

Personal Data Protection

Coordinator **LDH**



Ligue des droits de l'Homme

Partners **AEDH – EDRI – IURE - PANGEA**

SPANISH REPORT

Methodology

This report is based on (a) the results of the project “kick-off” meeting (Paris, February 2009) where the four main areas of research were identified, (b) the common matrix template to collect information about specific cases in tabular format, (c) the discussion among members of Pangea along this activity to gather information, define the approach, select the topics to report, and select the organizations and individuals to interview, (d) the compilation of information for each case, (e) the interviews and the writing of the subsequent summary contained therein.

The following interviews with external experts or representatives of different organizations were held:

- Internet Users Association (AUI) – Miguel Perez-Subías: The objective of this national association is to promote the development of Internet, the Information Society, protect and defend its users.¹
- Carlos Sánchez Almeida – Lawyer and expert on civil rights on the Internet and ICT technologies. He was a member of free (Electronic Frontiers), an organization geared to defending civil rights.²
- Commission of Freedoms and Computing (CLI) – Antoni Farriols: The Committee on Civil Liberties and Informatics works actively to defend the fundamental right to protection of personal data with the firm objective to sensitize citizens, business and government of the importance of the required standards in this area.³
- Association of Internauts – Javier Cuchí: Their main purpose of AI is advocacy, information, education protection of users and consumers of telephone communications and Internet.⁴
- Rafael Fernández Calvo (Journalist, consultant and professor of computer law. Socio de ATI (Asociación de Técnicos Informáticos), member of the Internet Society and Privacy International; co-founder of the CLI (Commission of Freedoms and Computing). Partner of ATI (Informatics Technics Association)⁵.
- Samuel Parra: Auditor and consultant on data protection.⁶
- Technology for Everyone (TxT) – David Franquesa: Association formed by people linked to the schools of computing and telecommunications at the UPC University.⁷

¹ <http://www.aui.es>

² <http://www.bufetalmeida.com>

³ <http://asociacioncli.es/>

⁴ <http://www.internautas.org/>

⁵ <http://www.ati.es>, <http://www.privacyinternational.org/>

⁶ <http://www.samuelparra.com/>

⁷ <http://txt.upc.edu>

- EdPAC – Carles Sedó: Education for Critical Action is a non-profit association founded by people linked to social intervention from various fields.⁸
- Catalan Data Protection Agency (APDCAT) – Esther Mitjans (director): The Spanish Data Protection Agency (Catalan agency).⁹

The notes collected from these interviews have been the basis for the summary of findings and the choice of topics to report in more detail.

The rest of this report is structured as follows: first we summarize the legal framework in Spain regarding privacy, second we present the summary and findings as a result of the interviews with different key persons and organizations, and third we include the fact sheets selected and compiled for this report.

Legal framework regarding Privacy

The Spanish Constitution (1978)¹⁰ recognizes in Section 18 the right to privacy (personal, family, home), secrecy of communications, data protection:

- “1. The right to honour, to personal and family privacy and to the own image is guaranteed.*
- 2. The home is inviolable. No entry or search may be made without the consent of the householder or a legal warrant, except in cases of flagrante delicto.*
- 3. Secrecy of communications is guaranteed, particularly regarding postal, telegraphic and telephonic communications, except in the event of a court order.*
- 4. The law shall restrict the use of data processing in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights.”*

Article 18.4 takes explicitly into consideration the legislative responsibilities regarding ICTs (data processing), and the the first data protection act (LORTAD, 1999), developed that article regulating archives containing personal data in automatized support.

The national laws that regulate on-line information and communication implement European Commission directives at the national level. The main laws are:

- The Data Protection Law¹¹ (LOPD, 1999), regulating the procedures manage databases with personal information, and privacy in general. It complies with the European Directive 95/46 CE.

⁸ <http://www.edpac.org/>

⁹ <http://www.apdcat.net/>

¹⁰ Spanish parliament (2003), *The Spanish constitution*: <http://narros.congreso.es/constitucion>

¹¹ *Boletín Oficial del Estado (1999) Ley Orgánica de Protección de Datos*
<http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf>

- The E-Commerce Law¹² (LSSI, 2002), implementing Directive 2000/31/CE, and partially Directive 98/27/CE; and Law 56/2007,¹³ of “Impulse Measures for the Information Society”. These laws deal with e-communications generally, and also regulate the provision of e-services, including the obligations around holding customer data. Amongst other things, they define universal service, the kinds of public information that must be published, e-government obligations, the obligations to service providers regarding customer support, as well as website requirements such as accessibility.
- The Telecommunications Law (Law 32/2003, 2003) regulating the use and exploitation of communication networks.
- The Electronic Signature Law (Law 59/2003, 2003), regulating the use of electronic signature by citizens, public administration and enterprises in economic activities.
- The E-Administration Law¹⁴ (LAECSP, 2007) recognises the right of citizens to on-line interaction with the public administration and obliges the government to guarantee that right.

