! and Boo-Box. The first is responsible for the second most recurring cookie of all of those analyzed, present in five of the seven sites analyzed.

- Transparency: Concern is far from universal

[60] Although we did not analyze the practices of users with regard to these technologies, they are clearly present among the players identified.

The number of companies that made their identification difficult by using a name in the html beacon that was different from their own company name caught our attention. This practice was observed in 13% of the cookie operators and 12% of those responsible for the beacons.

- Social applications: A vulnerable point

The use of the two social networks analyzed without installing or accessing applications did not show an association with the use of third party trackers, which shows that, in these sites, the addition of applications implies not only allowing their developers to access information on the users' profiles, but also exposes them to the actions of a high number of trackers.

- Third party action: Handing off responsibility

In general, we verified that the analyzed sites allow companies contracted by third parties to distribute advertisements on their sites. In these cases, the users are subject to the privacy policies and practices of these companies, which makes it more complex and difficult for the Internet users to manage their privacy.

- Agreements and principles

Among the companies that operate beacons, 32% are members of the NAI (Network Advertising Initiative)[61] and 56% are certified by TRUSTe[62] or adhere to the Safe Harbor[63] agreement. Among the cookie operators, these numbers drop to 19% and 23%, respectively. These corporations and agreements seek to facilitate the respect of user privacy in the commercial and advertising relationships present on the Internet.

- Privacy policies and opt-out: Area of uncertainty

Among the cookie operating companies, 19% did not have a privacy policy on their website. For the beacon operators, this number drops to 4%. The possibility of opt-out was offered by 46% of the cookie operating companies. However, except in rare cases, we found that the opt-out for beacons is not explained clearly on the websites of the companies and privacy policies analyzed, which made it difficult to even measure this option to prepare this report. An important point is that, in many cases, the opt-out mechanisms offered by the companies consist of installing a cookie on the user's

[61] NAI is a council of companies that develops self-regulation standards for the online advertising industry. It offers opt-out for cookies of several of the companies analyzed through the site (http://www.networkadvertising.org/), but does not clearly indicate whether the opt-out also works for the beacons. This opt-out depends on the placement of a cookie of the company on the user's computer.

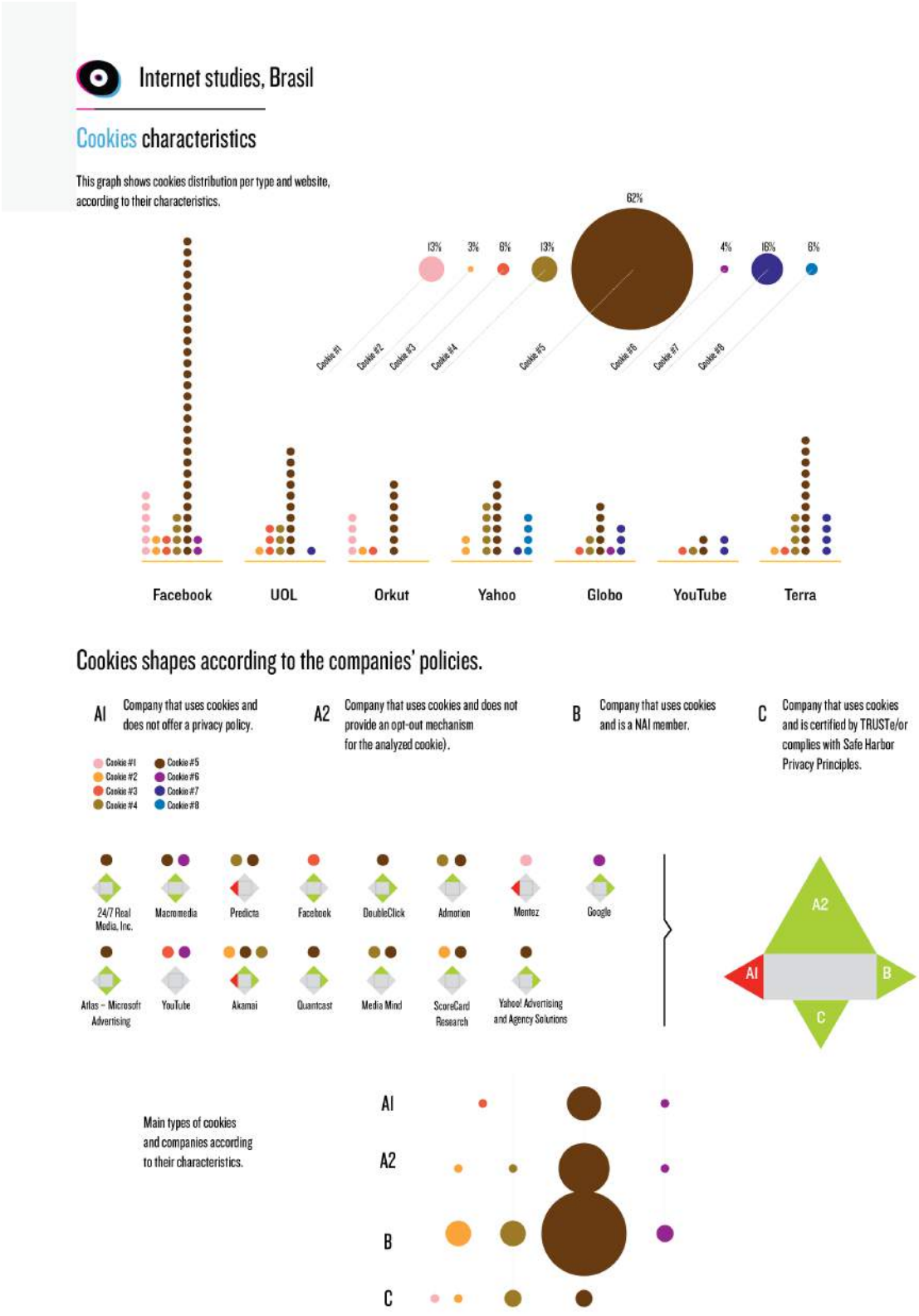
[62] TRUSTe is a company based in California (USA) that offers certification of privacy practices for companies and their websites. If a company is certified by TRUSTe, this does not imply compliance with standards such as EU Directive 95/46/EC but rather only that the company respects its own privacy policy.

[63] Adherence to Safe Harbor Privacy Principles allows American companies to show their respect and compliance with the data protection standards of the European Union (EU Directive 95/46/EC).

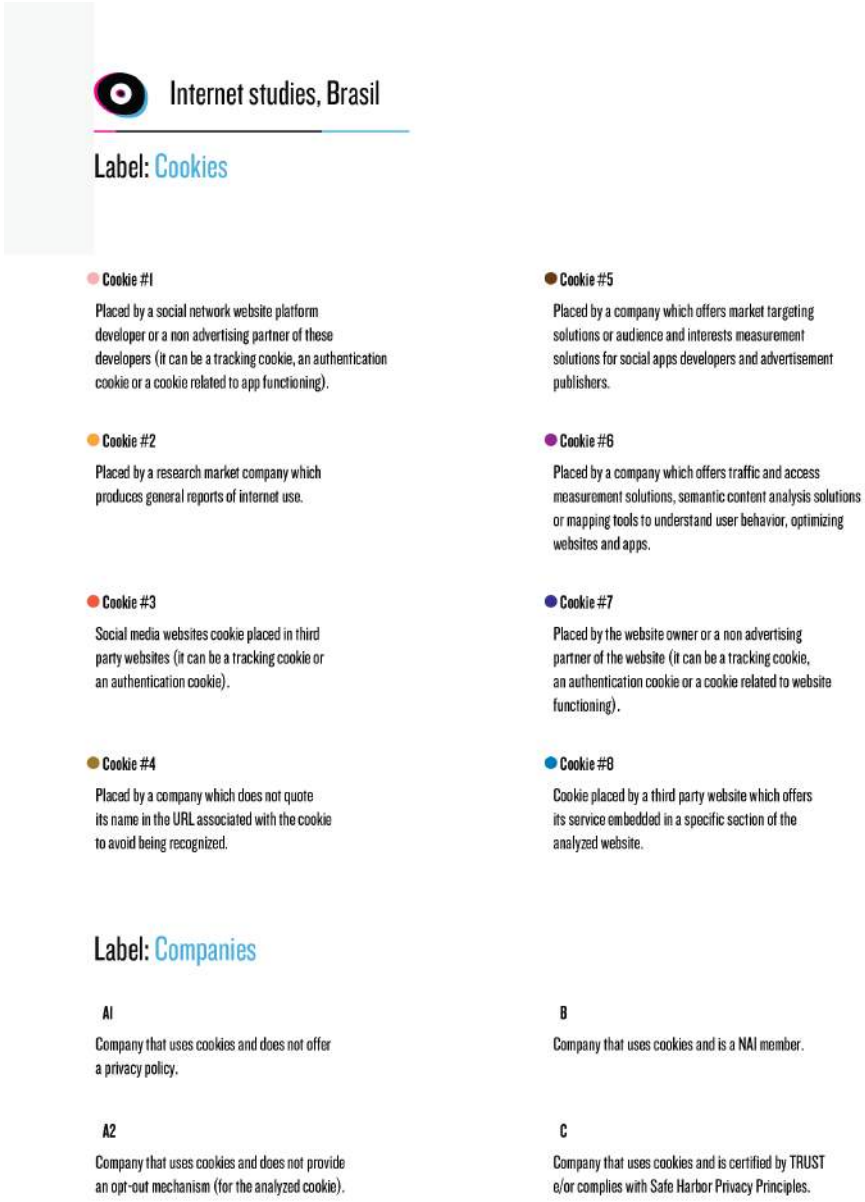
computer to indicate this option. We verified that this cookie often appears with the same identification as the tracking cookie for the Internet user. This uncertainty is accented by the fact that the opt-out option does not work if the user chooses to deactivate cookies on his/her browser.

Graphs 30, 31, 32 and 33 show the most-used types of cookies and beacons, classified based on their function and purposes, as well as the practices of the companies responsible for them with regard to the privacy of the Internet users.

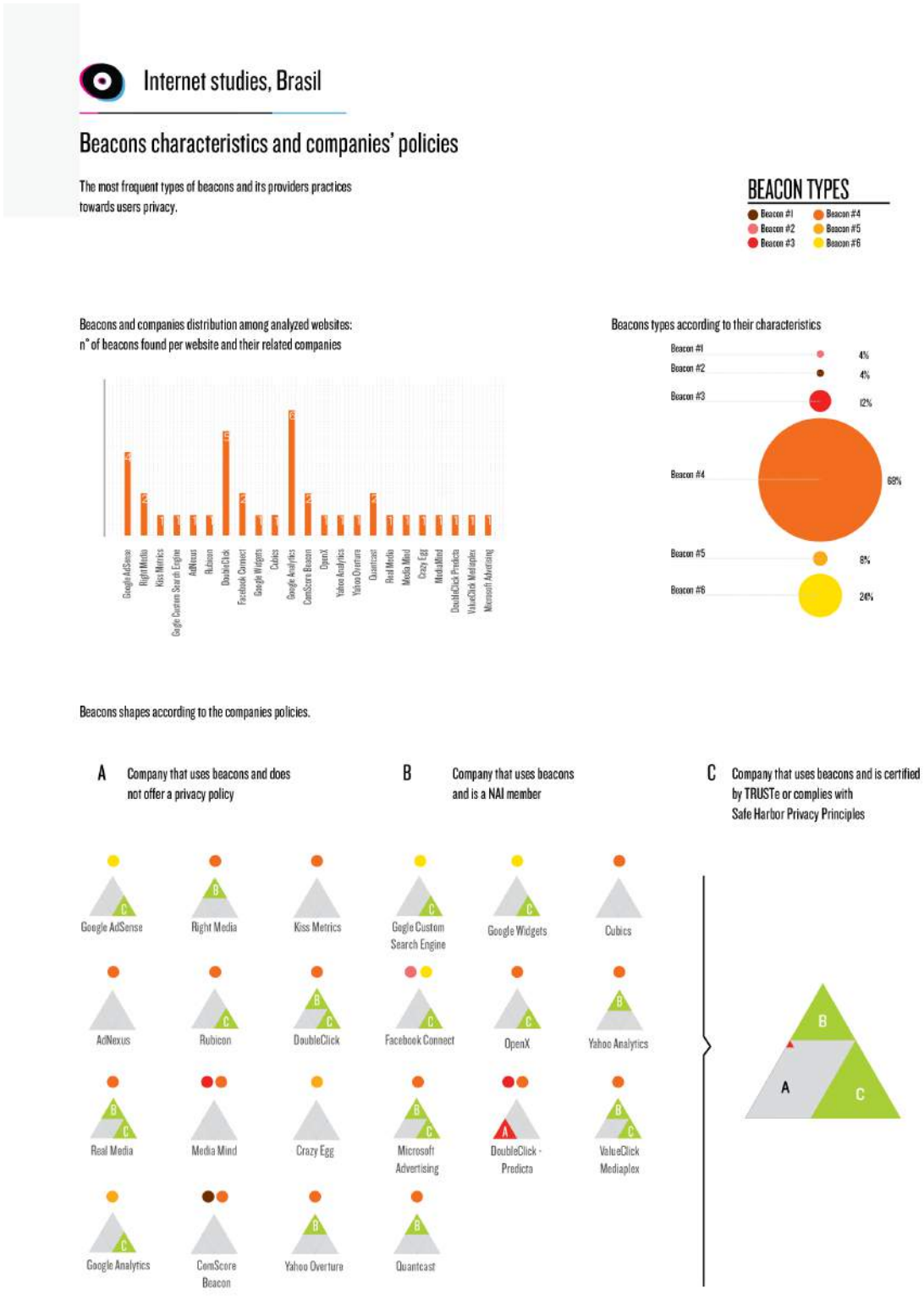
Graph 30: Characteristics of the cookies and policies of the companies



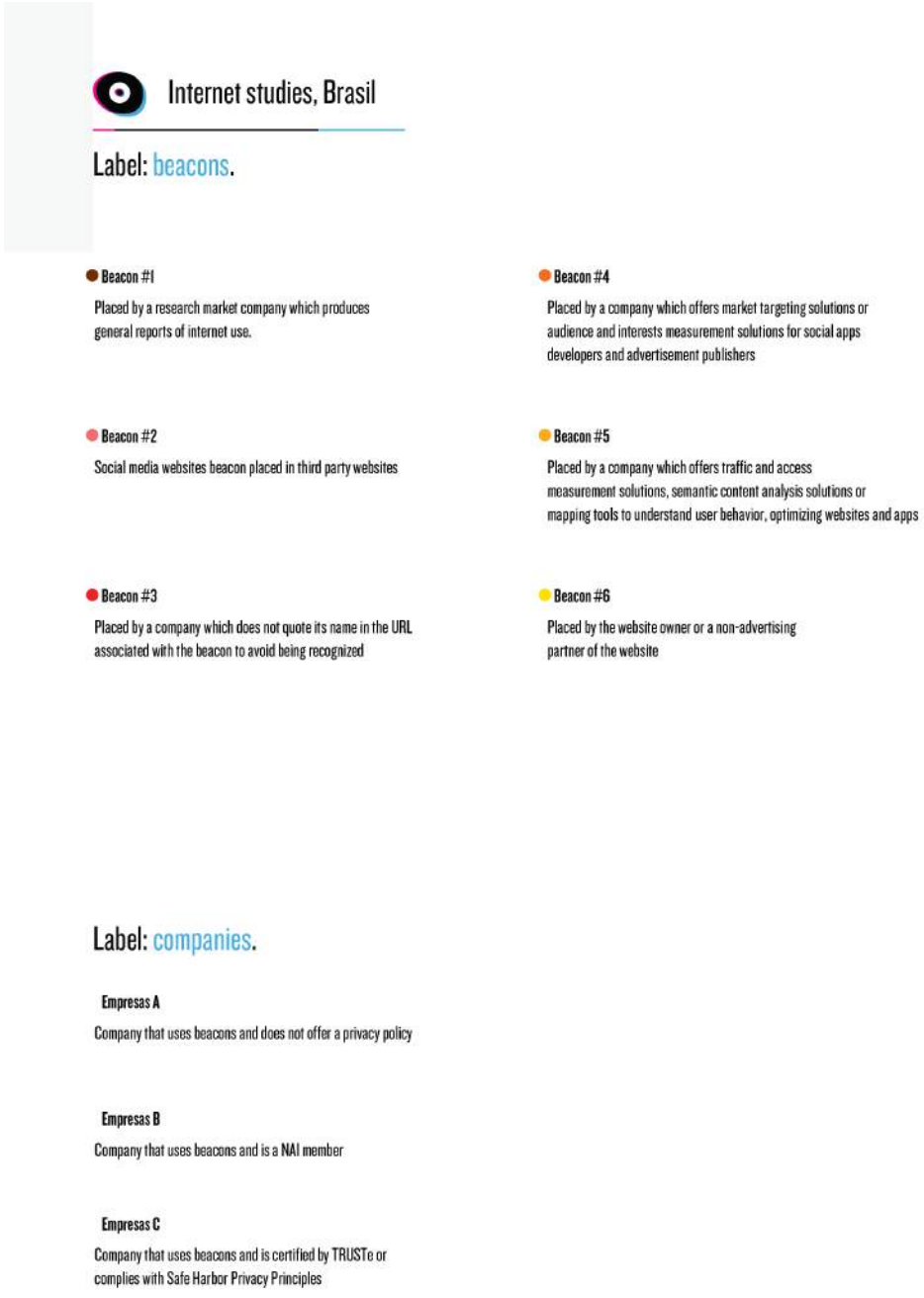
Graph 31: Etiquette (types of cookies and companies)



Graph 32: Characteristics of the beacons and policies of the companies



Graph 33: Etiquette (types of beacons and companies)



5.2.2 Survey on the introduction, exposure, and use of personal data in the Internet

Based on what this project proposes, a preliminary survey was made with questions on Internet usage, and the users' opinion on the introduction, exposure, and use of personal data therein. The purpose was to obtain information to show the user's perception of Internet with regards to the eventual exposure and use of their data; to prove the clarity and pertinence of the questions in order to integrate them into a questionnaire on the subject, with the option of applying it at a larger and more representative scale in a future phase of the project.

The first questions making up the survey were aimed at obtaining a socioeconomic profile of the person interviewed (gender, income, education level), followed by questions on their Internet usage habits (location, frequency, hours of usage, activities developed). This survey plan was based on a broader one, made by the Internet Management Committee in Brazil (CGI.br), which is applied by said Committee from time to time with the intention of gathering a representative sample of the Brazilian socioeconomic profile.

To structure such a probe based on the CGI.br questionnaire opens up an interesting possibility for future dialog, in as much as it allows for comparisons and cross referencing between the studies. The results of the CGI.br survey, published since 2005, have a considerable national outreach and academic acceptance. Besides, the work already done by this Committee allows for the inclusion of another type of information that is relevant in the construction of a more complete profile of those interviewed, even though that information may not be directly related with the subject of this study.

The questionnaire was voluntarily answered from a form available online. The call was made through social feeds (Facebook and Twitter), using contacts previously established by the researchers. The surveyed population was informed that this was an initial phase for the survey, in which data would be considered but that the questionnaire itself was being evaluated.

As a result, 69 answers of those obtained were considered valid, although within a rather specific sample profile: intensive Internet users, with high income and education levels, both for Brazilian and international standards. More than half o those interviewed (58%) have some form of post-graduate degree; half of them are among the top income range (over 5,100 Reales monthly, approximately equivalent to 3,100 US Dollars); and 89% of which use the Internet on a daily basis.

A semistructured questioning model was followed, that is, one with open and closed questions mixed. Only two questions asked offered open fields to textual answers with the intention of having the participants elaborate on the matter. The first one asked for a short description of eventual "issues about privacy or use of personal data on the Internet", the second one asked to "evaluate and make suggestions for the questionnaire." Only one of the participants criticized the number of questions and another expressed doubt in reference to the question "Currently in Brazil there are proposals circulating as to the creation of laws to fight anonymous Internet presence. Try to classify your position in relation to this matter, with 1 representing your most favorable position towards the proposed law and 5 representing the least favorable."

In relation to the research subject (perceptions on the matters of "privacy" and "personal data usage in Internet") the concepts of "use of data" and "personal data", as well as the notion of "privacy", were kept as open as possible. To that effect, certain alternatives were presented that allowed those surveyed to infer over the sense given to those concepts. For example, question nine, which probes for an instance in which the surveyed may have fallen victim of what they could classify as "issues of privacy or with the use of personal data on the Internet" (which obtained 21% of affirmative answers) was followed by a request to give a description of those issues. Most of these answers pointed to the receipt of spam, indicating to a perception that the email address had been inappropriately exposed or commercialized, resulting in the frequent receipt of unsolicited mail. Other issues pointed out were email invasion (four answers), credit card number theft (two answers), identity theft (one answer), phishing (one answer), inappropriate exposure of personal contact list (one answer), and unauthorized exposure of physical address (one answer).

There was likewise an aim to investigate the Internet behavior declared by those surveyed, more specifically in environments of possible personal data exposure such as the social networks. The most mentioned activity was the reading and sending of email (97%), followed by the use of social networks, at 87% (for this item, the services of Facebook, Twitter, and Orkut were given as examples). Those who answered affirmatively about the use of social feeds were asked how they perceived safety levels in such services, where a scale from 1 (very safe) to 5 (very unsafe) was presented to choose from. Most participants (38%) chose an intermediate point in the scale (3), 13% picked "very unsafe" (5) as their answer, 22% chose "4", 11% chose "2", and merely one of those surveyed picked "1" (very safe) for the answer.

The participants were then presented two questions related to the use of social networks and sites, followed by one that asked about what they considered "personal" data and that offered the same answer alternatives. These questions tried to list diverse kinds of data for which those interviewed could present standardized shared use behaviors, whether these data apply for complete exposure, for anyone, or for restricted exposure, only for authorized persons. The questions and the partitioning introduced seem to work in the sense that those interviewed show a less restricted behavior when exposing texts, images, or indications (of pictures, videos, and favorite artists music,

for instance) of their property. Meanwhile, they show a more reserved behavior when exposing multimedia materials and information linking friends and relatives.

This reserved behavior is also shown when exposing "personal data". When questioned on this matter, nearly all participants –around 90%– consider as personal data their telephone numbers (both cellular and landlines), address, fiscal number and, to a lesser extent, their email address. On the other hand, mention of multimedia materials linked to relatives and friends as "personal data" is high: around 60% when those involved are friends and/or the surveyed one; and nearly 80% when those involved are relatives, even if children. Comments made by the interviewed participant and the multimedia materials of their favorite artists, by them made, are the options least chosen (24% and 25%, respectively). What this type of answer indicates is that the participants understood the question in a peculiar way, that is, the "personal" part in "personal data" is not taken as something produced by that person, but rather some information they consider as delicate about themselves or their contacts network.

Questions that prodded in search of hints as to what extent the subjects of privacy and use of personal data online produced concern were also applied. Two similar questions looked into their degree of concern, where the lowest degree meant "unconcerned" and the fifth one, highest one, "very concerned". One of the questions dealt with "exposure of their personal data online" and another with "commercial use of their data online". For both questions, the highest number of replies coincided with the two highest points in the scale, four and five. However, the question that dealt with commercial use gathered the highest point in 36% of the answers, and 32% for the fourth point; whereas the question involving the sole exposure of personal data online gathered the most replies for the fourth point, at 34% (22% for point five). Ask about what agents would be most interested in gaining access to personal data, those interviewed chose in first place private companies (84%) followed by criminals (63%), then by the State (41%), and lastly by the police (18%). The answer in relation with the potential interest some might have helps to clarify the previous answers, given the high choice rate for the option of "private companies". Many might appear to pick this option with spam mail in mind.

Given the bill in Brazilian congress to set up tougher laws in relation with anonymous activities on Internet, certain questions were introduced on the matter, both on the practice (the use of pseudonyms for blog comments and social feeds, for instance) and on the perception of the allowance on the part of the current technological infrastructure of Internet. The great majority of those interviewed (42%) said they never used pseudonyms, a number that falls sharply one step farther down the scale (16%), until it finally reaches 5% by the last point, meaning, "always" [use pseudonyms]. In relation with the perceived level of anonymity in Internet, most of the participants chose the intermediate point (37%) in the scale from "totally anonymous" (0%) to "not anonymous at all" (17%). The tendency in those interviewed, however, was to perceive the Internet as little anonymous, since item two in the scale gathered 11% of picks and item four 26%.

Although data here shown may not have statistical representativity, given the number of completed questionnaires and a sample profile that does not adhere itself to the socioeconomic structure, it throws interesting indexes. It is apparent, for instance, that those interviewed admit to behaving less cautiously when expressing opinions and personal preferences. Their attitude changes and becomes more cautious when dealing with data and multimedia materials that involve relatives and friends, and is yet more restrictive when dealing with the exposure of personal telephone numbers, home address, and ID numbers. Such change seems to be related primarily with the fear of safety issues.

We have to take into account the high scholarship of those interviewed; however, the quality of their answers allows us to assume that the questions were sufficiently well understood and that they allow for a broader application of the sample, so that with a statistical structure it may reach all the Brazilian socioeconomic conformation and, finally, the Latin American one.

Alongside their function in gathering information on the perception of use and exposure of personal data in Internet, we have to highlight the fact that the survey and the questions there introduced end up calling public attention on the matter, thus contributing to a more ample debate on the subject.

We also believe that this report constitutes a first and important stage in the consolidation of the Latin American studies Network.

5.3 Personal data on Internet in Mexico

5.3.1 How the mapping of the Internet and personal data case was done in Mexico

The identification of subject matters relevant in the protection and control of personal data on the Internet in Mexico was divided into three main categories:

1. Researchers, lines of investigation
2. Public and private agents
3. Technologies

Each one of these categories was applied a specific methodology in order to reach the most appropriate results for the purposes of the research, as shown below:

i. Researchers and lines of investigation

Objectives: a) to explore the academic output of Mexican researchers writing on the matter in Mexico, Mexican researchers dealing with the matter in other countries, foreign researchers dealing with the matter in Mexico, and foreign researchers dealing with the matter at a global level.

b) To identify lines of investigation related to the matter of the project, to identify sources of information, as well as the selection of articles or documents by year of publication and country of elaboration.

Methodology

The method used to design this first category consisted in locating sources of valid and safe information within the Internet, where authors could be looked up and their line of research analyzed and compared with the project objectives, while keeping in mind the author selection criteria above mentioned.

Observations: For the purpose of the research, out of the 28 researchers looked up there are:

- 22 Mexican researchers
- 5 Spanish researchers
- 1 Argentinian researcher

Among the various authors writing on this subject, certain lines of research have been found that help in having parameters on what has been written:

- Privacy and the protection of data when considering cybernetic delinquency and computer security.
- The age of information and legislation
- Security and data protection rights
- Transparency and security
- Society of surveillance
- Media and education

Also, 19 researchers have direct links with the subject dealt with in this research, while the remaining 9 researchers are indirectly related to them. In reference to the Mexican researchers, they all directly tackle personal data protection, technologies, laws, the Internet, regulation, rights, and identity in Mexico; and finally all five Spanish researchers and the Argentinian one look at the theme from a global standpoint. The lines of investigation of each one of those looked up are aimed at personal data protection, technologies, surveillance, and legislation. Said researches are about one year old in 2010.

The articles by these researchers belong to various institutions such as:

- Biblioteca Jurídica.com
- Protección de Datos personales y privacidad.org
- UNAM (UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO) "Boletín Mexicano de Derecho comparado"
- El Universal. Diario de circulación nacional en México
- Biblioteca Jurídica Virtual UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO (UNAM)
- Comisión para el Acceso a la información pública
- Instituto de Transparencia de Sonora
- La Jornada. Diario de circulación nacional en México
- Gobierno del Estado de México
- Debate.com.mx
- INEGI (INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA)
- Página de la Presidencia de la República. México
- Isegoria revistas
- Universidad de Sevilla
- Red Iberoamericana de el derecho informático
- UAM (UNIVERSIDAD AUTÓNOMA DE MÉXICO) en la revista "El cotidiano"
- Universidad de Guadalajara en la revista "Comunicación y sociedad"
- Universidad de Sevilla en "Pixel-Bit. Revista de medios y comunicación"
- Instituto Tecnológico y de Estudios superiores de Monterrey en "Global media Journal"
- Universidad Oberta de Catalunya en "RU&SC Revista de universidad y sociedad del conocimiento"
- Universidad de Murcia en "RED Revista de Educación"
- Facultad latinoamericana de C.S en "Perfiles latinoamericanos"

ii Public and private agents:

In this respect, and especially government agencies holding data bases of personal data protection: IFAI does not have a personal data base, unlike INEGI and the IFE with their electors data base.

The methodology used in this second category consisted in identifying movements or public or private organizations that may have dealt with actions in pro of the protection and control of personal data, whether at a national, state, or international level.

Objectives:

a) To determine which movements or organizations may have practices that help in the spreading and reflection on the matter of personal data protection in the use of Internet in Mexico
b) To point out the actions taken by organizations in favor the control and protection of personal data, to identify the most recent actions, and to describe the ways in which those actions have been carried out.

Observations: There are various public and private institutions with an interest in the safeguard of personal data upon accessing the Internet. Among those institutions, there are 3 private ones and 18 public ones, whose actions all took place in the year 2010. This year was chosen because some of the institutions started dealing with the subject then, whereas in others the most relevant action took place that year.

Of the institutions looked up, three are Spanish, one American, one Chilean, and 16 Mexican. Among the actions performed by these institutions we can find: a) The introduction of the subject of data protection, promoting the knowledge of specialized articles in the federal legislation dealing with the protection of personal data, b) To publish in Internet sites, c) To use the Internet to create awareness of the issue of exclusion, and d) To publish articles in which concern is expressed over the lack of organization and legislation of personal data.

Out of the 21 institutions, 7 have an international aim and 14 a national one.

In order to illustrate this, shown below is a table with the name of the agent, whether it is public or private, and the action by it performed.

Table 3. Public or private nature of the agents

Agent	Public or private	Action performed

IEAIP(Instituto Estatal de Acceso a la Información Pública - State Institute for Access to Public Information)	Public	Invitation to deliberate on data protection
IFAI (Instituto Federal de Acceso a la Información - Federal Institute for Access to Public Information)	Public	Verdict on budget
Blog, Gurú político - Political Guru	Public	Introducing the subject of data protection
Revista Transparencia de Nuevo León - Transparencia magazine from Nuevo Leon	Public	Event: “Files and Accountability”, organized jointly with the National Security Archive, George Washington University
Benemérita Universidad Autónoma de Puebla - Puebla State University	Public	Specialized article on federal legislation for data protection, in their internet site
Universidad Autónoma de Nuevo León - Nuevo Leon State University	Public	A panel on data protection was set up, called “Perfectionable, the data protection system”
Alianza Cívica	Public	Organized a training course on data protection, in Sonora

iii: Technologies: For the elaboration of this third category, the technologies related to the objective of this research have been identified.

Objectives: a) To identify the technologies which, because of their characteristics, could become means for the control and protection of the users personal data.

b) To identify companies or systems that control or manage personal data for their operation.

Observations: In the "Technologies" group we find Google-maps, cookies, Facebook, wi-fi networks, Street View; that are set up to make public people location, keep a log of web sites visited, and make communication easier. All aforementioned technologies facilitate the gathering of personal data.

i Researchers and lines of research

Author: Avilés Karina

Title: Identity theft crime up

Subject: Identity theft in Mexico is a crime on the rise, the most rapidly growing crime in the world due to the ease with which other persons' identities can be forged by replacing photographs and personal data. This type of crime can be carried out through fake emails, online banking processes, data base sale, or the attack of people specialized in such activity. However, there is no specific legislation on the matter and it is very important to gain awareness thereof, since sharing data over social feeds is very easy and awareness of what others could manage with our information is unknown.

Type of document: Newspaper article

Year of publication: 2010

Publication:
http://www.jornada.unam.mx/2011/02/21/index.php?section=politica&article=016n2pol

Keyword: security

Author: Carrillo Edgardo

Title: Personal data protection in Facebook time

Subject: This is a text from the conference "Personal data protection in Facebook time", which explains the relevance and also the risk or repercussions of uploading provocative pictures, or pictures of oneself drunk, to one's profile page. Here's a number of recommendations on how to protect our personal data in Internet: in first place, to create a self-protection awareness, starting by an understanding of the usage conditions of the social feeds where they are subscribed and then applying at least the security controls therein; thus, to understand the similarities between real life

and the Internet, to make contact with only those people we may know, not to forward chain messages, not to share with the aim of gathering more friends, to protect the computer, and to adequately configure the security options.

Type of document: Blog article

Year of publication: 2010

Publication: http://transparenciasonora.org/colateral/index.php?artids=19&cat=1&categoria=1

Keywords: privacy and delinquency

Author: Castells Manuel

Title: The Internet, Freedom, and Society, an analytical perspective

Subject: It deals with the creation of the Internet and its becoming a tool for information control.

Type of document: Magazine article

Year of publication: 2003

Publication: http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=3050041

Keywords: control, technology, Internet, security

Author: Cunjamá López Emilio Daniel

Title: Watching society and policing state: an analysis of technologies and information control

Subject: Surveillance technologies require subjects to supervise; the individuals are subject to being supervised as long as they consent to be objectivized by the vigilant eye. This way they can be caught by the other's vision. This is, surveillance technology represents the relationship between the subject (supervisor) and the object (supervised). In Mexico it is assumed that the police force watches you, the IRS watches you, your health is being looked after, altogether there is a state supervising you. Then the state is the supervising subject and the society is the supervised object. In fact, the state promotes a self watching society: "if you witness an unlawful action, denounce it"; but what happens when society stops being that object, de-objectivize itself, leave the framework, to move around in the picture and then even be in itself the one taking the pictures? When do the supervisors start being those supervised, when do they become objects of scrutiny and are no longer the ones supervising?

Type of document: magazine article

Year of publication: 2001

Publication: http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=32513865002

Keywords: Surveillance, control, technologies

Author: Crespo José Antonio

Title: Data trafficking and insecurity

Subject: The existing link between corruption and impunity in Mexico allows for confidential information to be easily leaked and for them to spread to Tepito or the social feeds, altogether generating an apprehension over the submittal of that information, to avoid such requirement in as much as it is possible. Meanwhile, there is precisely a discussion over the creation of a law to avoid the propagation of confidential information that the citizens surrender to the government or the private sector.