At regional level each Spanish community (*Comunidad Autónoma*) has a law regulating different aspects from related with the Information Society and communications. For example in Catalonia there is the Catalan Protection Data Law (Law 5/2002, from Catalan Parliament), regulating all the aspects related with Information Society (development, application, regulations, norms, etc) in Catalonia, with special attention to data protection issues.

In addition to these, in Spain there are other national regulating normative like *Reales Decretos* and *normativa reglamentaria estatal*:

- Royal Decree 994/1999, to approve the regulation of the security measures related with automated files containing personal data.
- Royal Decree 1332/1994, to develop different aspects of the Law 5/1992, regulating the automatic treatment of personal data.
- Instruction 1/98, by the Protection Data Agency, related with the access rights to modify and cancel data.
- Instruction 1/2000, by the Protection Data Agency, related with the international movement of data.

The European Commission Directives that are considered in all the laws mentioned above are:

- Directive 95/46/CE of European Parliament and European Council (October 1995), related with data protection regarding people.
- Directive 2002/19/CE of European Parliament and European Council (March 2002), related with acces to electronic communication networks and their resources.

¹²Boletín Oficial del Estado (2002) Ley de Servicios de la Sociedad de la Información <http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf>

¹³Boletín Oficial del Estado (2007) Ley de Medidas de Impulso de la Sociedad de la Información <http://www.boe.es/boe/dias/2007/12/29/pdfs/A53701-53719.pdf>

¹⁴Boletín Oficial del Estado (2007) Acceso Electrónico de los Ciudadanos a los Servicios Públicos <http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf>

- Directive 2002/20/CE and Directive 2002/21/CE of European Parliament and European Council (March 2002), related with electronic communication services.
- Directive 1999/93/CE of European Parliament and European Council (December 1999), to establish a common "marc" for the electronic signature.

The Spanish Data Protection Agency¹⁵ is the government administrative institution working at different levels in the protection of personal data being processed in Spain. It was created based on the Data Protection Law from 1999. It is a public law body with legal personality and full public and private capacity to act independently of government in the exercise of their functions. The agency is in charge of supervising the compliance with data protection laws by those responsible for the files (public, private companies, associations, etc.)

At regional level there are regional Data Protection Agencies in each Spanish community working at a regional level. Currently there are three agencies (Madrid¹⁶, Euskadi¹⁷, Catalonia¹⁸). Their responsibilities cover publicly owned files created or managed by the respective autonomous communities, local administration, public universities and public law corporations.

Summary and findings from interviews

The following is a summary of the main findings obtained from the interviews. A more detailed summary of the topics and ideas raised from each interview is in a separate document which should not be made public as it contains opinions expressed during interviews from each of the experts.

General reflections on youth and ICT technologies

ICT technologies are sometimes linked to addictions, dependency, sedentary lifestyle, double personality pathologies (face to face and virtual), growing infantile behaviour (overprotection, less developed social awareness according to age). Concept of real isolation and individuality; distortion of reality (a false sense of sharing with friends while alone).

Although ICT technologies are a mean of identity for young people, in the end they can lead to non differentiation (everyone want to do or play the same). There is a standardization of the way of establishing relations in the social network; there is no respect to the identity, etc. There is as well a risk of supplant the place of others in relation to roles and personality.

ICT technologies do not offer much choice in deciding (young people with less freedom). There is the fantasy of control on a tool, while this is not true. Today, most young people do not care about controlling private information; they claim they have nothing to hide. In contrast, they see control

¹⁵ <http://www.agpd.es>

¹⁶ <http://www.madrid.org/apdcm>

¹⁷ <http://www.avpd.euskadi.net>

¹⁸ <http://www.apdcat.net>

as something which provides them greater safety and security (“as they are not ‘bad’, there’s no risk in being watched” ...). Since there is a false sense of security, they provide personal data without any caring, the more the better to rate highest or maximize visibility in the different applications. The false sense of intimacy that gives the screen invites people to express without restraint, which they are, what do they like, who are they dating with, etc.

In many situations and places there is great ignorance about the fact that the use of ICT technologies may pose problems for young people.

The boys, as they grow up, they dedicate longer time to the net relationships – or by mobile phone- and less time for listening to music, watching videos, view or practice sport or other interesting subjects.

Today, Internet is one of the least private places; it offers many possibilities for users but also a number of risks, which must be taken into account, if it is not used correctly. It means an uncontrolled expansion of personal data without taking into account the impact it can have, for example, when entering the job market, when it is too late, as it is nearly impossible to remove data from the public Internet space once that information is published.

In contrast, the most successful applications are those which facilitate aspects of life for user, but in exchange the information provided by them can be “exploited” by the service providers without the awareness of the originators.

There is a worrying lack of technological literacy. Absolute ignorance and lack of desire to learn about ICT technologies by many officials and policy makers. Service providers do not have interest in reporting on the dangers or risks associated with the use of their products (they simply highlight the benefits).

Widespread ignorance of people about what their rights in the digital world

One of the big problems is that young people are not receiving an education on the risks and limitations as parents and educators do not know or are not aware of them.

The advance of new technology is not progressing at the same time as the awareness on the importance of privacy control and exercising privacy rights.

The pursue of greater security or greater control on the intellectual property can invade other rights such as privacy or freedom of expression and we should not let this happen as it will imply that of our social progress goes backwards.

It is not the bad use they can make but the helplessness and lack of protection they suffer as users.

It is very important to grow the awareness from parents. They must try to educate children and youth in the use of ICT technologies from very young and guide them during youth. Parents should also be well aware that the computer is not any hobby for his/her son so they should "guide" and "accompany" them as much as possible.

About social networks

They are the most dangerous (especially for young people as they make a more intensive use), since there is still a great ignorance about their potential impact. Once privacy is lost, it is lost forever.

They are a network environment in which it is easier to disclose private information – that is the nature of the social network: being sociable –, and hence, as an open field, protection is lower and exposure is higher.

In this kind of applications, the best thing to do is to educate and inform taking into account the different age levels. Many young people don't know that some of the information they provide can end being used in many different ways than the original one. The privacy policies of companies do not help at all, they are rather "ambiguous policies" (unclear, often only in English, too long with a language or structure that makes them difficult to understand ...).

Trouble to apply the Spanish law to foreign companies (who shelter in more permissive laws such as in the U.S.'s ones). Another problem is the difficulty in contacting the organization when the affected person is not a member of the specific application.

We should make the enterprises more co-responsible of the security in them. An appropriate policy on confidentiality –with severe and effective administrative criminal responsibilities, in case of violation– could balance the plus of intimacy that they are given.

About mobile phones

In former times parents had more information, higher awareness, about the relations of their children (using the fixed mobile at home). Today that parental awareness is not that easy given the multiple alternative forms of communication.

The intrusion into the privacy of individuals has increased dramatically with increasingly sophisticated mobile phones with built-in camera. There is a lot of helplessness when these devices are badly used, as the legal system of protection and guarantees can only work when the violations of privacy has been consummated and detected their effects.

About databases

It is virtually impossible to control all of the databases; and this, like so many other things on the Internet is like wanting to put gates to the field. Once personal data is obtained, it can then be transferred or sold with little or no trace left; when data from two or more different sources is mixed, it is almost impossible to find the source to proceed with prosecution. And we must add to this that Internet is a “no-land” network that makes the pursuit almost impossible.

In principle and formally they are well protected and regulated by the Spanish Data Protection Agency and by their autonomous delegations. However, there are some areas (policing and state security) that are still fairly opaque and kept quite away from legal protection. There are also databases that are not registered in the Data Protection Agency and therefore outside any control.

It's important to ensure appropriate treatment of public data (from the administration they are increasingly realizing about the importance of providing such information and of getting it regularized).

In the commercial sphere personal information has a clear economic value. Great part of the power is in the user's hands that are the one who chooses to share his data and the one who can complain when he/she has been abused. He/she can also pressure and reclaim so that the companies react and rectify or report properly. However, in practice, this requires quite a lot of effort from individuals and the actions quite ineffective.

It is usually very easy to provide information, but very difficult to effectively access, control or remove afterwards. There are often too complex and extensive clauses, especially difficult for young people.

Legislation

A new reality has been created (globalisation) that blurs the concept of territoriality, and calls into question the very nature of the laws and the legal device associated.

The Spanish legislation is advanced; the LOPD is really tough and there are sufficient mechanisms, but apart from that, the main problem is that prosecutors are collapsed and can not be answered immediately neither preventively to abuses. There should be a much more proactive activity.

The current Data Protection law dates from 1999 and as a result of a European Directive of 1995. It is been 14 years since the basis for this right were established. An adaptation to the current reality is needed since otherwise anyone participating in any Internet-based system is in a dangerous position (e.g. creating a Blog).

The law is sufficient protectionist but does not differentiate between a large multinational that handles millions of data each day and a small business with two employees or an individual. This principle of equality is one of the major shortcomings of our current rules.

Right now, more than legislation, what is more necessary are the awareness campaigns in schools and universities.

Most of the experts interviewed insist on empowering users as the most effective measure for a significant effect.

Awareness of young people

The great majority ignore what is personal data, how it can be protected, or what rights protect them in the event of a possible violation of privacy.

It is striking to compare the amount of money the Government has spent on campaigns to raise awareness of "piracy" (P2P), while raising awareness about dangers of the loss of privacy on the Internet is almost forgotten.

We are experiencing a slight improvement in terms of awareness-raising efforts, but this occurs after a long period of no activity.

Overall, so far most common actions are quite limited to issues of harassment and addiction. Further awareness campaigns would be needed regarding pro-privacy issues, control of communications, business instrumentation / pro-consumption.

It's very important to explain the risks and there is a need of raise awareness, especially among the youth who are more vulnerable. Hence the importance of the responsibility of families and educators as facilitators of information required in this regard, without forgetting the subsidiary role of government to fill gaps in the field of training and information.