Type of document: Blog article

Year of publication: 2010

Publication: http://www.debate.com.mx/eldebate/Articulos/ArticuloOpinion.asp?idArt=9823390&IdCat=6115&Page=2

Keywords: Protection, corruption

Author: Flores Vargas Rosalba

Title: Curtailing the trafficking and use of personal data, especially by private companies

Subject: Curtailing the trafficking and use of personal data, especially by private companies, as well as the identity replacement and even abductions; these will be the chores of the recently created Special Commission for Personal Data Protection whose president, PAN congressman Gustavo Parra, said it would call for forums and academic debates so as to include not only a lawmaker's vision but that of an entire society. Now what is important is to achieve within the state is to first let society know it has gained protection of its data.

Type of document: Web page article

Year of publication: 2010

Publication: http://poderedomex.com/notas.asp?id=61000

Keywords: Protection and identity, personal data

Author: García Barrera Myrna Elia

Title: Personal data protection in Mexico

Subject: This deals with globalized times and the boost of the new technologies, specifically the development of the Internet and of the information technologies, which together with other factors have paved the way for the incorporation in our laws of a couple of very recently produced rights, about which there are still many elements needing definition, of which we have: the right of access to information and the protection of personal data.

Type of document: Presentation

Year of publication: 2010

Publication: http://www.scribd.com/doc/39205110/La-Proteccion-de-Datos-Personales-en-Mexico

Keywords: Personal data, transparency

Author: García González Aristeo

Title: The protection of personal data, fundamental right of the 21st century. Comparative study.

Subject: This study goes about the importance that technological development gains on a daily basis, since it has become a revolution for those traditional organizational methods. Together with this, the treatment of information represents a risk, above all if that information deals with a person's data. Therefore, the use and control over anyone's personal data must be recognized not only as a guaranty but also as a fundamentally protected right. Hence the relevance of recognizing a fundamental right in the protection of data at a constitutional level and furthermore, guaranteeing its protection.

Type of document: Magazine article

Year of publication: 2010

Publication: http://redalyc.uaemex.mx/src/inicio/ArtPdfRed.jsp?iCve=42712003

Keywords: Human, individual, and privacy rights

Author: Gómez-Robledo Alonso

Title: Personal data protection: the case of the federal executive power

Subject: This is a study aimed at describing the juridical framework prior to the existence of the Federal Law for Access to the Governmental Public Information, which establishes the confidentiality and treatment of certain information in relation to physical persons. The principles of personal data protection contained in the international treaties signed into by Mexico are

identified, as well as a look into how they have been assimilated by the laws of access to the information in Chapter VI “protection of personal data”. Likewise there is an overview of the actions taken by the federal executive power in favor of the adequate treatment of personal data stored in their archives, which go from the adoption of a secondary legislation to the use computer tools for the registration o personal data systems.

Type of document: Book

Year of publication: 2010

Publication: http://www.bibliojuridica.org/libros/5/2299/3.pdf

Keywords: Access to information, law, protection

Author: González María de Luz

Title: Private information uncontrolled in Internet

Subject: This is an article which deals with the ease with which costumer lists, telephone number listings, and credit card information can be obtained; it is a search in which EL UNIVERSAL found online sites that offer data bases from 10 thousand Pesos, and that make evident the existent complicity with the police, since it is possible to scramble those who navigate those sites with the purpose of purchasing personal data.

Type of document: Newspaper news

Year of publication: 2010

Publication: http://www.eluniversal.com.mx/nacion/177168.html

Keywords: Security, Internet, and regulation

Author: González Hugo

Title: A delay for democracy

Subject: This article says about discussions in the Senate about the participation of Mexico in multinational treaties aimed at authorizing internet service providers to review the information that its users circulate online. Technology experts consider a coup against freedom, privacy, and the free use of the Internet might be approaching. The treaty, promoted in USA since 2007, wants for ISPs to review and analyze the users’ upload and download packs with the purpose, they say, of limiting piracy in the Internet.

Type of document: Magazine article

Year of publication: 2010

Publication:
http://www.elderechoinformatico.com/index.php?option=com_content&view=article&id=498:un-retrazo-a-la-democracia&catid=104:elderechoinformatico-mexico&Itemid=119

Keywords: Technology and Internet

Author: González Hugo

Title: SEGOB proposes to regulate the Internet as a strategy for the social inclusion in the make-believe of the poor.

Subject: This article is about the discussions on Internet regulation. It mentions the possibility of applying a regulation of contents in Internet. Leopoldo Brito (content director) showed concern in the sense of a legislation about contents in internet, and suggested an auto regulation with legislation, so that parents have a clear knowledge of the contents allowed, all this because of the serious problem of child pornography, violence, and sexual abuse, the only problem present in the debate is who is that person supposed to regulate the contents of internet.

Type of document: Web page article

Year of publication: 2010

Publication: http://www.presidencia.gob.mx/prensa/ultimasnoticias/?contenido=30874

Keywords: Regulation, Internet, freedom

Author: Herrera Ramos Mario

Title: Digital segmentation in Mexico

Subject: This study proposes the concept of "digital segmentation" to describe differential access of individuals, homes, and regions to the assets and services offered through the use of information technology at various levels: with the OECD countries between large and small companies, as well as between producers and those dedicated to home commerce with possible access to computers.

Type of document: Magazine article

Year of publication: 2005

Publication: http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=11501802

Keywords: Technologies, Internet, digital gap

Author: Ibarra Cadena Blanca Lilia

Title: Transparency in the Americas at half way.

The right to information and social benefits.

Subjects: This article refers to activities that took place in the VI International Transparency Week. It mentions issues dealt with such as transparency in Latin America, data protection on the part of the governments, personal identification data protection, limitations in national security. Which information must be reserved on the grounds of national security?

It makes reference to the relevance of transparency of information and public information, as well as the benefits thereof derived. For that purpose it gives examples of various sectors of society for which the utility this matter varies considerably from one to another, although it is of no less relevance to any. For instance, to have a government that reports with transparency is a confidence builder for a company, to know allotment procedures builds credibility, to be aware of government programs and their rules allows for the entrepreneurs to gather incentives. For housewife: to be aware of health services brings benefits, to obtain information on procedures for family assistance, to be aware of the state of work being done at home, to know about training programs for job hunting. Students: research, awareness about requirements, query about the functioning of governments.

Type of document: Web page articles

Year of publication: 2010

Publication: www.caip.org.mx/artículos/2010/0107 blic.htm

Keywords: Law, data protection, freedom of communication, security, transparency, right to information, reporting.

Author: **Jiménez Horacio**

Title: OECD urges personal data protection law

Subject: News in relation to OECD concerns for Mexico to push for a personal data protection regulation through the Federal Public Information Access Institute. It argues that out of the 30 countries conforming the OECD, 28 have specialized legislation on this matter and only Turkey and Mexico are still lacking one. Commissioner Singrid Arzt Colunga, representing the IFAI, presented the forum participants a series of proposals and consultations with the aim of enriching the legislation initiative that is currently (March, 2010) being drawn in congress.

Type of document: Newspaper news

Year of publication: 2010

Publication: www.eluniversal.com.mx/notas/664335.html

Keywords: Data protection law, privacy framework

Author: **Luna Pla Issa**

Title: Personal data protection in Mexico City

Subject: This article deals with legislation set up by Mexico City government in 2008 on personal data protection. This law sets forth substantial changes in the treatment and conformation of the systems the government uses, while it also presents a challenge in guaranteeing the rights this legislation grants. Then, personal data protection laws such as this one carry two purposes: 1) the design of a set of intertwined norms for the protection of personal data, which in turn implies the creation of norms and procedures for their creation, use, and extraction, as well as the treatment given to this information by the public entities, 2) to guarantee the exercise of the so-called ARCO rights: the rights to access, rectification, cancelation, and opposition; all of these being fundamental rights that the owner of the data is capable of exercising before the public body.

Type of document: Magazine article

Year of publication: 2010

Publication: http://www.juridicas.unam.mx/publica/rev/decoin/cont/15/cmt/cmt5.htm

Keywords: Personal data protection law

Author: **Martínez Nurit**

Title: NGO: RENAUT makes personal security vulnerable

Subject: RENAUT, the service for registering mobile phone numbers, is at the center of this article. It says many people have filed appeals to this duty, since consumer defense organizations warned that the registration of these telephone lines using personal data may result in higher risk to users security, especially minors. A1 Consumidor said they would provide support. Also, an open appeal has been elaborated (called “paquete-defiendas”) for those wishing to subscribe to it in order to gain legal action.

Type of document: Newspaper news

Year of publication: 2010

Publication: http://www.eluniversal.com.mx/nacion/176914.htlm

Keywords: Security, vulnerability, risk, corruption, personal data.

Author: **Manuera Giner Francisca**

Title: New technologies and exclusion, there is life beyond the Internet

Subject: New forms of poverty and social exclusion are the negative face of a society that defends values such as freedom, coexistence, tolerance, and equal opportunities. The new information and communication technologies open up new possibilities in the achievement of these values, but they can also generate new exclusion situations derived from the current economic growth model, which demands a greater flexibility and adaptability from a society in permanent and speedy change. Individuals and groups more socially disfavored, or those others who may not have the adequate training background in order to integrate the use of newer technologies may be left behind in social participation processes. So it is up to all of us, partly, that we should consider these as negative byproducts of modern times or else to start educational actions not set on economic parameters but rather on those of social justice.

Type of document: Magazine article

Year of publication: 2004

Publication: http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=36802606

Keywords: Technologies, poverty, social exclusion, education, and equality.

Author: **Ortiz Henderson Gladys**

Title: Access and use of information and communication technologies among Mexican children: the case of Monterrey.

Subject: This text shows some of the results stemming from an investigation made on the access and use of information and communication technologies among children from fifth and sixth grade in the city of Monterrey. It deals with the characteristics of media exposure in which children develop, paying special attention on the access to Internet, on how they learn to use it, and how they navigate in it.

Type of document: Magazine article

Year of publication: 2003

Publication:

Keywords: Technologies, poverty, social exclusion, education, and access.

Author: **Pérez Luó Antonio Enrique**

Title: Guardianship of informatics freedom in a globalized society.

Subject: This work bases its purpose in a triple and converging objective: 1) at first it analyzes some of the most relevant events reflecting computing risks for rights and freedoms, 2) it offers a summarizing chart of the judicial response to threats against freedoms; such response having

materialized in three generations of laws protecting personal data, whose corresponding informative features are listed, 3) it finally calls for a global judicial response.

Type o document: Web page article

Year of publication: 2010

Publication:

Keywords: rights and freedoms

Author: **Rangel Rodríguez Samuel**

Title: Social feeds and transparency: between the public and the private.

Subject: It starts out commenting on the definition of personal data, considering as such home address, phone number, fiscal number, religion, sexual orientation, bank accounts, affective and home lifestyle, clinical files, biometric information such as digital fingerprints and iris features, among others. Altogether, data that may affect a person's private life. Then let us reflect upon the possibility that these data may fall into the hands of delinquents. While in other countries, especially across Europe, there are federal and local authorities whose job is to oversee the protection of everyone's personal data, making sure that the authorities do not misuse them, even applying sanctions; in our country the advance in this respect is sadly little.

Type of document: Web page article

Year of publication: 2010

Publication:

Keywords: Internet, social feeds, vulnerability

Author: **Romero Pavía**

Title: The use of information and communication technologies in the basic education of youth and adults in rural and urban communities of Mexican southeast

Subject: The use of information and communication technologies at various levels and education systems has a significant impact in the development of the students learning and in the strengthening of their competences for life and work, as they could favor their access into a society of knowledge. This work reflects a research carried out on the use of ICTs in the basic education of youth and adults through the Education Model for Life and Work, both in its virtual and online modes, in rural and urban communities of the state of Yucatan. The results of this study document the opinion of young and adult people with respect to their abilities in the use of ICTs, their

opinions on both virtual and online modes, and the difficulties they encounter as users. The results are discussed under the 2007-2012 Mexican Education Sectorial Program.

Type of document: Magazine article

Year of Publication: 2001

Publication: http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=54715149004

Keywords: Technologies, exclusion, digital gap.

Author: **Saavedra Ponce Viridiana**

Title: COMAIP: the law must contemplate the protection of personal data.

Subject: Presidents from transparency organizations in eastern Mexico, on visit in Jalisco, argued that legislation for personal data protection must be carried out. César Octavio López, president of the Mexican Conference for Access to Public Information, stated that (the ITEI is a solid institution and that guarantees the work continuity."

Type of document: Newspaper news

Year of publication: 2010

Publication:
http://www.lajornadajalisco.com.mx/2009/08/06/index.php?section=politica&article=007n2pol

Keywords: Personal data, transparency

Author: **Sánchez Martínez José Alberto**

Title: The Internet and one's surveillance: morphing and post-image in the century of cameras and screens.

Subject: It is possible to think that the 21st century will be one of cameras and screens, one in which reality will be recorded and broadcasted. Unlike the 20th century, cameras and screens will gain unprecedented relevance, most of all in the dialog between the Internet and everything digital. Some suspect something else: that in our century the use of cameras and screens will grow towards video surveillance. What this work pretends is not to assume video surveillance from the perspective of state control, but rather to understand what happens with camera and screen in the relation established by the Internet, how cyberspace users relate, with oneself, what role one assumes. This text explores identity as a statute of video surveillance, self image crisis, even the visual regionalization that flows into the morphing and the post image.

Type of document: Magazine article

Year of publication: 2000

Publication: http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=32513865004#

Keywords: Internet, technologies, software surveillance

Author: **San Martín Velasco Cristos**

Title: Privacy and protection of personal data in Internet. Is it necessary to have a specific regulation in Mexico?

Subject: Privacy and the protection of personal data are important elements in the various forms of e-commerce, but have gained major relevance particularly in the business area, online purchases, or simply when users exchange information and data between themselves or with companies and the government online. The issue of personal data protection is becoming more relevant in another kind of electronic commerce sites as is the case of Government to business, especially in as much as the Mexican government implements its E-Government system, through which it pretends to guarantee citizens their free access to an array of public services.

Type of Publication: Web page article

Year of publication: 2010

Publication:

Keywords: Personal data, transparency.

Author: **Siles González Ignacio**

Title: Off to conquer an online world: the Internet as an object of study (1990-2007) in communication and society.

Subject: This article explores the development of research on the Internet between 1990 and 2007. To this effect, an analysis is made of the main thematic axes of the studies on this medium as carried out over nearly two decades, meanwhile diverse debates are presented as they constituted its evolution as an object of study. There is a suggestion that studies on the Internet constitute a field of knowledge under construction, with a growing academic legitimacy.

Type of publication: Magazine article

Year of publication: 2001

Publication: http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=34601003

Keywords: Internet, identity

Author: **Tello Leal Edgar**

Title: Information and communication technologies and the digital gap: their impact on Mexican society.

Subject: It is something desirable to reach a society of knowledge where the individuals' inclusion in the generation is total, that societies of knowledge may become fountains for everyone's development and above all for the least developed countries. The purpose of this article is to analyze the roles of the digital and cognitive gaps in the knowledge societies as causes for the exclusion of companies and individuals in the use of communication and information technologies in Mexico. As a consequence, nowadays we find a new form of exclusion, known as the digital gap, which is capable of widening the abyss separating regions and countries and citizen groups in a society. The cognitive gap makes evident the potential for exclusion inherent to knowledge societies, when their development is limited to the promotion of an economy of knowledge. Meanwhile the work shows figures of the digital gap in Mexico, as much in homes as in companies, so as to expose an unequal access among geographic areas of the country, that not only depends on the available infrastructure but also on the abilities of the population for the use of information and communication technologies.

Type of document: Magazine article

Year of publication: 2001

Publication: http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=78011231006

Keywords: Technologies, exclusion

Author: **Winocur Iparraguirre Rosalía**

Title: The computer and the Internet as strategies for social inclusion in the make-believe of the poor.

Subject: The new technologies make up a part of the popular fancy, although most people may not have access to them, these fancies build wishes, expectations, and aspirations, but also fears and anxiety that the computer may become an element of social exclusion, this research is based in San Lorenzo Chimalpa, Chalco.

Type of document: Blog article

Year of publication: 2010

Publication: http://campus.usal.es/~teoriaeducacion/rev_numero_06/n6_res_winocur_rosalia.htm

Keywords: Technologies and social exclusion.

Author: **Zabia de la Mata Juan**

Title: Data protection: comments on the rules.

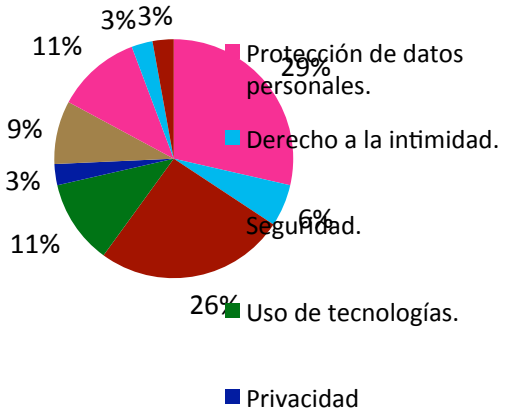
Subject: In November 2005, the Ibero-American Network of Data Protection created a group of "auto regulation instruments" through Mexico's declaration, with the purpose of analyzing the validity and efficacy of the codes of conduct or analogous instruments, taking into account the relevance of the initiatives taken by those responsible for the archives or treatments for the protection of data to be carried out through instruments of auto regulation. The document "Auto Regulation and Protection of Personal Data" was then elaborated, in which there is mention of: the incorporation of legal texts on data protection, explicit decisions on the use of auto regulation mechanisms, and the invitation to the states and those responsible for the treatment of personal data to promote the adoption and implementation of mechanisms of auto regulation.