We must be careful –not just parents but the whole society or other civic groups– to the trends within and outside the network to anticipate and counteract these phenomena.

Conclusions and Recommendations

Nowadays there is a proliferation of intrusive technologies, but the most concern are those where the intrusion into privacy leaves some permanent effects, that means that once privacy is lost, it is lost forever (for example: social networks).

There's an absolute ignorance and lack of desire to learn about new technologies by many officials and policy makers. The laws require a greater application and response which is not given.

Legal conditions of many services are imported from Anglo-Saxon legal tradition countries (where the right to privacy does not have the protection that it is in the EU) and they try to place them in our system.

Social networks shouldn't be controlled by firms which mainly seek immediate economic benefit (with all that this implies, and the corresponding impact). As it is very difficult to influence directly to the policies of the current dominant network, it seems more feasible to promote real social alternatives where to have more impact and control.

Young people are not receiving an education on the risks and limitations as parents and educators do not know or are not aware of them (they face new situations without prior references and this involves some excessive risk-taking).

It is essential to raise awareness that can be developed from the civil society organizations and in its frame. In addition, parents should be more involved.

Establish codes of practice of use, transparency, participation and service for both Public Administrations and organizations in general.

In practical terms, when working with ICT applications and communications:

- Configure user profiles of applications with the greatest privacy level. Require that all applications have always restricted the options for privacy and asking the user to authorize any transfer of private information explicitly and giving information on the risks assumed and not vice versa (by request from the user).
- Never give personal information too easily, only the indispensable minimum, and do not provide information that is considered compromising if disclosed.

In terms of raising awareness and educating youth, there is need to:

- More accessible information on privacy regulations on products and services.
- More dissemination and awareness (e.g. awareness coming from social work organisations, government, service providers)
- The traditional and Internet-based communication media should be more involved in this work to reach more people.
- Internet has many advantages in communication, but it should be know better how to manage its risks.
- One can not expect the public authorities to make the necessary means to protect our privacy. We must take care of by ourselves.

In public policy terms, there is need to:

- Discuss a revised legislative framework at European level for the right of privacy and intellectual property management that is common and to analyse the network as a space of coexistence and well-being generation, wealth and power to all citizens.
- Establish codes of best practice of use, transparency, participation and service for both public administrations and organizations in general.
- Undesirable phenomena in the network start in the physical world. The priority is to pursue the illegal administrative “crime” in the real world, before attempting to censor the net.

In the individual sphere, there is the need to learn to turn off devices more often, to control them and do not let to be controlled, and interact more often face to face.

Related initiatives from the organizations contacted

APDCAT (Data Protection Catalan Agency)

The Data Protection Agency is focusing its force in strengthening information and training services to facilitate as much as possible young people to manage their own risk prevention.

The work done by CLI -Committee on Informatics and Liberties- during these last months must be highlighted (it has been done together with the all Spanish Data Protection agencies and the Education ministries): preparation of manuals for young people of different ages, to create later discussion and reflection with teachers in schools.

From the Agency, it is repeatedly requested to suppliers to provide greater transparency and to be more concise in their policies (they consider that the Government should be more demanding in this regard).

The Agency recently launched an on-line consultation in its website to help people to know the files with personal data related to them, so that they can learn the purpose, who are responsible for them, etc.

CLI (Committee on Civil Liberties and Informatics)

With the work started two years ago, the association has achieved that different entities have united to try to put the knowledge of the right to privacy and data protection as a priority for the younger population starting from the school age. They have also published advice on how to prevent problems associated with social networks.

The Committee on Civil Liberties and Informatics has developed a series of proposals¹⁹ which aim to improve the obvious shortcomings of the Spanish Data Protection law (LOPD) that has been delivered to the various parliamentary groups.

EDPAC (Education for Critical Action)

The Catalan Agency of Youth of the Catalan government initiated in 2005 the offer to all secondary schools preventive sessions on the topic of privacy within the program “schools pack”. It was soon the most requested workshop. The EdPac organization is responsible for developing and disseminating material on this topic. This educational material offers activities for social agents and young people facilitators who want to speak from a critical and careful point of view.

¹⁹ Proposals available at <http://www.asociacioncli.es/>

Far from a neutral view of the uses of these tools, the materials begin by trying to raise concern on how uncritically these tools are used, even though they establish a link between the use of them and certain situations among young people: such as individualisation, the increasing difficulty to speak and write properly, its definition as being consumers, his sedentary lifestyles, or the progressive control of their communications. They propose to involve more the families in these matters.

TxT (Technology for Everyone)

There are activities oriented to build a desirable vision of social networks (for example: current awareness and research project "Ecopuntura" with the UPC university): Assess impacts which are occurring in the current model -critic vision- and encourage the construction of "more free" alternative social networks, with a more real power of decision made by users and with more control of their information, not accessible to anyone (being careful for intimacy/privacy; so individuals will always decide, and in a more transparent way control who can see or cannot see his/her information), a social network which looks after individuals rights (more clear and transparent use conditions).