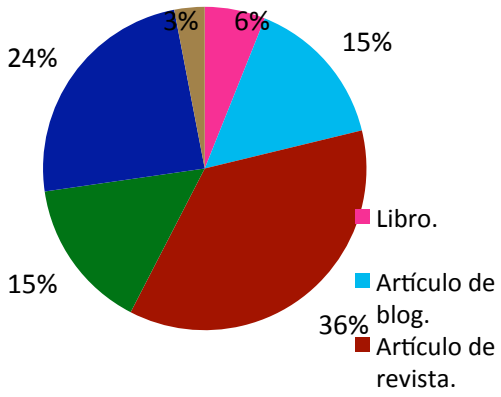
Type of document: Book

Year of publication: 2010

Publication:
www.books.google.com/books?id=R4GWPWwW8JcC&pg=PA644&dq=proteccion+de+datos+personales+mexico

Keywords: Judicial security, fundamental rights, and data protection.





The protection of personal data in Mexico constitutes an issue whose study has generated diverse approaches; the very nature of the phenomenon has already exerted influence in the construction of analysis categories needed for its understanding. However, the output of documentation and related information might seem not as solid in its scientific buildup. Mostly, the contributions on the subject come from publishing forms such as blog articles, newspaper opinion notes, etc. Then, it might seem that the study of personal data protection in Mexico is isolated in the production of scientific knowledge that should take place in universities and in research and education centers. Mapping results indicate that 76% of information sources come from blog entries, editorial groups, or electronic portals; while 24% stem from a research project hosted by some research center and under the tutorship of a researcher. Likewise, the issue of personal data protection in Mexico is an ongoing one that is still to constitute itself as a debate in the building of the government public agenda.

ii Relevant agents

Agent: **Political Guru**

Kind/Modality: Public, blog.

Proposal: To position the issue of personal data protection in the definition of a governing public agenda.

Year: 2010

Description: From the creators of the Political Intelligence Center (CEINPOL) that was active from 1 February 2009 to June 2010, comes now Political Guru (founded 1 July 2010). A Mexican Internet site specialized in exclusive editorial political contents, with a daily analysis of national and international events. Made in Acapulco, Guerrero State, Mexico. Political Guru is not a tabloid, is not news oriented: it is exclusively a medium for opinion and analysis.

Scope of incidence: The use of technologies and security.

Agent: **Transparency of Nuevo Leon**

Kind/Modality: Public, magazine.

Proposal: Event: “Archives and Reporting”, organized jointly with the National Security Archive at George Washington University.

Year: 2010

Description: This is an electronic magazine looking for data transparency, aside from publishing documents related to personal data protection. The Nuevo Leon Commission for Access to Public Information sponsors it.

Scope of incidence: The use of technologies and personal data protection.

Agent: **Puebla State University**

Kind/Modality: Public, university.

Proposal: To publish a specialized article on personal data protection legislation on its web site.

Year: 2010

Description: This is Puebla State University’s official web page, belonging to its Direction of Institutional Communications, which is in charge of making public all activities and concerns of its student body.

Scope of incidence: Personal data protection and science sharing.

Agent: **Federal Institute for Access to Information (IFAI)**

Kind/Modality: Public, institution

Proposal: VIII Ibero-American Encounter on Data Protection, Mexico City, 29 September 2010.

Year: 2010

Description: A series of conferences was organized. Amongst the best is that of Chantal Bernier on personal data protection in the digital age.

Scope of incidence: Internet, the use of technologies, vulnerability.

Agent: **Nuevo Leon State University**

Kind/Modality: Public, university.

Proposal: A data protection panel took place, called “Perfectible, the data protection system.”

Year: 2010

Description: The main subject in this panel was the reform to the Federal Law of Personal Data Protection, [which] has been given neither divulgation nor importance.

Scope of incidence: Divulgation of the issue of personal data protection

Agent: **Civic Alliance, building an active citizenship.**

Kind/Modality: Public, civic association

Proposal: To define personal data that are protected by the law

Year: 2010

Description: [The association] held a training course in Sonora on the subject of personal data protection.

Scope of incidence: Personal data protection, opinion, and participation.

Agent: **Mercedes Benz**

Kind/Modality: Company

Proposal: Mercedes Benz set up a section in its web page where it discloses what treatment your personal data will be given, upon entering the site.

Year: 2010

Description: It makes clear that personal data are handled in accordance to the law when making any transaction.

Scope of incidence: Personal data protection, security.

Agent: **PC World**

Kind/Modality: Private, portal

Proposal: It announced an article through its web page showing ten forms of safely navigating the Internet.

Year: 2010

Description: This is an online portal that allows the making of safe and timely decisions. Aside from offering a rapid access to the contents of the magazine, it also gathers a series of services aimed at helping to find answers to most frequent issues that arise upon working with a computer. Due to the fear of security when navigating, ESET lets users know of ten simple steps for navigating safely. Some of the most important are: to avoid suspicious links, not to go into dubious web sites, not to share important personal information in doubtful forms, and to only accept invitations from known contacts.

Scope of incidence: The use of technologies, security.

Agent: **National State University of Mexico (UNAM) - CERT**

Kind/Modality: Public

Proposal: UNAM-CERT is a team of computational security professionals. Aside from providing a response to computing security incidents to sites that may have fallen victims of an attack, as well as publishing information with respect to security vulnerabilities, it produces alerts as to those effects, and makes investigations in an ample range of computing, thus helping to make web sites more secure.

Year: 2010

Description: This is a team whose purpose is to aid in the security of sites that may have been under attack.

Scope of incidence: Personal data protection, security, and cyber attacks.

Agent: **Office of Information Security. UNAM.**

Kind/Modality: Public

Proposal: To let people know computing protection schemes.

Year: 2010

Description: It gives aid when incidents arise, elaborates bulletins on computing security, and designs security schemes.

Scope of incidence: Security

Agent: **Habeas Data**

Kind/Modality: Public

Proposal: It announces that Mexico will be home to the conference of commissioners on data protection.

Year: 2010

Description: Habeas Data is the foremost organization of privacy professionals in Latin America. It is dedicated to incentivizing and boosting conscience on Personal Data protection in Argentina and Latin America. It holds around 600 documents including laws, norms, bills, jurisprudence, articles, news, seminars, and conferences. Among the articles found, one says about: Announce on the next big event in favor of personal data protection.

Scope of incidence: Personal data protection.

Agent: **E-nnovative**

Kind/Modality: Enterprise

Proposal: To create awareness on the issue of exclusion through Internet

Year: 2010

Description: This is a Mexican enterprise dedicated to the development and design of web pages. It offers the tools necessary to keep your computer up to date. Within this web page, there is a blog that contains articles related to technology such as the following: Analyze how the Internet, aside from being a vehicle for establishing relations, can also exclude and it uses the example of IRS tax returns.

Scope of incidence: Violence, Internet, exclusion, and technologies.

Agent: **Civic city**

Kind/Modality: Public; blog

Proposal: It analyzes the information technologies and how they have prompted social exclusion.

Year: 2010

Description: Ciudad Viva is an initiative of the HOUSING AND PUBLIC WORKS COUNCIL, which adheres within a political project to improve urban living. It deals with the enhancement of the neighborhoods, key elements of connection with people living in cities.

Scope of incidence: Social exclusion, technologies.

Agent: **Diario crítico de México**

Kind/Modality: Public, editorial group

Proposal: It publishes news on technology and social exclusion.

Year: 2010

Description: This is an editorial group publishing articles on all matters, aside from being in various countries, from Spain to Latin America.

Scope of incidence: Social exclusion, the use of technology.

Agent: **Culture for all**

Kind/Modality: Public, blog

Proposal: It follows the advances in technology and how they help culture and thus to achieve a more fair and equalitarian society.

Year: 2010

Description: This is a blog in favor of equal access to culture, without exclusion. The purpose of this inclusion bill is to achieve accessibility by those with some form of handicap, this way guaranteeing a culture for all.

Scope of incidence: Inclusion, access to information.

Agent: **Personal data protection.**

Kind/Modality: Public, foundation and profile.

Proposal: This is a foundation in favor of personal data protection, which has established a Facebook group with the purpose of informing, educating, and positioning within the public debate the issue of personal data protection in Chile and abroad.

Year: 2010

Description: This page by the foundation of the same name informs and educates on the relevance that must be given to the matter of personal data protection. By being in Facebook, it pretends to inform the young and adults in general on the importance of this issue.

Scope of incidence: Personal data protection.

Agent: **Privacy International**

Kind/Modality: Public

Proposal: This organization holds international campaigns in favor of privacy since 1987.

Year: 2010

Description: Privacy International is a non-governmental organization with the main function of promotion and support. Its objectives are: to create awareness and to educate on the threats to personal privacy, in order to control the nature, efficacy, and the reach of the measures taken to protect privacy and personal data, to manage research on threats to personal privacy, to control and to inform on the supervising activities of the security and intelligence forces. This year, its campaigns, its activity through the media, and its projects follow up on its continuing promotion of privacy rights in the developing countries.

Scope of incidence: Personal data protection, privacy.

Agent: **CSO, Spain**

Kind/Modality: Public, blog.

Proposal: This blog contains news for security within the cyberspace, such as: “Social feeds: benefits and risks for data privacy”

Year: 2010

Description: It makes public various subjects in relation with th protection of personal data and privacy in the Internet.

Scope of incidence: Personal data protection.

Agent: **Salomon**

Kind/Modality: Public, editorial group.

Proposal: This group publishes articles where concerns are exposed over the lack of organization and of legislation on personal data.

Year: 2010

Description: In an article they talk about the deficiencies in data security matters in the USA, and the relation that may exist with Spain for 2011, where a new legislation for data protection hints at potentially high costs [in fines] for those companies that infringe data protection laws. Some of the most relevant data protection subjects for 2011 in the USA are: low-tech information theft may continue, we may see a rise in the loss of information as a consequence of a loss of electronic equipment, the gathered information may tend to be minimized in order to lower the amount of information lost.

Scope of incidence: Personal data protection.

Agent: **Digital politics**

Kind/Modality: Public

Proposal: It promotes the correct use of technologies of information and communication for [maintaining a high] quality in public institutions of the three powers of state, at federal, state, and municipal levels.

Year: 2010

Description: This is an article on the matter of state public health services where a proprietary medical file system –in Sinaloa, for instance– has helped in keeping a greater amount of information on patients and illnesses. This pilot project may be of benefit in the sense that we may be able to communicate hospitals and clinics in an effort to develop a common strategy in electronic health care.

Scope of incidence: The use of technologies.

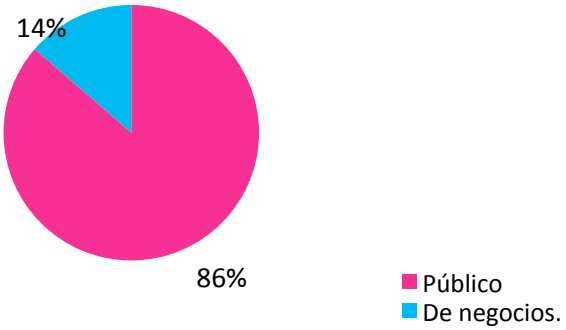
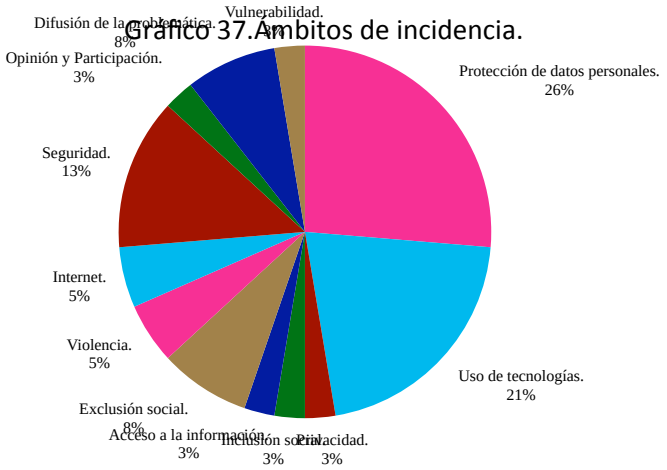


Gráfico 37. Ámbitos de incidencia.



The production of information on the matter might seem to come from public agents as a result of their modality. This is, the set up and update of various blogs, web pages, civic association portals, editorial groups, etc., take place as per the contributions of those individuals interested in the matter. However, the debate in Mexico on the protection of personal data continues to be rather volatile. Data indicate that the debate is intensely heterogeneous in the definition and approach to the issue.

iii Technologies and Normativity. The protection of personal data in Mexico

Following the theoretic model proposed for the identification of the typology in constitutional systems in the matter of informational rights,[64] constitutional recognition of the protection of personal data may be known attending to two constitutional groups. In the first one, we find those paradigmatic constitutions, having incorporated a constitutional clause in relation to the recognition of the protection of personal data, the right to informative self-determination or informatics rights; thus excluding its proclamation and recognition as a right derived from intimacy and private lifestyle. In the second group of fundamental laws, those rather minimalistic and old-fashioned are assembled, since the protection of data is not recognized as an autonomous right but rather considered by the judicial order as a right derived from personal intimacy, due to which its protection is developed through one or more particular ruling laws.

In as much as concerns us here, it is important to indicate that the paradigmatic nature of those constitutions that recognize the protection of personal data as an autonomous right, and the *Habeas Data* as its *ad hoc* judicial mechanism, is due to that they are identified with constitutional and democratically constituted States, or else with national States resulting from a political-institutional rupture.

As a consequence, the recognition of personal data protection as such or else named differently from the rights to intimacy and private lifestyle, is found as a fundamental right in the constitutional texts of: Albania, Argentina, Armenia, Azerbaijan, Bolivia, Brazil, Cabo Verde, Colombia, Swiss Confederation, Croatia, Ecuador, Slovakia, Slovenia, Spain, Estonia, Russian Federation, Finland,

[64] The model is based on the observance to the rules of recognition of freedoms and rights. Hence there are, in this typology: 1. Constitutions that do not contain provisions with respect to those freedoms and rights; 2. Constitutions that do not protect or else do not recognize those freedoms and rights, or that without doing it delegate their regulation on particular laws; 3. Old fashioned constitutions (19th c.), thus called because of the recognition to those freedoms and rights, but in a generic way, i.e. stemming from classical theoretical perceptions; 4. Minimalist constitutions, which aside from recognizing freedoms and rights in an informative way, they grant the individual a minimum of possibilities for their participation in public affairs; 5. Quasi-paradigmatic constitutions that allow for the exercise of freedoms and rights, and the incorporation of institutions that permit the exercise of democracy, and 6. Paradigmatic constitutions, so called because aside from making freedoms and rights constitutional, they also introduce institutions for their strengthening, as is the case in the introduction of judicial guarantees ad hoc. Cfr. Villanueva, Ernesto. Derecho comparado de la información, Universidad Iberoamericana-Fundación Konrad Adenauer, México, 2002, pp. 31-33.

Gabon, Georgia, Guatemala, Hungary, Kazakhstan, Macedonia, Moldavia, Nicaragua, Netherlands, Paraguay, Peru, Poland, Portugal, Czech Republic, Romania, Serbia and Montenegro, South Africa, Sweden, Ukraine, and Venezuela.

Parallel to their recognition, in the fundamental charters of Bolivia, Brazil, and Cabo Verde a constitutional mechanism has been instituted for their protection and effective promotion, called *Habeas Data*.

Before going on to relate the evolution of the right to informative self-determination in the international sphere, it is relevant to point out that there is a variety of personal data. In this sense, the term *personal data* refers to all kinds of information related to the person identified or identifiable, such as that on their ethnic origin; or that making reference to their physical, moral, or emotional characteristics, to their family or affective lifestyle, to their address, telephone number, assets, ideology and political views, religious and philosophical beliefs and convictions, mental and physical health states, sexual inclination; or any other similar characteristics that may affect their intimacy, whether public or private, and that may be or may have been manually or automatically processed.[65] As may be seen, the risk to which human dignity is exposed, confronted by a diversity of data processing techniques, renders them sensitive, that is, considered as "… *information whose contents pertain private matters and whose general recognition may be a generator of detriment or discrimination.*"[66]

Thus, there is coincidence with the thesis that maintains that a personal data on its own does not have any value, but that it gains it when linking it to others that might allow for the identification of an individual.[67] This amply states the risk of exposure for an individual's privacy and intimacy, due to the latent threat inherent to the informatization of activities. The silent supervision that takes place of an individual's steps is, before the enemies of democratic life, the argument that allows the foundation of the State interest in the elaboration of policies and norms for the protection of

[65] It is worthy to add to the concept of personal data the implication of their termination o their transfer to third parties. To that respect vid. Messía de la Cerda Ballesteros, Jesús Alberto. La cesión o comunicación de datos de carácter personal, Thomson-Civitas, Madrid, 2003.

[66] Pierini, Alicia. op. cit. supra, p. 25.