These alternative social networks would be a meeting point for people working or moving to certain common issues (to share resources and impacts -a very suitable model for the social organizations-). It has been being studied how to engage younger population (perhaps creating networks for schools, making awareness campaigns in schools on certain issues and that they can decide whether to be involved or not, and especially promote that parents also participate and share with their children. The idea is to recover the social life but also exploiting the advantages of the new tools). This projected social network will be more participatory, managed more collectively to take advantage of the communication capabilities it offers and to minimize the risks or misuses that currently derive from existing social networks.

FACT SHEETS

Based on the initial choice to topics, the interviews with experts from different organizations and our own experienced, we have selected the following topics and fact-sheets relevant to youth:

- Social networks (Facebook, Tuenti) are attracting many people, particularly the youth. These applications create opportunities to share personal information such as interests, ongoing activities, personal interests, list of friends, photos, audio and video clips. The bright side is how easily people can set-up groups of common interest, how easily self-made content can be published, and how easily content propagates through the social network. The dark side of it is the loss of control on personal information that is uploaded, that once made public it cannot be undone in practice as it can be exposed and copied in unexpected and undesirable ways; with exposure to personal attacks such as cyber-bullying, internet fraud or other types of harassment.
- Personal communications (mobile telephones, electronic mail, instant messaging). These are the main ICT based communication tools for youth. Recent mobile phones can include all possibilities and all the risks in one single small device that can be carried and used almost everywhere, with cameras that capture pictures, audio, video, internet connectivity (with web, email and instant messaging/chat), voice and short messages. The potential for communication is as large as the risks regarding privacy, which are enormous.
- Biological Identity (electronic identity card: DNLe, electronic passport, fingerprint databases): The most widespread effort that affects youth in terms of biological identity is the introduction of electronic identity cards. While for the rest of the population it will be introduced progressively as the old identity cards expire (every 10 years for adults and longer for elderly people), most youth will directly start using the new DNLe. In addition to the information printed in the card, it is also a smart card that contains a photograph of the face, the scanned copy of the handwritten signature, biometric fingerprints from both index fingers, and two digital certificates for the purposes of authentication and digital signature.
- Mobility (transport card).

I N T E R P E R S O N A L C O M M U N I C A T I O N S - M E S S E N G E R

THEME	Interpersonal communications
Identification of technology	Messenger (Instant messaging)
Technology used/tool (For each teams, a card pro tool)	Windows Messenger, Live Messenger, Chat applications, Google Talk, Skype (Chat mode)
Country/ use area	Spain ↔ world
Frame of use	<p>Interpersonal communications.</p> <p>In general communication between friends, family, etc. for personal use, for leisure.</p> <p>In some cases it is used at work for communications between employees, employees with the boss, etc. It could be just used for communications, or also as alerts systems, communications with clients (for client attention, for support to client, etc..)</p>
Population concerned: target and age	<p>Data from INE (Institute National Statistics) - 2008</p> <p>53,8% of spanish population is using Windows messenger and/or others instant messaging systems.</p> <p>People between 14 and 35 years old are the most important users of these technologies. Polls form INE shows an important decreasing in the use of instant messaging in people older than 35 years old.</p> <p>16-24 years old = 86%</p> <p>25-34 years old = 61,5%</p> <p>35-44 years old = 39,3%</p> <p>45-54 years old = 31,0%</p> <p>55-64 years old = 29,5%</p> <p>65-74 years old = 20,7%</p>
% of users/of young users	<p>Windows Messenger use (data from INE 2008)</p> <p>16-24 years old = 86%</p> <p>25-34 years old = 61,5%</p>
Trends (measured / supposed)	No data about tendency, but it is supposed that the use has been increasing in the last years, specially between youngers, but perhaps today the increasing rate is low just because the phenomom of the social networks.
Known or potentials dangers / Risks	Lies, exagerations, etc.. using this services are usual in some cases. Some people tend to lie about themselves to be more interesting in order establish relations with people. Sometimes they lie to trick people to do some things or to establish relationships with people of different

	<p>age, etc.</p> <p>People may be alienated if all their communications are using these systems, and may not have real personal communications.</p> <p>People may become unsocial, lonely, with difficulties to communicate in real life.</p> <p>In extreme situations some people can have really important health problems (problems of personality, depression, problems of communication...)</p> <p>There is also the danger of the «false identity». People can use another identity to send messages and communications which may be invented or impersonate anyone.</p> <p>e-bullying</p> <p>harassment</p> <p>«pedophilia» (some cases of pedophiles (child molesters) using these systems to contact with children and young people)</p> <p>grooming (Grooming: any action to affect morally or psicologically someone with the intention to achieve emotional control. Source INTECO. (www.observatorio.inteco.es))</p> <p>Possibility of creating profiles for people (companies can create profiles with personal data using the information given during the communications and kept in the historic files. They can know personal opinions, political tendencies, sexual tendencies..... and they can use the information for unknown purposes).</p>
others	
Generated data bases	
Associated data base/ creation (a line pro database)	<p>Users files (with all the data upload by the users)</p> <p>Use files (logs, list of users and acces data.)</p>
What justifies the inscription in the file /Risks?	To use the service
Purposes /contents, main data included / Risks?	In general this files are created and mantained in order to give the services.
File masters? Risks?	Files are controlled by companies owning the service
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Employees of theses companies