[67] Cfr. Riande Juárez, Noé Adolfo. ¿Por qué debe legislarse en México en materia de Protección de Datos Personales Automatizados? *(Why must there be a legislation in Mexico with respect to the Protection of Automatized Personal Data?)* Address presented in the 8th Ibero-American Congress on Law and Informatics, on 21-25 November 2000 at the Mexico State Campus of the Tecnológico de Monterrey. The author says that: *When the intention is to respect data as it is linked to an inventory, to a payroll, or to statistics, not caring for its relation to people, what is being protected is the service or the good performance of an administrative or productive mechanism but not the people in their intimacy, in their dignity, their integrity or their freedom.* Likewise vid. the verdict by the Spanish Supreme Court on *Protection of personal data. Extent of the expression "personal data". Data of personal nature: Classes. Request to the General Vehicles Department on the ownership and loads of the vehicles registered under certain names. Personal data not accessible to the public. Correct negation.* In it the Court established that: *The expression "personal data" is not synonymous of "data of personal nature" because not always an information is personal in nature and because, furthermore, there are data of a personal nature which are not personal data.* Cfr. Amadeo Gadea, Sergio Luis. Informática y nuevas tecnologías, LA LEY, Madrid, 2001, pp. 9-10.

national and international security, as much as it can be used to weaken and undermine the values of freedom and dignity of the individual. [68]

On the other hand, the origin of the prerogative for accessing information in Mexico goes back to the constitutional reform of 1977. In it, ten words were added to the final part of Constitutional Article 6 to establish: *The right to information will be guaranteed by the State*.

Within the framework of the so-called *political reform*, fostered by then President José López Portillo, there was an intention of allowing for the political parties the access to mass communication media, that is, to the age of radio and television. [69] In the speeches given before the Congress, *"… the relation between the right to information and the democratic and electoral game was highlighted, since only they who are informed may opt consciously, and not those who are swayed or disoriented; then, the right to information is demanded through the State in order to make democracy possible."* [70]

In principle, the Political Constitution of the United States of Mexico recognized the right to intimacy and to privacy within the scope of the personal, familiar, and of the properties and assets

[68] This tendency to the humiliation and the contempt for the freedom and the dignity of a person has become more widespread after the terrorist attack on the Twin Towers at the World Trade Center (WTC) in New York on 11 September; as a consequence, certain security enforcement measures were implemented at the international airports in many cities around the world, so that the Transportation Security Agency agents could search the luggage, documentation, and identity of all passengers flying to the USA.

[69] In the Statement of Motives that accompanied the Initiative of reforms and additions to the Political Constitution of the United States of Mexico, introduced by the Federal Government, it was considered that: The nature of public interest recognized to the political parties in the initiative makes it necessary to confer on the State the obligation of securing the conditions for their development, and of favoring and supplying the basic elements that they might require in the actions destined to gathering civil adhesion. It is also necessary to guarantee in an equitable manner the means for the national political parties to amply spread their principles, theses, and programs, as well as the analyses and opinions that may be formulated with regards to the issues of society. To that end, it is deemed convenient to establish as a prerogative of the political parties their permanent access to radio and television, without restricting it to election periods. This prerogative of the political parties has the purpose of perpetuating in a more effective manner the right to information, which with this initiative is included into the sixth article of the Constitution and which will be basic for the improvement of a civic conscience and will contribute to making the latter more informed, vigorous, and analytical; which is essential for the progress of our society. Since the political parties are essential in the ideological and political action, the exercise of their right to disseminate their ideas through the media will translate in a greater respect to ideological pluralism, and the freedom of expression and its correlative right to information will be plentiful.
On the other hand, the diversity of opinions expressed regularly by the political parties in media as relevant as are the radio and the television, added to the other means for generating information, will contribute to make it more objective and to better integrate the public opinion once the latter is enriched by a greater variety of criteria and viewpoints. Cfr. Comisión Federal Electoral. Reforma Política; Gaceta informativa de la Comisión Federal Electoral, Tomo III, México, 1978, p. 12. This is how the Right to Information had been initially understood by the Supreme Court when it issued the isolated thesis of jurisprudence P. LXXXIX/96, under the Description: Individual guarantees (Right to information). Grave violation in a provision set in the second paragraph of Article 97 of the Constitution. It is configured by the attempt to achieve impunity of the authorities that act within a culture of deceit, of machinations, and of concealment, through the infringement of Article 6 of the Constitution, which was augmented by the diverse isolated thesis P. XLV/2000, under the Description: Right to Information. The Supreme Court originally interpreted Article 6 of the Constitution as a guarantee of the political parties, later expanding this concept to individual guarantee and the obligation of the State to inform truthfully.

[70] Carpizo, Jorge. Nuevos Estudios Constitucionales, Porrúa-UNAM, México, 2000, p. 401.

(residence and documentation)[71] and of the private communications.[72] Of the first of those, we can say that it was conceived in conformance to the arguments and concepts that have informed liberal constitutional texts; with respect to the second, it is necessary to point out that it is a right that derives from the latter one, but its purpose is to protect the privacy in communications, corresponding its configuration with the Human Rights of third generation.

Chronologically, Mexico can be identified as a country that up to the year 2002 could be considered old-fashioned in terms of personal data protection, since the protection to freedom of information was considered as an extension of the rights to intimacy and private life, and its protection took place through a series of particular judicial norms.

With the purpose of evening up criteria on transparency and the access to information at a national level, on 13 December 2006 the governors Luis Armando Reynoso Femat of Aguascalientes, José Reyes Baeza Terrazas of Chihuahua, Fidel Herrera Beltrán of Veracruz, Amalia García Medina of Zacatecas, as well as Alejandro Encinas Rodríguez from the Federal District, submitted before the Congress an initiative of reforms and additions to the Political Constitution of the United States of Mexico which was welcomed by the leaders of all political parties represented in the Low Chamber and consequently was introduced before the House on 19 December 2006.

The *Chihuahua Initiative*[73] –as it was colloquially known– proposed to reform the sixth constitutional article "*… in order to broaden the reaches of the right to information at all levels of government and the political parties.*"

[71] Thus, Article 16 of the Constitution, in its first paragraph, establishes that: No one individual can be molested, nor their family, home, documents, or possessions, except through a written warrant from the corresponding authority that could give the basis and motivation of the legal cause for such a procedure.

[72] In the twelfth paragraph of Article 16 (previously ninth paragraph), it is established that: The private communications are inviolable. The Law will sanction any act attempting against the freedom and privacy thereof. Only a federal judicial authority, on request by a federal authority accredited by the law or else the head of the Public Ministry in the corresponding federative entity, will be able to authorize the intervention of any private communication. To that effect, the competent authority will have to base and motivate, in writing, the legal causes of the request, expressing also the kind of intervention, its subjects and its duration. The federal judicial authority shall not grant such authorizations when the subject matter is electoral, fiscal, mercantile, civil, labor, or administrative in nature; nor in the case of communications held between a detainee and their defense attorney.

[73] The genesis of this initiative is in the so-called *Guadalajara Declaration* signed on 22 November 2005.
Complementarily, the *Mexico Declaration*, stemming from the work carried out in the *Fourth Ibero-American Encounter for the Protection of Personal Data* (2005) concluded: 1. To assume that the protection o personal data is a fundamental autonomous right. 2. To assume and to take into consideration the implication of personal data in the telecommunications and in the implementation of the electronic government. 3. It is necessary to study the normative development and the globalization in the area of marketing, the financial sector, and the international data transfer. 4. To assume health data as especially protected. 5. It is necessary to have a law for the protection of data, considering the internationally recognized principles in public and private entities.

With respect to the protection of personal data it proposed: *The information concerning private life and personal data shall be considered as confidential and it shall be of restricted access in the terms granted by the law.*

The proposal of "constitutional change" made by the governors considered that personal data, aside from being confidential, should also be of restricted access. Such an argument implies, in principle, that all personal data are confidential by antonomasia, which inhibits the possibility of issuing a particular law to regulate diverse categories of personal data and; secondly, in establishing that access to all personal data should be restricted would in turn provoke a weakening of some important public institutions such as the Public Property Registry, Commerce Registry, Civil Registry, etc. [74]

After the painstaking labor that a constitutional reform entails, on 20 July 2007 the official Journal of the Federation published the Decree by which a second paragraph was added, with seven section, to the Sixth Article of the Political Constitution of the United States of Mexico.

Particularly, in sections II and II it was established that information that refers to private life and all personal data are protected in the terms and with the exceptions fixed by the laws; and that every person, without the need of crediting any interest or of justifying its use, shall be granted free access to public information, to their own personal data, and to the correction of these.

However, the legislative process of reforms to the constitution has eased the incorporation and extension of the right to the protection of personal data into the scope of the penal process and when its possession is in the hands of individuals.

[74] On this particular matter, the United Commissions on Constitutional Points and the Public Function of the Chamber of Deputies of the Congress of the Union, in the sentence through which they perfected and approved the *Chihuahua Initiative*, established:
"…a second limitation to the right of access to information is established, as it refers to the protection of private life and of the personal data. This information can not be subject to the principle of publicity, since it could pose serious danger for another fundamental right, that of intimacy and private life. It is fundamental to clarify that even though they are intimately related, there must be no confusion between private life and personal data. The first refers to the realm of privacy of the person with respect to the intervention from the state or from other entities. Personal data, on the other hand, are an expression of privacy.
The second section establishes also a reservation of the law in the sense that it will correspond to the law to determine the terms of the protection and the exceptions to that right. It is thus perfectly possible to consider that certain private information or personal data, when gaining a public value, could be published through the mechanisms that the law determines. This is the case, for instance, of the public registry of the property, the income of the public employees, or the regulation of the exercise to consent by the owner of the information for it to be divulged. In other words, there are circumstances in which, through the ministry of the law, personal data could be made public without the consent of their owner.
In other cases, the law will provide the possibility that some personal data may be divulged when a jurisdictional or administrative entity determines that there are particular reasons to justify their public release, with the previous guarantee of audience to the one implicated. At any rate, the authorities shall ponder carefully so as to justify the fact that information that belongs to the private realm should be divulged because of convenience to public interest."

To this effect, the reformulation of the penal code in 2008 brought along its establishment as a process of accusatory and oral orientation by the Political Constitution of the United States of Mexico; and by being governed by the principles of publicity, contradiction, concentration, continuity, and immediacy, it recognizes for any victim or offended party the right to conceal their identity and other personal data in the following cases: when they are minors; when dealing with the crimes of violation, abduction, or organized crime; and when the judging party deems necessary for the protection of the defendant, safeguarding at all times the rights to defense.

In spite of this, the Congress of the Union observed that from the constitutional standpoint it was not enough with the scope of coverage of personal data as foreseen by the sixth article, since it was necessary to also protect the personal data owned by individuals, as well as to extend the right that everyone has to the protection of their personal data, to the access, correction, and cancellation thereof; as well as to manifest opposition in the terms fixed by the law, which establishes the basis of exception to the principles governing the treatment of data, due to reasons of national security, public order decisions, public security and health, or to protect the rights of third parties.

In this sense, section XXIX-O of constitutional article 73 was added, as well as a paragraph to article 16.

From a prospective viewpoint, it is evident that the legislative work carried out by the Congress of the Union not only waged the international experience in the matter; it must be considered also as a stimulus for the discussion, approval, and issue of a Federal Law of personal data protection in possession of individuals,[75] aside from broadening the denomination of the Federal Institute of

[75] We must point out that at federal level there are seven bill initiatives for the issue of regulatory norms to personal data, out of which five are aimed at the issuing of a Federal Law for the Protection of Personal Data.
Deputy Luis Miguel Barbosa Huerta introduced the bill initiative for the Federal Law for Electronic Signature and Commerce, Text Messages and Services of the Information Society, which was dictated and approved in the Chamber of Deputies with 422 votes in favor and one abstention, on Tuesday 26 November 2002; dictated and approved by the Senate with 84 votes in favor, on Tuesday 8 April 2003 and therefore turn in to the Federal Executive government for the corresponding constitutional effects (Parliamentary Gazette, number 999, Tuesday 14 May 2002; available at: http://gaceta.diputados.gob.mx/Gaceta/58/2002/may/20020514.html#Ini20020514Barbosa).
Deputy Jesús Aguilar Bueno, from parliamentary group of the Institutional Revolutionary Party (PRI), introduced on Thursday 7 October 2004, the bill Initiative to reform the Federal Penal Code in the matter of child pornography, corruption of minors, communication and correspondence, revelation of secrets, and illegal access to computing systems and equipment, general forgery of documents, threats and disclosure of personal data, crimes against individuals in their patrimony; the Federal Penal Procedures Code in the matter of the securement of the defendant and confrontation, as well as the Federal Law Against Organized Crime, in the matter of the nature, object, and application of the law (Parliamentary Gazette, number1600-I, Thursday 7 October 2004; available at: http://gaceta.diputados.gob.mx/Gaceta/59/2004/oct/Anexo-I-07oct.html).
1. Senator Antonio García Torres, from the PRI parliamentary group, in session of the Permanent Commission on Wednesday 14 February 2001 (Parliamentary Gazette, number 688, Thursday 15 February 2001; available at: http://gaceta.cddhcu.gob.mx/Gaceta/58/2001/feb/20010215.html).

Access to Public Information, the reform also amplified its faculties so that other than overseeing the promotion and spread of the right to information and resolving over the negation to the requests for access to information and protection of personal data under the custody of government offices and entities, it may also widen the knowledge of the rights to protection of personal data among the Mexican society, as well as promote its exercise and supervise all due observance to ordinances related to the protection of personal data kept by credit information societies and those individuals with the task of collecting and storing persona data, exclusively for personal use, and without intention of public divulgation or commercial use.

From another standpoint, it must be considered that it also placed the protection of personal data in its rightful constitutional place. [76]

---

2. Deputy Miguel Barbosa Huerta, from the Democratic Revolution Party (PRD), in session of Thursday 6 September 2001 (Parliamentary Gazette, number 832, Friday 7 September 2001; available at: http://gaceta.cddhcu.gob.mx/Gaceta/58/2001/sep/20010907.html).

On account of this, a Minute was turned over to the Chamber of Deputies, with the previous approval on he part of the Senate, with a degree bill through which a Federal Law for the Protection of Personal Data is issued; the former being as of yet under study by the Governance and Public Security Commission of the Chamber of Deputies (Parliamentary Gazette, number 1082, Thursday 5 September 2002; available at: http://gaceta.diputados.gob.mx/Gaceta/58/2002/sep/20020905.html#Minuta20020905DatosPersonales).

In conformity with this, Senator García Torres introduced before the Senate an initiative of reform to Article 16 of the Political Constitution of the United States of Mexico with the object of guaranteeing for every person the right to protection and the access to their own personal data (Parliamentary Gazette, number 692, Wednesday 21 February 2001; available at: http://gaceta.cddhcu.gob.mx/Gaceta/58/2001/feb/20010221.html#Ini20010221Antonio).

Throughout the year 2005, there was high expectation with regards to the approval of the Minute with the decree bill through which the Federal Law for the Protection of Personal Data is issued; however, political differences within the Chamber of Deputies, but particularly because of the considerations argued by the united Commissions of Governance and Economy in the *Draft of decision with modifications of the united Governance and Economy Commissions on the minute with Decree bill through which the Federal Law for the Protection of Personal Data is issued.* [sic: unfinished idea]

3. However, Deputy Jesús Martínez Álvarez, from the Convergence parliamentary group, submitted for consideration before the Chamber of Deputies the Initiative bill for the Federal Law for the Protection of Personal Data (Parliamentary Gazette, number 1895-I, Thursday 1 December 2005; available at: http://gaceta.cddhcu.gob.mx/Gaceta/59/2005/dic/Anexo-I-01dic.html#Iniciativas).

Senate

4. For his part, Deputy David Hernández Pérez, from the Institutional Revolutionary Party (PRI) parliamentary group, submitted another Initiative bill for the Federal Law for the Protection of Personal Data (Parliamentary Gazette number 1953-I, Thursday 23 February 2006; available at: http://gaceta.cddhcu.gob.mx/Gaceta/59/2006/feb/20060223-I.html#Iniciativas).

5. Deputy Sheyla Fabiola Aragón Cortés, from the National Action Party (PAN) parliamentary group, submitted another Initiative bill for the Federal Law for the Protection of Personal Data (Parliamentary Gazette number 1972-I, Wednesday 22 March 2006, available at: http://gaceta.cddhcu.gob.mx/Gaceta/59/2006/mar/20060322-I.html#Iniciativas).

Finally, we must credit the initiative through which sub-section N) is added to section 29 of Article 73 of the General Constitution, with the purpose of granting attributions to the Congress of the Union for the legislation in the matter of the protection of personal data in the custody of individuals, submitted by the deputies Luis Gustavo Parra Noriega, María del Pilar Ortega Martínez, Rogelio Carvajal Tejada, Dora Alicia Martínez Valero, Esmeralda Cárdenas Sánchez, and Jesús de León Tello, members of the PAN parliamentary group.

[76] Prior to the constitutional reform of July 2007, the States of Morelos and Mexico constitutionalized the right to the protection of personal data.

Through Decree number 1069, published in the Official Journal on 11 August 2003, Article 23-A was added to the Political Constitution of the Free and Sovereign State of Morelos; said precept establishes that the State Congress will establish an autonomous organism for the custody of the right of access to the public information of all individuals, to protect personal data, and to make impartial statistics, surveys, and polls that may help in the compliance of the functions of the public powers and to the democratic development of the State, called Morelian Institute of Public Information and Statistics.