Data retention delays/ risks Right to be forgotten	
Rights to know or to modify data?	
Covert purposes/ Risks/uncontrolled future evolution	
Others (interconnections...)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	<p>LOPD, LSSI, LGT (Ley General de Telecomunicaciones) controlling these kind of services.</p> <p>Spanish laws for protection of honour, personal and family privacy and personal image are also competent for these subjects.</p> <p>At international level are also competent the «human rights declaration»(1948), International pact for civil and politic rights (1966)», International pact for economic, social and cultural rights (1966)</p>
Risks for freedoms despite the law	
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	
Conformity with the European right (Charter of fundamental rights, directives...)	<p>LOPD and LSSI are spanish laws directly related with the european community directives.</p> <p>Rome agreement from 1950 and European Union fundamental rights chart from 2000. are also competent in these subjects. Spanish laws take them into consideration.</p>
Implementation (or not) of the legislation? / Risks	
Others	
This tools and young public or young adults	
How far are young people concerned?	A high proportion of young people and young adults are not concerned of the risk related with the use of instant messagin services.

	For them instant messaging services are an important method of communication (mainly with friends and family, but sometimes also for work) , and they are easy to use, but only a few of them are more or less concerned with the security problems related and the good practices for using the service and protect their data and privacy.
Awareness of issues or of risks	In general they are unaware of the possibly risks, very few people use nicknames and don't give personal data, very few has some kind of control over their visibility in the service and who can contact with them.
Indifference or reaction	
Awareness campaigns/ results	EdPac (spanish association) has done a campaign with some materials explaining the habitual behaviour of youngsters using chats, how they can realise they has been become addicted «enganchados», some suggestions to make a good use of chats, etc.
Good practises	<p>AEPD has prepared an information documentation to inform about the instant messaging services and to give advise about using them, and also give some important recommendations (use a nickname, your nick not beig related with your personal data, not give personal data, not open or download images or files,...)</p> <p>INTECO (institute of new technologies of Spain) is doing some studies about instant messaging systems, specially concentrated in children and young adults. They are preparing a guide for good practices using instant messaging services, and some guides for parents ans teachers for educational purposes.</p>
Campaign to be led. On which themes?	
Others	
Conclusions	Instant messaging is a widespread tool in youth
Recommendations	Guidance, guidance is needed to be aware of the uses, and specially the risks of these tools in regard to privacy and the use of chats in public forums.

I N T E R P E R S O N A L C O M M U N I C A T I O N – E M A I L

THEME	Interpersonal Communications
Identification of technology	Electronic Mail messaging
Technology used/tool (For each teams, a card pro tool)	Internet Connection (modem, cable: ADSL, wireless: wifi) Mail protocols (POP, IMAP, Web, SMTP) User identified by e-mail address
Country/ use area	Spain - world
Frame of use	Different types of communication, sending files (text, images, music, video...), sending comercial information, administration information, cultural information, events, etc. Communications between people at personal level, for work, for leisure, for cultural purposes, for administration purposes (banks, government,...)
Population concerned: target and age	Wide range of ages, % of spain inhabitants are using mail messages: Data from IDESCAT (Institute of stadistics from Catalonia) indicates that 89,8% of Catalonia inhabitants use the mail.
% of users/of young users	??
Trends (measured / supposed)	The use of mail messages is really widespread in our country. It has increased very high in the lasts years. Today, a high % of spanish people has one or more email addresses and make an intensive use of this communication method for a lot of different purpuses. Data from IDESCAT. Use of mail in catalonia: 2006 – 86,9% 2007 – 90,3% 2008 – 89,8%
Known or potentials dangers / Risks	Spam viruses malware phising « fraudulent » comercial/information uses (not spam but unsolicited informations) False identity (using identity of another person to send emails) Problems with data protection (people sending emails with a lot of adresses not hidden. Increase the risk of receivng spam and

	viruses)
others	
Generated data bases	
Associated data base/ creation (a line pro database)	<p>Logs of use at ISP (logs for the use of the services)</p> <p>User files at ISP (files with users data, for accessing the service, and administratives purposes – payments-)</p> <p>Files at enterprises, organizations, government... for different purposes: comercial, information, services, public services (e.g. by goverment or local administrations)</p>
What justifies the inscription in the file /Risks?	<p>In general people are in these kind of files because they have solicited certain kind of services or they want to access certain services or informations.</p> <p>Many times too much data is required for accessing services, in general more than strictly needed for the service, and nearly always without explanation about what it will be done with that data.</p>
Purposes /contents, main data included / Risks?	<p>In general theses files are needed for:</p> <ul style="list-style-type: none"> - control purposes in order to give a service, or - for control of use in order to give a good service, or - to comply with the spanish law, or - for payment of the services.
File masters? Risks?	<p>ISP</p> <p>enterprises</p> <p>administration</p>
Who accesses the files/ Sharing of the data base? Access limits? /Risks	<p>Enterprise/administration who own the file,</p> <p>Some enterprises belonging to a group use to pass the files between partners. (sometimes not clearly specified to the user)</p> <p>rs.</p>
Data retention delays/ risks Right to be forgotten	<p>ISP logs – 1 year</p> <p>Other files – unknown</p>
Rights to know or to modify data?	<p>User have rights to acces, modified or cancel data as specified at Spanish law but sometimes it is not clearly explained how to do it, which are the rights, or the enterprises doesn't accomplish with the modifications requested by users.</p>
Covert purposes/ Risks/uncontrolled future evolution	?

Others (interconnections...)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	Spanish laws: LOPD, LSSI and others. Spanish laws for protection of honour, personal and family privacy and personal image are also competent for these subjects.
Risks for freedoms despite the law	Some bad practices by the service providers (abusive conditions to give a service, not clear information to the users, ...)
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	
Conformity with the European right (Charter of fundamental rights, directives...)	Yes LOPD and LSSI are Spanish laws directly related with European community directives.
Implementation (or not) of the legislation? / Risks	
Others	
This tools and young public or young adults	
How far are young people concerned?	
Awareness of issues or of risks	In general people are not conscious about the possible risks of using mail messages. Too many times people send massive messages without hiding the addresses, so they are making public private data from other people. They are unconscious on how easy is to collect mail addresses from their emails by the companies in order to use them for commercial purposes, for sending spam, for spreading viruses, etc.
Indifference or reaction	
Awareness campaigns/ results	AEPD has some materials prepared in order to educate people in the good practices for using mail services and also other Internet services. They are doing educational campaigns in primary and secondary schools.
Good practises	Some recommendations by AEPD:

	<ul style="list-style-type: none"> • to use a nickname • not to give too much personal data in your email address • to choose a good password and change it periodically • maintain as private as possible our email address • to use the BCC field to send massive messages • to use secure methods for sending mails • configure your mail client with a good level of security and activate the spam filters, and viruses filters • not use the option for saving password • update your mail client frequently • avoid to send chain messages
Campaign to be led. On which themes?	Campaigns to educate people in the good practices to use the mail service
Others	
Conclusions	Email is under a situation of abuse and overload. Education on good practices is key.
Recommendations	Campaigns to educate people in the good practices to use the mail service.

THEME	Interpersonal communications
Identification of technology	Mobile telephony
Technology used/tool (For each teams, a card pro tool)	Data connection (voice, video, data), Internet connection (wifi, modem...), mail (pop, imap, smtp), sms, web,
Country/ use area	Spain <->world
Frame of use	<p>Personal communications, Social relations, friendship, downloading files (music, videos, games..), to play, comercial uses, administrative issues (bank messages, messages related with credit card payments, ...) activism ?</p> <p>Data from Fundacion BBVA (june 2008)</p> <ul style="list-style-type: none"> → sms = 68,9% → photos camera = 50,7% → bluetooth = 33,7% → video (record/watching) = 32,8% → games = 29,3% → mms = 28,2% → download music, logos, images = 21,2% → mp3 = 19,5 % → radio = 16,1% → Internet = 8,4% <p>Data from Fundacion BBVA (june 2008) uses by ages:</p> <ul style="list-style-type: none"> → sms (14-25years old) = 87% → sms (26-35years old) = 76,3% → sms (36-50years old) = 53,8% → sms (51-65years old) = 28,6% → camera (14-25years old) = 55,2% → camera (26-35years old) = 37,1% → camera (36-50years old) = 24,8% → camera (51-65years old) = 8,4% → bluetooth (14-25years old) = 43%

- bluetooth (26-35years old) = 25,4%
- bluetooth (36-50years old) = 12,5%
- bluetooth (51-65years old) = 4,1%
- video (14-25years old) = 36%
- video (26-35years old) = 19,5%
- video (36-50years old) = 10,1%
- video (51-65years old) = 2,8%
- games (14-25years old) = 38,6%
- games (26-35years old) = 16,8%
- games (36-50years old) = 6,8%
- games (51-65years old) = 1,7%

Data from The 3r Observatorio de Tendencias (3r Trends watch) :

Young people using mobile phone to access the internet mainly search for information (76%), receive/send email messages (68%), looking for addresses and routes (58%), instant messages (55%).

Young people are interested in using more services at mobile phones.

GPS services = 52%

email = 39%

surfing on the web = 34%

Population concerned:
target and age

A wide range of ages, important number of young people.