In spite of the constitutional recognition granted to information relative to private life, and of the incorporation of the right to the protection of personal data as autonomous fundamental rights, a normative system was previously configured, composed of a catalog of laws and regulations through which personal data are protected. Nowadays, there is a Federal Law of Transparency and Access to Governmental Public Information as well as 30 state transparency laws, a variety of municipal regulations and a number of others corresponding to constitutional and constituted autonomous organs of the State.

Hence, it is possible to report the existence of judicial provisions that regulate personal data in fields such as: the exercise and protection of political-electoral rights of the citizens, the electronic commerce, fiscal and credit areas, statistical and geographical information, labor, automotive control, population identification, health, copyrights, telecommunications, private sector controls, among others. [77]

Aside from that normative cast, there are other regulations contained in International Treaties, secondary laws, regulations of constitutional precepts, codes, regulations, agreements, definitions, etc.; which exert an enormous influence in the conformation of a judicial framework for the protection of personal data, which in turn is accompanied by an aggressive policy of transparency, reporting, and access to the information.

A special relevance have gained the international obligations acquired on the matter by Mexico, amongst which, those derived from the *Economic Partnership, Political Coordination and Cooperation Agreement between the United States of Mexico and the European Community and its Member States, the Decision of the Joint Council of such Agreement; and the Decision of the Joint Council for the Interim Agreement on Commerce and Matters Related to the Commerce between the United States of Mexico and the European Community*, on 8 December 1997; which could be considered a Free Trade Treaty between Mexico and the Member States of the European Union. [78]

On the other hand, through Decree number 44, published in the Government Gazette on 30 April 2004, two paragraphs were added to Article 5 of the Political Constitution of the Free and Sovereign State of Mexico, in which primarily a guarantee to protection, respect, and divulgation of the public information is established; and secondly, public powers and autonomous organs are obliged to making their actions transparent, to guarantee the access to the public information, and to protect personal data in the terms defined by the regulatory law.

[77] On the issue Cfr. Piña Libien, Hiram Raúl. El derecho a la autodeterminación informativa y su garantía en el ordenamiento jurídico mexicano, Instituto de Transparencia y Acceso a la Información Pública del Estado de México, México, 2008.

In a similar orientation Gómez-Robledo, Alonso y Ornelas Núñez, Lina. Protección de datos personales en México: el caso del Poder Ejecutivo Federal, UNAM, México, 2006.

[78] Cfr. Decreto Promulgatorio del Acuerdo, published on the Official Journal of the Federation on 26 June 2000; as well as the Official Journal of the European Communities on 28 October 2000 L 276/45.

In said Agreement, the information and communication technologies are recognized as one of the key sectors in the development of the SI, as well as of the economic and social development. To that effect, the Mexican government and the member states of the European Union are committed to carrying out various joint actions such as the establishment of dialog on cooperation in relation to current regulations for online services, including such aspects as those pertaining the protection of privacy and of personal data; as well as to promote the reciprocal access to data bases, in the terms agreed upon.

Therefore, in articles 41 and 51 of the Treaty, there is in first place an agreement for cooperation for achieving and improving the levels of protection, and to prevent the obstacles to exchanges as may be required by the transfer of data of personal nature. Secondly, to guarantee a high degree of protection with respect to the treatment of personal data and data of other kinds, in compliance with the norms adopted by the specialized international organizations and by the Community. Said norms are detailed in the Appendix to the Agreement and are: the Guidelines for the regulation of personal data computerized files, modified by the UN General Assembly of 20 November 1990; the Recommendation by the OECD Council on the guidelines to which the protection of privacy and the personal data flow across borders abide, from 23 September 1980; the Council of Europe Agreement on the protection of the individuals with respect to the automatized treatment of personal data, from 28 January 1981; and Guideline CE/95/46 of the European Parliament and of the Council, on 24 October 1995, in relation to the protection of the individuals in as much as pertains the treatment of personal data and the free circulation of these data.

As can be seen, Mexico must not only comply with its obligations in the matters addressed in the text of the Agreement, but also with the contents of other international decisions stemming from the forums of which it is a member state; alas, to comply with the decisions made by the European Union in the context of personal data protection. That is, with the requirements and demands set forth in Guideline 95/46/CE, concerning the observance to the leading principles of the freedom of information.

This would hardly transcend, were it placed in the simple terms of compliance with the international obligations acquired; however, the transcendence accompanying the application of Guideline 95/46/CE does not lie on the mere compliance to obligations, but rather on the incorporation of Communitarian Legislation in the sphere of a third country's internal Legislation. In other words, the incorporation in the Mexican Legislation of European Union Legislation, of the supra-nationality of which the latter takes advantage in order to gain validity, application, and harmonization.

6. CONCLUSIONS

The initial purpose of this project was to carry out a first stage in the promotion of a public debate, as well as influence in public policies, with respect to the protection of personal data in Latin America. In this first stage, the project has been narrowed to two countries: Brazil and Mexico, and there was an intention of identifying the main institutional, legal, academic, social, and technological figures around three subjects: a) National identification documents, b) video-surveillance in public spaces, and c) the Internet.

After a detailed presentation and organization of the data supporting the research done in both countries, which was described in the previous sections of this report, we now try out some important conclusions from this investigation. These conclusions have been organized in two ways. Firstly, analyzing the results gathered from the studies by subject and by country (subjects "a" to "f"). And, finally we highlight some general considerations for each country, described from the perspective of a comparative analysis that might help as a starting point for future international studies, particularly with the participation of other socio-economic and cultural contexts from Latin American countries.

a) About the proliferation of CCTV in Brazil

Some aspects must be recalled and pointed out after the surveys carried out for this initial mapping of the proliferation of CCTV in Brazil. First of all, we must take into account that, as mentioned before, this is a preliminary study: it has the intention of marking the first systematic approach on the subject in Brazil, with an ample collection of data and a restricted qualitative in-depth view of the implications and repercussions of the main tendencies observed. Nonetheless, it is valid to remember the continental dimensions of both countries, mainly Brazil, which made for the territorial approach to be narrowed to three states plus the Federal District, and their capitals.

In the case of CCTV systems, there is a clear perception of a growing interest in the subject and, mainly, in the continually broadening application of supervision cameras and the integrated systems, with a growing and structured market at various levels (from multinational companies to small and medium sized local monitoring and security firms), as well as a growing interest within the real estate market in issues of assets security, working as a leverage for the growth and commercialization of electronic surveillance equipment, especially in the popularization of these systems and the small-scale commerce.

Large and small companies coexist in what international entrepreneurship reports call an ecosystem of suppliers, thus stimulating the market and showing Brazil as: a) a challenge for international enterprises not yet established in the country, since they would have to adapt themselves to a more disputed competition due to an already established marketing structure; b) and as an image and example of the great mercantile potential for Latin America, especially about the other countries, for CCTV equipment and technologies and image-based monitoring. Therefore, Brazil's relevance in the international interest for CCTV firms is high, in relation to technologies and marketing, making it fertile for future and massive investments, particularly if taking into account the two large-scale events the country will be hosting over the next couple of years: the World Soccer Football Cup in 2014 (with direct impact in various regional capitals) and the Olympic Games of 2016 (with a specific impact in the region around Rio de Janeiro). In this specific case, there is intense debate on the political scene, in the academia and in the media, over the real implications of these large-scale sports events for Brazil and the involved regions. There is much criticism over the possible negative development of certain aspects, such as the use of public resources on construction for the events, the impact of public policy on areas such as urban infrastructure and social housing, the relation between local political institutions and the international institutions responsible for the events (such as the FIFA and the International Olympic Committee), and finally in relation to the monitoring and security structures installed on demand of the events.

It is evident, also, that there is a growing scientific interest on the matter, showing the potential for debate around the subject of CCTV in the Brazilian academic sphere. In this aspect, the predominance of academic work is to be highlighted (dissertations, term papers, theses) over the presence of newspaper articles and works on events as a proof, on one hand, of the initial broadening stage in higher education of the study on surveillance and, on the other, a significant process of formation and training of professionals, teachers, and doctors with research in areas correlated to imaging electronic surveillance, CCTV, video surveillance, etc.

It is clear, as well, the contradictorily opposed moment shown by the Brazilian judicial scene in the states and capital surveyed, where little or no attention is given to the discussion of actions and implications of the video surveillance, as well as to the nature of the situations in which this activity takes place. There is barely a latent, rather instrumental, concern with the application of video surveillance in the monitoring of individuals and groups in public and private spaces. Such a scenario is no different from the specific legislation on the other two great subjects in the present work, as will be seen below.

Finally, it is necessary to limit the worrisome forecast obtained from this mapping. In spite of the stimulant growth in the number of studies/research related to the subject of CCTV in Brazil in the last few years, and of the important evolution in the interest for the matter experienced in the academic environment in the country, one can perceive a certain irregularity between the organization of the market and the low degree of participation from the society in the debate on the

matter reflected on the construction of a legislation. There is, on one hand, a high esteem of the security and, consequently, of the whole technological apparatus as destined to the matters of security of the estates and personal with a market that is prepared to cover the demand and, on the other hand, a judicial environment that is unconcerned with the understanding of the logics of the growth in CCTV installations and their possible implications in relation to privacy, individual rights and the configuration of spaces in the cities.

b) About the national identification document in Brazil

With respect to the matter of Civil Identity Registry (TIC) in Brazil, there are 24 legislators, linked to 53 documents (law proposals, laws, debates, etc.) Of these documents, only two deal with the implementation of the document in a critical, reflective, manner. The vast majority (41 documents) only deals with the implementation as a technical procedure. It is important to mention that lawmakers that would normally propose debate or public participation, in this case only request that the possibility of the use of the document be extended to include also the handicapped. Also, there are three documents that not only deal with the implementation of new identification forms, but also propose the creation of DNA banks in order to help in the identification of the population. Taking into account the private, public, and researching actors, approximately 85% of them agrees with the document, meaning that they do not argue, question, o reflect upon the matter. As it has already been mentioned by Doneda and Kanashiro (Bruno, Firmino, and Kanashiro, 2009), the implementation of a unique document in Brazil has, in first place, a technocratic aspect, or a technical supremacy that erases its political characteristics. It is often conducive to the recognition of a true inability on the part of the opposition to question the procedures. Thus, in general, what is most evident (even in the media) is an identification system practically clear of blemishes or negative spots. The very nature of this fact already indicates the relevance of carrying out a more precise analysis of a system whose consequences will be felt directly among all Brazilians.

In fact, the process of application of the identification document in the country does not adequately go through the judicial sphere. The slowness for the regulation of the law that instituted the document and its implementation without this regulation makes this scenario evident.

Nor are there in Brazil the legal mechanisms that could be directly linked to such a process and that could determine the forms of control and of supervision of the document itself. Likewise, there is not a clear legislative position on the access and use of personal data that will make up part of the document and the related database. It is important to underline again that the computing systems used to gathering personal data often belong to private companies of the electronic security sector.

Aside from the absence of laws, the new Brazilian document has not been tied to public, political, or academic debates in order to clarify for the citizens the processes that now take place in the country. The population is neither questioning the new document nor the collection of personal data (even biometric information), since there is a culture of giving such information in their daily life, including the fingerprints already present in the old document (RG). In other words, Brazil presents an uncommon case of lack of legislation, a high of acceptance on the part of the population for yielding information, absence of information and debate on the existing bills in the country (even technical information for the legislators), and an absence of research that could contribute to inform the population.

The vast majority of research dealing with biometry and identification takes place in precise areas, more concerned with the proposal of more efficient technical systems. Among the studies on humanities there is a greater presence of research on information management, and very little on critical studies or those reflecting upon the matter.

Therefore, the country appears to be a very attractive market for the industry of electronic security and for what nowadays is called the industry of identification. One of the key players in this case identified is Abrid (Association of Enterprises of Digital Identification Technology). It is important to mention that other events such as the Congress of Digital Citizenship and Certforum raise questions about the application of RIC. In these events it is common to find, among promoters, organizes, sponsors, or fans, the presence of some of the firms linked to Abrid, such as Akyiama Corporation, Gemalto, GD Buri, M.I. Montreal Informatics, Oberthur Technologies, NEC, etc.

It is possible to point out that in the country there is an unequal distribution of power between the State, the private sector, and he citizens, thus weakening the latter who are helpless in the control over their own personal data. The slowness of regulation of legislation 9.454/97 set off, for instance, a possible previous judicial revision and popular participation. This way an imbalance in the share of power between state and individual (as well as the private companies participating in the project) took place. There are no legal possibilities of effective legal control or protection of the citizens with respect to their personal data, thus causing an imbalance that is not compensated by possible solutions –for instance, the option of using less invasive technologies.

There are increased possibilities of controlling and carrying out surveillance on the citizens in Brazil, while the citizens in other countries can hold public or political debates, academic investigations, as well as [the use of] norms and identification systems that allow for their protection against the specific risks of a unique identification system. In this sense, the “digital gap” threatens grow among the citizens of different countries, not exactly in the manner that the subject is talked about most commonly (meaning, the access to information and the services of a Society of Information), but rather in the form of an access to information and ulterior control

exerted with increased intensity over the citizens in certain nations. In Brazil, there is a real risk of placing the country among the group of the latter, characterized by a greater control.

c) About personal data in the Internet in Brazil

It is relevant to point out and retake some of the elements mentioned in this matter on the problem of treatment and regulation of data in the Internet in Brazil, taking into account the final considerations for this part of the report.

In the field of the legislation, we consider that the current state of the laws and law drafts in Brazil reveals that the protection of personal data is a minor concern, if we consider the amount of laws and bills that defend it. Most of the bills on this matter in the sphere of Brazilian legislation chose to center their concern on the possibility that a common Internet user may commit a crime. This is to say that, in the majority of cases, security and the combat to "cybercrime" are privileged, in detriment to the protection of personal data, the guarantee to anonymity, and the defense of privacy. In other terms, the common Internet user is seen less as a citizen whose rights (relative to privacy, to anonymity in the communications, and to personal data) need to be defended than as a potential criminal who must be stopped. Actors such as consumers, legal entities, firms, and public institutions (which are more directly involved in the collection, treatment, and use of personal data in the Internet) are among the least cited, appearing in 5%, 3%, 2%, and 2% of the analyzed laws/bills, respectively. Few bills/laws focus on the regulation of the use of personal data with commercial purposes, looking for phenomena such as the elaboration of computational profiles – sets of data on taste, preferences, and interests of the users, collected very often without their consent, and which are used to anticipate their behavior and to direct commercial ads in alleged line with their personality. This observation is corroborated by the low presence rate of the terms "profile" and "commercial advertisement", which appear in 3% and 2%, respectively, of the analyzed bills. One could also infer, moreover, that the Internet is less used as a medium of communication and of production of contents that must be democratized and secured, than as a medium for potential criminal actions that must be controlled. This concept of the Internet is especially present in the bills/laws that choose cybercafés as centers of control and of responsabilization [sic], demanding of those establishments to identify their users and to keep a log with their registration data. Such establishments have played an important role in the digital inclusion in Brazil, since most of the low-income population lacks access to the Internet from their homes (as was noted in the introduction to this subject; Cf. item 5.1 in this report). This role is underappreciated by the great majority of Brazilian bills/laws actually determining such establishments rather act as potential centers for cybercrimes. An evident symptom of this aspect attributed to cybercafés is a prohibition, set in some bill drafts, for their construction within a certain distance of schools.

One of the bills most representative of the swaying tendency to criminalizing is the addendum of the Senate to the Bill of the Chamber 89/2003, known as PL Azeredo (Cf. Item 5.2.1 in this report). This bill shows how the imperative of security and the intention of catering to the interests of the copyright industry can restrict freedom, the possibility of collaboration, of creation and development of knowledge in the context of the digital communication networks, especially the Internet. [79]

Meanwhile, in spite of the great majority of bills privilege the combat on cybercrime, in detriment of the protection of personal data, the current political situation in Brazil ended up favoring the proposal of a bill draft for the protection of personal data (Cf. Item 5.2.1 in this report). This draft, put forward by the Ministry of Justice, has greater possibilities of making it to Congress for voting than other bills that acted against personal data protection in the Internet. Thus, although the number of bills threatening the privacy of Internet users –opposing the establishment of legal frameworks to secure the protection of personal data– be higher, the Brazilian governmental context favors the sending of a bill draft on personal data protection to be passed on to the Chamber of Deputies. This way, the Brazilian society awareness with respect to the implications of the treatment and the regulation of personal data is urgent and timely.

The outlook encountered in the Brazilian legislation, notoriously inclined towards privileging a program directed at fighting cybercrime in detriment of a program directed at personal data protection policies, is not mirrored likewise in the academic output on the matter. The mapping of existing studies reveals that the subject of "privacy" is the seventh most frequent, whereas "crime" appears in ninth place among the most recurring subjects. However, it is important to consider – according to what was seen in the classification of indicators per article (Cf. Chart 24) and in the classification of indicators per article and per journal (Cf. Chart 25), together with the preliminary analysis on the summaries of the articles– that the academic output reflects two main ways in which the issue of personal data in the Internet is dealt with. The first one associates this issue with the areas of privacy and control, while the second one associates it with the realm of security and crime. It must be pointed out, also, that in this scenario firms/organizations and the market stand out as key players, followed by consumers and the electronic commerce.

Even in the mapping made in existing studies, we highlight the dominance of the Law as the area of knowledge where production is the greatest and where more articles are published in relation to privacy and to the regulation of personal data in the Internet. This indicates, at least in quantitative terms, the superiority of a judicial perspective over the issue of personal data in the social communication networks. In the area of communications, the second one in academic output, the

[79] It is important to highlight that the project has received harsh criticism leading to a social activism organized against its approval, which is still under discussion in the country. Among those movements it is worthy of mention Mega No (http://meganao.wordpress.com/), whose manifest objective, supported by various blogs, was to become a nucleus against the marked tendency to surveillance online, as well as an online petition available at: that was signed by more than 150000 people.

subject of surveillance is more frequent when compared to the most often recurring areas of knowledge. It is evident also a quantum leap in the general production on the subject after the year 2000, leveling up over the last decade, which can be explained by the awareness of the digital communication technologies, especially the Internet, at a world and local level. In the analysis of recurrence of the five key terms most pertinent to our research ("personal data", "surveillance", "data protection", "monitoring", and "privacy") we highlight the dominance of the concept of "privacy" in all recent years within the scope of the research (1999-2011). The term "personal data" appears with a significantly lesser frequency, compared to the term "privacy", although its recurrence is maintained throughout the timeframe mentioned. This scenario may indicate that the treatment of the matter of personal data in the Internet is focused on issues concerning privacy, which does not exhaust its many implications for social, political, economic, and individual life. Meanwhile, this hypothesis can only be verified through a specific research on the matter, which is not considered within the scope of this report.

If in the output of academic publications the subject "personal data" loses importance to "privacy", the same does not apply in the field of events, since four of them took place over the past two years (out of a total of 22) focused specifically on treatment and regulation of personal data in Internet in Brazil. The subject of "privacy" is also present among the events, but to a relatively lesser extent. The presence of governmental agents is also noticed (particularly the Public Ministry and the Ministry of Justice) among the most frequent institutions sponsoring these events.

This presence is articulated with the proposal of the bill draft on personal data protection, mentioned in the subject related to legislation, and reappears in the institutions whose actions have implications in the regulation of the treatment given to personal data in Internet in Brazil. Three out of the four institutions identified are initiatives advanced through the cooperation of ministries and education and research institutions, as well as the civil society. We thus identified efforts on the part of the Brazilian government in favor of the promotion, in recent years, of a public debate on the regulation and treatment of personal data in the Internet.

The response to this promotion on the part of society could be identified in the mapping of movements and organizations from the civil society. Although still numerically of little relevance (nine in total), we highlight the progressive increase in these movements in recent years, as well as their intersection with different areas of action (human rights, consumer rights, communication rights, knowledge production and innovation in communication technologies, political activism, defense of freedom of speech, and digital culture), which favors plurality of the public debate on the matter. We also highlight that, as much in institutions as in the movements and organizations from the civil society, the use of the Internet as a decisive player in the encouragement of the participation of society in public debate over personal data in the Internet. Online platforms and discussion boards occupy an important place among the recent actions identified.

The last field mapped, concerning the role of technologies of collection, monitoring, and treatment of personal data in Internet, may be the one that keeps the lowest profile among the rest, with a few exceptions. In spite of the massive presence of these technologies in the most popular sites, platforms, and services available in Brazilian Internet, this actor receives relatively little attention as much in the area of legislation (with the exception of the bill drafts for the Civil Framework of Internet in Brazil and the Protection of Personal Data) as in the academic output and in the movements and organizations. There are hints to that the institutions involved in the government and regulation of the Internet in Brazil, identified in this research, are the most related to this matter. This way, we can point out a contrast between the little visibility of this actor and its strong presence in Brazilian Internet. Two tendencies identified in this context contribute to this low visibility: the difficulty of detecting this kind of technology in sites, applications, and services that we use on a daily basis; and the still significant margin of ambiguity on the part of these sites in what pertains to the explicitness of their policies of privacy; their collection, monitoring, and treatment of personal data practices (as detailed in the relevant subject, 19% of the firms operating cookies do not have any policies of privacy in their sites.) It should be pointed out, also, the little margin of option left to the users, which makes controlling more difficult on their part with respect to their personal data. This aspect can be verified in at least four identified tendencies: a) the fact that more than half the firms that operate cookies do not offer an "opt-out" mechanism (which allows the user to turn those tools off in the case they do not wish for their persona information to be collected or monitored); b) the fact that this mechanism, when offered, is of difficult access and/or use (as in the case of companies using beacons); c) the transfer of responsibility, on the part of the sites analyzed, to third-party hired firms, making users subject to the privacy policies of these; d) the vulnerability of the user of social network applications, since their actions are subject to a great number of trackers and their profile information becomes accessible for the developers of these applications.

Taking into account the massive presence of these tools for the collection, monitoring, and treatment of persona data in poplar sites in Brazil, contrasting with the small margin of knowledge and control of these tools on the part of the user, we consider it of high relevance to disseminate the information produced in this research in order to encourage debate and the influence of public policies on the matter in Brazil. The strategic character of these tools in the planning of services, publicity, audience, and the use of Internet sites, also highlighted among the tendencies identified in this report, indicates that such tools and practices tend to grow and to become more complex. It is thus evident the relevance of civil society participation in the public debate about the implications of these tools in the privacy, freedom, and the control over personal data of the Brazilian Internet user. This report pretends to become a vehicle for the advancement of such participation.

d) About the proliferation of CCTV in Mexico

Based on the analysis of CCTV made here, we can notice the ways in which these swing between the care and the control of the population. If at a municipal scale CCTV appear as supportive of the operation of the stoplight systems, its range of operation has grown into other areas, particularly public security, and, although in some cases they tend to be linked to other surveillance means –as is the case in Tlalnepantla– or to gain a greater independence –as it happens in Toluca– in both cases their use is generally geared towards the location of abnormal or atypical behaviors –all of which are naturally founded on prejudices– evolving into tools for the control and containment of social and political movements. This places over the discussion table the use of CCTV as means for the inclusion of certain sectors of society and the exclusion of others, which constitutes differentiated citizenships.

With respect to consumerism, it is possible to observe the behavior of individuals in shopping centers. Consumerism has become the one element that defines urban citizenship [where] the architectural space and the experience of procurement in shopping centers contribute to their definition. Shopping centers are spaces where the individuals give sense to their subjectivity and confirm, at the same time, a sense of belonging into the community. However, these spaces are two-faced: they are public spaces into which all can enter, but where not all have access to the products there offered, thus becoming spaces for social exclusion, which is strengthened, as shown already, by the start up of various mechanisms of surveillance, both electronic and "face-to-face". Likewise, the use of CCTV helps in regulation life in the workspace, transforming it into tools for control and discipline.

Therefore it is necessary to introduce in the debate within the social sciences the way in which this surveillance is being carried out in such spaces, in as much as their presence is a political issue pointing at the very definition of citizenship, in the sense of the processes of social exclusion and inequality that it produces. The resort to CCTV and other kinds of surveillance mechanisms, in public and private spaces within the cities, is becoming a way for the increase of inequality in the access to certain aspects of citizenship. These technologies are not, as studied already, neutral instruments; their set up does more than respond to the needs for greater security and social protection. Together with this, they become mechanisms that allow the magnification of processes of typification, through which it is possible to define the people who are, or are not, legitimate users of certain spaces. Therefore, they constitute processes in themselves to be added to others, already established by the dynamics of the economic and political spheres, new forms of social differentiation. Their impact, therefore, is not little. Nowadays the individuals find themselves subject to their scrutiny in the context of the urban space: in public and private offices, on the streets, in shopping centers, to mention only a few. People find themselves thus before a context of permanent surveillance in which, at every moment, their status as citizens is at stake.

Undoubtedly, it is not the same to use CCTV to control and contain a social and political movement than to detect a "non-consumer" who might produce a disturbance in the expected behavior at a

shopping center, or an employee who uses the hallways in their working space for socializing; the impact in the civil and political rights is not the same. But if we consider that social institutions – such as the city or shopping mall here– function as supports for the constitution of the individuality of the modern person, that is, the raising of their interiority and their citizenship, it is clear that surveillance weighs specifically in its conformation: it can support as much as it can become a machine for the negation of individuality and, therefore, of certain rights.

Stemming from the justification that the installation of CCTV responds to the need to guarantee security, an aversion sets in to a variety of behaviors considered to escape from what is typically deemed "normal". This is what Bauman calls "mixophobia": a reaction in search for a community of equals that guarantees the exclusion of otherness, although it is generally only achieved through management and administration. The development of this kind of behavior among those who operate CCTV in different spaces is conducive to the reduction, ever so marked, of the capability to negotiate behaviors, as well as the ability to coexist with the other. As Bauman himself points out (2008), the unknown others tend to appear more terrifying in as much as they are farther, unknown, and incomprehensible, withering thus the dialog with them. The problem lies, then, in that mixophobia is fed by the practice of territorial alienation that generates and recreates it. Therefore, it is pertinent to consider to what extent the installation of CCTV is a contributing factor to this in a country where inequality issues are already enormous and constantly on the rise.

e) About identification systems in Mexico

In Mexico, surveillance and its technologies are tightly linked to the subject of security, since public and private entities make use of their tools to confront the insecurity generated by the rise in crime. Due to this, even though Mexico counts with a diverse precedent in the registration and identification of the population, the project of a unique identification document and of an identification card for minors constitute special cases in this tradition of registration and identification.

These particularities have called our attention to identify troublesome points that may be important to retake in the future in order to carry out more in-depth research. In the first place, there is a connection between the intention of the governments to gather personal data that are concentrated in systems of unique identification and the effects of this collection in the real efficiency of existing bureaucratic apparatus. The possible argument is that systems of this kind can only contribute to the construction of more democratic societies in as much as the issue of the use of data is regulated with clarity and precision.

It has been pointed out that in Mexico there is a more specific regulation with respect to the information on population that the Federal Government can collect, as opposed to the lack of federal regulation shown in the case of CCTV an of Internet. However, the controversy brought about by the project of a unique ID reveal that it is necessary to deepen the study and proposal of concrete actions for articulating the interests and viewpoints of the various agents summoned by devices of this nature. The question that arises at this point is in relation to the character of these proposals, since it is necessary to think whether they will be occupied if impacting on the laws, the rules, or the logic of organization of the agents and organizations involved in their planning, running, and administration.

Therefore, for the case of Mexico, a new project of personal identification has been highly questioned in the realm of the public. The advantages of this questioning lie in revealing a fertile ground for debate; the disadvantages being that this debate has been largely lead by political and partisan interests, which calls for the stimulation of discussion from different spheres such as the one of non-governmental organizations and the academic world, in order to involve in the arguing different perspectives and also strengthen some of the already existing ones.

At a more concrete level, the controversies spurred around the project of an identity card focus on three critical points: a) the real need for a new identification document taking into account the existence of other forms of identification; there was a warning in the sense there might be an unnecessary duplications of documents, aside from the unnecessary use of resources, b) the private and public entities indicated to carry out the management and control of the creation of the document, particularly in a context of questioning over the handling of data that has taken place in the country, on the part of public and private entities, and c) whether modifications to the existing normativity are adequate, in order to allow for the collection of a number of biometric data that different participants have seen as excessive, unnecessary, and even violating the privacy rights.

Crossing every one of these points is the questioning about the institutional strength of the State. This questioning is set forth in the skepticism shown by various agents on the existing ability to rationally manage the process of identification of the population without mixing it with political interests. Another expression of the questioning on the federal and local governments goes about their ability to apply the existing regulations protecting personal data, since there is a perception among the population that a clear answer is still to be given on whether there may have been cases of sale or loss of personal information databases. This is a critical point in the current context of crime-ridden violence, in which the population lives in a latent distrust that in turn provokes a reticence towards participating publicly and collaborating with the governing bodies with the release of information that, they fear, may not be really protected and can thus put the individuals in situations of greater vulnerability to delinquency, whether violent or not. Lastly, the questioning of the institutional strength of the State has been expressed in the struggle between the various political forces, where these are unable to coincide completely over the normativity to follow in

order to carry out processes such as this one. In this research, we have observed that the reforms to the Regulation of the General Population Law have generated inconformity actions from various agents.

The research carried out presents itself before this scenario as pertinent in the stimulation of debate at an academic level, especially if we consider that even when the process of registration and identification of the Mexican population has accompanied the consolidation of the Mexican State, the discussion concerning the protection of data is relatively recent, drawing special attention to the role of the Law as a pioneering area in this discussion. The contributions from this field are invaluable in as much as they make explicit the judicial logic of the starting of projects such as this one; however, it is still necessary to make inter-disciplinary approaches to the issue since, as we have seen, the issues braided around the identification document are not exclusively judicial in nature.

f) About personal data in the Internet in Mexico

Final considerations

As can be seen, the research carried out in Brazil indicates that the role of the private sector is powerful in the areas of Internet and video surveillance, where both agents are important in the expansion of video surveillance in public and private spaces, and of the monitoring of data through the Internet.

Notice also that the gap in the legislation destined to the protection of personal data is reflected as much in the context of video surveillance as it is in the new national document of identification. This scenario is not completely reproduced in the Internet, where there is a context of conflict between a majority of the bills defying anonymity in the use of the Internet while demanding for mechanisms of identification and monitoring of the users, on one hand; and on the other, a minority of bill drafts aimed at guaranteeing the protection of personal data in the Internet. The latter, although fewer, are relatively stronger and more effective, since these were proposals by the Brazilian government that could be carried out against the majority of the bills mentioned.

The academic output has shown, both with regards to video surveillance and to the Internet, a significant increase in the number of published articles on the subjects over the past 10 years, with an emphasis on the strong presence of the humanities and the social sciences, as well as the judicial sciences (as was in the case of the Internet). Standing out, also, is the critical nature of the

academic output in both regards, which is not seen in the academic studies on the new document of identification in Brazil, mostly brought in from the area of the exact sciences and with a critical output of little significance.

Generally speaking, the judicial debate over the protection of data in Brazil is centered almost exclusively on the matters concerning the Internet, because of which it is not common in matters related to the use of surveillance devices or the new identity card. All three areas indicate, to a greater or lesser degree, a minimal public debate on the main subject of the investigation. Although in the area of the Internet an increase can be seen in the groups of interest –relatively organized– that go about the legal debate, this is still limited and localized, and is yet more scarce in the cases of national identification and surveillance cameras. Such scenario points to the need to make public the results shown in this report, with the purpose of contributing to the growth of this debate in Brazil and in Latin America.

7. BIBLIOGRAPHY

Amadeo, S. (2001). "*Informática y nuevas tecnologías"*. Madrid: La Ley.

Arizaga, M. C. (2000), "Las murallas y barrios cerrados. La morfología espacial del ajuste en Buenos Aires" Caracas: *Nueva Sociedad*, Núm. 166, pp. 26-37.

Arteaga, N. (2011). "Urban Surveillance in Mexico". En Rodrigo Firmino, Fabio Duarte and Clovis Ultramar (Coordinadores*). ICTs for Mobile and Ubiquitous Urban Infrastructures: Surveillance, Locative Media and Global Networks* (págs. 324-340). IGI Books

Arteaga, N. (2011). "Securyte Metamorphosis in Latin America". En Vida Bajc & Willen de Lint (Coordinadores). *Security and Everyday Life* London: Routledge. (págs. 236-257).

Arteaga, N. (2010a). "Privay and Surveillance in Mexico and Brazil": A Cross-National Analysis. En Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon (Coordinadores). *Surveillance, privacy and the Globalization of Personal Information: International Comparisons.* Mc-Gill-Queen's University (págs. 212-229).

Arteaga, N. (2010b). "Video-Vigilancia Del Espacio Urbano: Tránsito, Seguridad y Control Social".México: *Andamios*, 7 (14), 263-286

Arteaga, N. (2010c). "Consolidación De Los Archipiélagos De Seguridad en América Latina".México: *Espiral, 17 (49)*, 163-195

Arteaga, N. (2010d). Orquestracao de Vigilancia Eletronica: Uma Experiencia Em CFTV No. México. En Bruno F, Rodrigo Firmino Marta M. Kanashiro (Coordinadores). *Tecnologia, visibilidade e vigilancia* (págs. 17-35). Sulina

Arteaga, N. (2009a). "*Sociedad y Vigilancia en el Sur-Global. Mirando América Latina"*. México: Miguel Angel Porrua-UAEM. ISBN 9786074011715

Arteaga, N. (2009b). "The Merida Initiative: Security-Surveillance Harmonization in Latin America". *European: Review of Latin American and Caribbean Studies*, 87, Octubre 2009, 103-110

Arteaga, N. (2007a). "An Orchestriaton Of Electronic Surveillance: A CCTV Experience in Mexico". *International Crimal Justice Review,* 17 (4), 325-335

Arteaga, N. (2007b). "Seguridad Pública en el Estado de México: Perspectiva Gerencial y Micro-Gestión De Riesgos". *Revista Criminalia*, LXXII (2), 75-94

Bauman, Z. (2008a), "*Confianza y temor en la ciudad. Vivir con extranjeros*, Arcadia", Barcelona:Tusquets

Bauman, Z. (2008b), "*Tiempos líquidos. Vivir en una época de incertidumbre"*, México: CONACULTA, Tusquets.

Bruno, F. (2006). "Dispositivos de vigilância no ciberespaço: duplos digitais e identidades simuladas".Brasil: *Revista Fronteira* (UNISINOS), VIII, p.152 - 159, 2006.

Bruno, F. (2008). “Monitoramento, classificação e controle nos dispositivos de vigilância digital”. Porto Alejgre: *Revista FAMECOS*, 36, p.1–7.

Bruno, F. (2009). “Distributed Surveillance: Video, Monitoring and Mobility in Brazil”. *Wi Journal of mobile media*, Summer, p.1 – 10.

Bruno, F.; Firmini, R.; Kanashiro, M. (orgs). (2010). “*Vigilância e visibilidade: espaço, tecnologia e identificação”*. Porto Alegre: Sulina.

Caldeira, T. (2000). *Cidades e muros, crime, segregação e cidadania em São Paulo*. São Paulo: Editora 34/Edusp.

Carpizo, J. (2000) “*Nuevos Estudios Constitucionales”*, México Porrúa-UNAM

Castel, R. (2003b) “*Propiedad privada, propiedad social, propiedad de sí mismo: conversaciones sobre la construcción del individuo moderno”*. Argentina: Politeia

Castells, M. (2003). “*Internet, libertad y sociedad, una perspectiva analítica”*, Disponible en: http://redalyc.uaemex.mx/redalyc/src/inicio/ArtPdfRed.jsp?iCve=3050041

Chabat, J. (2010). “La Iniciativa Mérida y la relación Mexico-Estados Unidos en Busca de la Confianza Pérdida” Méxio:CIDE.

Christopherson, S. (1994), “The Fortress City: Privatized Spaces, Consumer Citizenship, *Post-Fordism”: A Reader*, A. Amin. Oxford: Blackwell, pp. 409-427.

Cunjamá, E. D., Loría H. (2010). “Sociedad de la vigilancia y Estado policial: Análisis de las tecnologías y aparatos de control”. *El Cotidiano*, núm. 161, mayo-junio. México: Universidad Autónoma Metropolitana Azcapotzalco. pp 5-11

D’Ottaviano, M. C. L. (2006). Condomínios Fechados na Região Metropolitana de São Paulo: fim do modelo centro rico versus periferia pobre? *Anais*, In: XV Encontro Nacional de Estudos Populacionais, ABEP, Caxambú/MG.

Dubie, P. (2003) *“La protección de datos en Latinoamérica y el interés de España por un nivel de protección adecuado”*. Entrevista realizada por Ruipérez García Pablo Revista de Informática, Universidad Nacional de Educación a Distancia (UNED).

Ellin, N. (1977), “Shelter from the Storm, or Form Follows Fear and Vice Versa”, en Ellin, N.; Blakely, E.J .Nueva York: *Architecture of Fear*; Princeton Architectural Press.

Figueroa B. (2003), “Reflexiones sobre la pertinencia y concreción de un registro de población”, México: *Estudios Demográficos y Urbanos*, 52; 5-31.

Flint, J. (2006), “Surveillance and Exclusion Practices in the Governance of Access to Shopping Centers on Periphery Estates”, *Surveillance and Society*, 4(1), pp. 52-68.

García, P. J. y Villa M. (2001), “De la sociedad vigilante a la urbanidad preventiva”, México: *Perfiles Latinoamericanos*, núm. 19.

Gaytán, P. (2010). “Vigilar y negociar. Imaginario sociomediático de la seguridad pública y campo vacío ciudadano”. *El Cotidiano*, núm. 161, mayo-junio, México: Universidad Autónoma Metropolitana – Azcapotzalco pp 13-22

Giddens, A. (1987), “*The nation-state and violence*, Berkeley”.California: University of California Press.

Giglia, A. (2001), “Los espacios residenciales cerrados: el caso de Villa Olímpica”, en María Ana Portal (coord.). *Vivir la diversidad. Identidades y culturas en dos contextos urbanos*, México: CONACYT.

Gill, M. y Spriggs A. (2005). “*Assessing the impact of CCTV*. London”: Home Office Research, Development and Statistics Directorate, 43. Disponible en: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.7998&rep=rep1&type=pdf>, Último acceso: 20 feb. 2009.

Gómez, S. (1986), “Democracia y poder en México: el significado de los fraudes electorales en 1979, 1982, 1986”, México: *Nueva Antropología*, 31; 127-157.

Gómez-Robledo, A. y Ornelas, L. (2006). “*Protección de datos personales en México: el caso del Poder Ejecutivo Federal”*, México: UNAM.

González L. (1981). “La República Restaurada y Vida Social” México: El Colegio de México.

González L. (1988), “El liberalismo triunfante”, en José Velazquez (ed.), *Historia General de México*, México: El Colegio de México.

Hernández, H. (2008), “*Democracia y federalismo: la credencial electoral con fotografía como instrumento formal de la transición democrática*”. México: Universidad Autónoma de Baja California.

Hilbert, M. (2001). “*Latin America on its path into the digital age*: where are we? Santiago. United Nations: Publication.

Kanashiro, M.M. (2006a). “A inserção das câmeras de monitoramento para segurança no Brasil”. Caxambu: *XXX Encontro Anual da ANPOCS, Anais*.

Kanshiro, M.M. (2006b). “Sorria, você está sendo filmado: a inserção das câmeras de monitoramento para segurança em São Paulo”. Sao Paulo: En *Dissertação de Mestrado*, Unicamp.

Kanashiro, M.M. (2008) “Surveillance cameras in Brazil: exclusion, mobility regulation, and the new meanings of security”. Brazil: En *Surveillance & Society* (Online), v. 5, p. 270-289.

Katz, J. y Hilbert, M (2003). “*Building an Information Society:* a Latin American and Caribbean Perspective”. Santiago: United Nations Publication.

Lajud L. y Quiroz, M. 2007 “La Necesidad de Legislar para Regular el Uso de la video Vigilancia en México”.México: Universidad Autónoma de Puebla.

López, L. (1999), “*Centros Comerciales: espacios que navegan entre la realidad y la ficción”*, México: Nuestro Tiempo.

Lyon, D. (2009) "*Identifying citizens"*. Cambridge: Polity Press.

Marioto, M. y Firmino, R. J. (2010). "Medo e segurança na cidade contemporânea: estratégias de marketing para condomínios horizontais em Curitiba".Brazil: En *Relatório de pesquisa*. Curitiba: PUCPR.

Messía de la Cerda Ballesteros, J. A. (2003). "*La cesión o comunicación de datos de carácter personal"*, Madrid: Thomson-Civitas.

Nieto, H. (2007) "Registro Nacional de Población". México: En Revista de los Tribunales Agrarios no. 43 Septiembre-Diciembre.

Nougréres, A. B. y Doneda, D. et al. (2008). "Proteção de dados pessoais na América Latina". Brazil: En Habeasdata.org.br, 20 abril 2008.

Pérez, A. (1989). "Los derechos humanos en la sociedad tecnológica". En G. Losano, Mario, *et. al. Libertad informática y leyes de protección de datos personales*. Madrid: Centro de Estudios Constitucionales. pp. 145 y ss.

Pierini, A. *et al.* (1999). "*Habeas Data"*, Universidad, Buenos Aires.

Piña, H. R. (2008). "*El derecho a la autodeterminación informativa y su garantía en el ordenamiento jurídico mexicano"*. México: Instituto de Transparencia y Acceso a la Información Pública del Estado de México.

Riande, N. (2000). "¿Por qué debe legislarse en México en materia de Protección de Datos Personales Automatizados?". Ponencia presentada en el marco del *VIII Congreso Iberoamericano de Derecho e Informática*, celebrado del 21 al 25 de noviembre de 2000 en el Campus Estado de México del Tecnológico de Monterrey.

Rotker, S. (2000), "Ciudades escritas por la violencia (a modo de introducción)", en Susana Rotker (ed.), *Ciudadanías del miedo.* Caracas, Venezuela: Nueva Sociedad-The State University of New Jersey.

Shields, R. (1992), "*Lifestyle Shopping. The subject of consumption"*, London: Routledge.

Villanueva, E. (2002). "*Derecho comparado de la información"*. México: Universidad Iberoamericana-Fundación Konrad Adenauer.

Villegas M. (1973), *Historia moderna de México: El Porfiriato y vida social"*, México: Hermes.

Wood, D. M. y Firmino, R. (2009). "Inclusion or Repression? Opening up questions of identification and exclusion in Brazil through a case of 'identity fraud'." Londres: En *Second Multidisciplinary Workshop on Identity in the Information Society. Proceedings of II IDIS.*

Wood, D. M y Graham, S. "Digitalizing surveillance: categorization, space, inequality".Londres: En *Critical social policy*, vol. 23, n. 2: 227-248.

Zukin, S. (1995), "*The cultures of cities"*. Blackwell, Cambridge, Massachusetts, US.

Documentos Oficiales

Agencia de notícias do Tribunal Superior Eleitoral (TSE). *Justica Eleitoral inicia recadastramento biométrico dos eleitores de Goiânia*. 2011. Disponível em: <http://agencia.tse.gov.br/sadAdmAgencia/noticiaSearch.do?acao=get&id=1368545>, Último acesso: 19 abr 2011.

CGI.br (Comitê Gestor da Internet no Brasil). *Pesquisa TIC de Domicílios 2010*. São Paulo, 2011.

Diario Oficial de la Federación (2008), 25 de agosto de 2008; disponible en http://dof.gob.mx/nota_detalle.php?codigo=5057719&fecha=25/08/2008

Diario Oficial de la Federación (2011), 19 de enero de 2011; disponible en http://dof.gob.mx/nota_detalle.php?codigo=5174983&fecha=19/01/2011

Gaceta informativa de la Comisión Federal Electoral (1978), Tomo III, México, 1978.

Gaceta Parlamentaria (2001). Núm. 688, jueves 15 de febrero de 2001; disponible en: http://gaceta.cddhcu.gob.mx/Gaceta/58/2001/feb/20010215.html

Gaceta Parlamentaria (2001). Núm. 692, miércoles 21 de febrero de 2001; disponible en: http://gaceta.cddhcu.gob.mx/Gaceta/58/2001/feb/20010221.html#Ini20010221Antonio

Gaceta Parlamentaria (2001). Núm. 832, viernes 7 de septiembre de 2001; disponible en: http://gaceta.cddhcu.gob.mx/Gaceta/58/2001/sep/20010907.html

Gaceta Parlamentaria (2002). Núm. 1082. 5 de septiembre de 2002; disponible en: http://gaceta.diputados.gob.mx/Gaceta/58/2002/sep/20020905.html#Minuta20020905DatosPersonales

Gaceta Parlamentaria (2002). Núm. 999, martes 14 de mayo de 2002; disponible en: http://gaceta.diputados.gob.mx/Gaceta/58/2002/may/20020514.html#Ini20020514Barbosa

Gaceta Parlamentaria (2004). Núm. 1600-I, jueves 7 de octubre de 2004; disponible en: http://gaceta.diputados.gob.mx/Gaceta/59/2004/oct/Anexo-I-07oct.html

Gaceta Parlamentaria (2005). Núm. 1895-I, jueves 1 de diciembre de 2005; disponible en: http://gaceta.cddhcu.gob.mx/Gaceta/59/2005/dic/Anexo-I-01dic.html#Iniciativas

Gaceta Parlamentaria (2006). Núm. 1953-I, jueves 23 de febrero de 2006; disponible en: http://gaceta.cddhcu.gob.mx/Gaceta/59/2006/feb/20060223-I.html#Iniciativas

Gaceta Parlamentaria (2006). Núm. 1972-I, miércoles 22 de marzo de 2006, disponible en: http://gaceta.cddhcu.gob.mx/Gaceta/59/2006/mar/20060322-I.html#Iniciativas

International Telecommunication Union (ITU) (2010). *Measuring the Information Society*. Geneva.

Jacinto, S. *Frequência digital nas escolas constituirá identidade cidadã*. Serviço de comunicação do Serviço Federal de Processamento de Dados (Serpro), Notícias 2004. Disponível em: <http://www.serpro.gov.br/noticias-antigas/noticias-2004/20040823_01>, Último acesso: 29 mar. 2009.

Secretaría de Gobernación (1982b), *Diagnóstico del registro civil en México, 1980*, México: Secretaría de Gobernación

United Nations Conference on Trade and Development (UNCTAD) (2002). *Electronic Commerce Strategies for Development*: *The Basic Elements of an Enabling Environment for E-Commerce*. Geneva. Disponible en <http://www.unctad.org/en/docs/c3em15d2.en.pdf>. Último acceso: 30 de junio de 2011.

Recursos electrónicos

ComSCORE. Orkut Continua Liderando o Mercado de Redes Sociais no Brasil, e a Audiência do Facebook Quintuplica. *ComScore*, 7 out. 2010. Disponível em: <http://www.comscore.com/por/Press_Events/Press_Releases/2010/10/Orkut_Continues_to_Lead_Brazil_s_Social_Networking_Market_Facebook_Audience_Grows_Fivefold>. Último acesso: 12 maio 2010.

El Informador. (2011). *Conectarán cámaras públicas y privadas para ampliar vigilancia*. Disponible desde el 15 de mayo de 2011 en http://www.informador.com.mx/jalisco/2011/277745/6/conectaran-camaras-publicas-y-privadas-para-ampliar-vigilancia.htm

Espinosa de los Monteros Hernández, Roberto [Online], "El Registro Civil: una historia sesquicentenaria", Instituto Nacional de Estudios Históricos de las Revoluciones de México, Secretaria de Gobernación Available at: *<http://www.inehrm.gob.mx/Portal/PtMain.php?pagina=exp-registro-civil-articulo>* [Viewed 04-05-2010]

Fernández, Emilio. (2010). Camiones tendrán videocámaras. En *El Universal.* Obtenido el 10 de mayo de 2011 desde http://www.eluniversaledomex.mx/ecatepec/nota2519.html

http://www.al.sp.gov.br
http://www.alep.pr.gov.br
http://www.alerj.rj.gov.br
http://www.alexa.com/topsites/countries/BR
http://www.camara.gov.br;
http://www.causaencomun.org.mx.Causa en Común
http://www.cedla.uva.nl/10_about/institute.html
http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LGP.pdf , Consultado el 16 de julio de 2011
http://www.eluniversal.com., mx/notas/739734.html
http://www.eluniversal.com.mx/nacion/176153.html
http://www.eluniversal.com.mx/nacion/184095.html
http://www.eluniversal.com.mx/notas/740779.html
http://www.ghostery.com/ http://www.networkadvertising.org/
http://www.gobernacion.gob.mx/es/SEGOB/Sintesis_Informativa?uri=http%3A%2%2Fwww.SEGOB.swb%23swbpress_Content%3A1549&cat=http%3A%2F%2Fwww.SEGOB.swb%23swbpress_Category%3A1
http://www.imldb.iom.int/viewDocument.do?id=%7B4E02258C-8466-4A4F-AD72-DFADC0E4F602%7D Consultado el 16 de julio de 2011

http://www.informador.com.mx/mexico/2011/320634/6/corte-desecha-juicio-contra-cedula-de-identidad.htm
http://www.jornada.unam.mx/2009/10/31/index.php?section=politica&article=011n1pol,
http://www.jornada.unam.mx/2009/11/25/index.php?section=politica&article=009n1pol
http://www.jornada.unam.mx/2009/12/15/index.php?section=politica&article=003n1pol
http://www.jornada.unam.mx/2010/01/20/index.php?section=politica&article=008n2pol
http://www.jornada.unam.mx/2010/02/17/index.php?section=politica&article=007n2pol,
http://www.law.duke.edu/about/mission
http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html
http://www.milenio.com/node/621419
http://www.orkut.com/MembersAll
http://www.publicaciones.cucsh.udg.mx/pperiod/espiral/index.htm
http://www.renapo.gob.mx/swb/swb/RENAPO/Beneficioscedi
http://www.renapo.gob.mx/swb/swb/RENAPO/cedi
http://www.renapo.gob.mx/swb/swb/RENAPO/MedidasCEDI
http://www.renapo.gob.mx/swb/swb/RENAPO/renapo
http://www.senado.gov.br
http://www.surveillance-and
society.org/ojs/index.php/journal/about/editorialPolicies#focusAndScope

IMS Research (2011). *Brazil is Not The Only Nut to Crack in Latin American CCTV Market*. Disponible en: <http://bit.ly/ims_cctv>, acceso en 10/02/2011.

Jiménez, R. (2011). Invertirán 96 mdp en videovigilancia de Edomex. *El Universal*. Disponible desde el 24 de marzo de 2011 en http://www.eluniversal.com.mx/notas/754273.html. Obtenido el 16 de junio de 2011.

Rodriguez, J. C. (2010). O Orkut será superado pelo Facebook no Brasil?. En *Webinsider*, 3 de mayo de 2010. Disponible en : <http://webinsider.uol.com.br/2010/05/03/o-orkut-sera-superado-pelo-facebook-no-brasil/>. Último acesso: 12 de mayo de 2010.

Rodríguez, Y. (2011). Vigilarán 11 mil cámaras principales calles del DF. *W Radio*. Disponible desde el 13 de junio, en http://www.wradio.com.mx/nota.aspx?id=1488591. Consultado el 16 de junio de 2011.

Suerveillance Studies (2006) A Report on the Surveillance Society. En *Full report for the Information Commissioner of the UK*. Disponible en: <http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf>, Último acceso: 30 de febrero de 2009.

Torpey, J. (2000), *The invention of the passport. Surveillance, citizenship and the State*, Cambridge: Cambridge University Press.

Valentino-Devries, J. (2010). What the know about you. En *The Wall Street Journal*, 31 jul. 2010. Disponible en: <http://online.wsj.com/article/SB10001424052748703999304575399041849931612.html>. Último acceso: 20/01/2010.