Data (Fundación BBVA study from June2008)

83,3% of Spanish population use mobile phone

->Data by genre:

Men – 84,4% / Women – 82,2%

->Data by social class

high-medium = 93,8%

medium = 89 %

medium-low = 70%

->Data by age:

14-25 = 95,2%

26-35 = 97%

36-50 = 94,4 %

51-65 = 79,3 %

	66 and older = 44,5%
% of users/of young users	<p>Data from Fundacion BBVA use of mobile phone by age:</p> <p>14-25 = 95,2%</p> <p>26-35 = 97%</p> <p>Data from INE (Spanish Institute of statistics):</p> <p>In 2004 the use of mobile phones by people under 15 years old was of 52,3%</p> <p>In 2008 the use of mobile phones by people under 15 years old is of 78,5%</p>
Trends (measured / supposed)	<p>In general there is a notable increase in the use of mobile phones in Spain.</p> <p>Data from Fundación BBVA:</p> <p>mobile phone use in 2005 = 75%</p> <p>mobile phone use in 2008 = 83,3%</p> <p>The 3r Observatorio de Tendencias (3r Trends watch) says that the use of mobile phones by young people has increased 64% in the last year.</p> <p>Important increase of the mobile as a way to acces Internet and Internet services (the « low » prices offered by mobile phone companies permits more and more young people to have Internet connection on their mobile phone.</p> <p>The 3r Observatorio de Tendencias (3r Trends watch) says that the use of mobile phones by young people as a way to access the Internet has increased from 8% to 19% in just 6 months.</p> <p>Young people is the group that spends more hours connected to Internet by the mobile phone. On average young people spend 2.6 horus per week, but people from 15 to 19 years old is spending 3.5 hours per week.</p> <p>The tendency is to continue increasing.</p> <p>And the age young people is having their first mobile phone is lower and lower.</p>
Known or potentials dangers / Risks	<ul style="list-style-type: none"> - Leaving personal data for downloading files, for accesing services, etc. - Using the mobile for spying, for buylling, for harassment. - Modern mobile phones have better cameras (photo and video) and they are being used for «illegal/bad» actions (buylling, harassment...). Different cases in Spain at secondary school (harasement againts teachers or other classmates), at the street against people at street or

	<p>homeless or ancient people.</p> <ul style="list-style-type: none"> - Simply used to take photos or videos without the permission of the people appearing in them. - Potential control / location of people based on the position of their mobile phone. (Different services of these type are being offered by some companies, for exemple Google applications for mobile phones (Latitude) in order to use it as a GPS and to locate where you are).
others	
Generated data bases	
Associated data base/ creation (a line pro database)	<p>Logs at mobile phone companies.</p> <p>User files at mobile companies (to give the service and payments)</p> <p>Files at companies for downloading files</p>
What justifies the inscription in the file /Risks?	To have the service offered by the company
Purposes /contents, main data included / Risks?	For giving the services
File masters? Risks?	Files are controlled by the companies (mobile phone companies, companies to doownload files...)
Who accesses the files/ Sharing of the data base? Access limits? /Risks	<p>Employees of theses companies</p> <p>Possible cession of data file between companies ?</p>
Data retention delays/ risks Right to be forgotten	
Rights to know or to modify data?	There are the rights established by the Spanish law of data protection, to acces, rectify or cancel data. But sometimes it is difficult for people to find what they have to do, or where there are the forms to do it (complex language, small fonts and messages hidden as much as possible create difficulties to people for exercise their rights).
Covert purposes/ Risks/uncontrolled future evolution	Companies use the data files with comercial purposes. Sometimes the files are shared between companies of the same group of enterprises for treatment with comercial purposes and it's possible that people don't know these kind of actions are possible. In general there is lack of information about what the companies are doing with the personal data.
Others (interconnections...)	

Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	In Spain LOPD and LSSI are the laws controlling these type of services.
Risks for freedoms despite the law	
If revision of the regulation: reasons?	
Conformity with the European right (Charter of fundamental rights, directives...)	LOPD and LSSI are spanish laws directly related with the European community directives
Implementation (or not) of the legislation? / Risks	<p>In general companies are applying the law, but some practices are in the border line of the law.</p> <p>Some companies are more conscious of data protection and are giving the users the opportunity to define the level of consentment they give to treat their data.</p> <p>Some companies also consult available list of people that don't want to receive comercial publicity.</p>
Others	<p>Sometimes companies apply the law but put difficulties to people for exercising their rights (hidden messages, small fonts, complicated systems for the submission of complaints, etc). So the law could be correct, but a revision of its application and interpretation could be needed in some cases.</p> <p>In general people are really misinformed about their rights and suffer the abuses of companies without complaining.</p>
This tools and young public or young adults	
How far are young people concerned?	The 3r Observatorio de Tendencias (3r Trends watch) says that young people use the mobile phone as a tool for keep in contact with friends and have fun, but they don't think they are mobile dependant. 58% thinks mobile simplifies and improve their social relations, and 51% thinks mobile is a tolls for fun, games, music and photos.
Awareness of issues or of risks	They are not really concerned with the possible dangers related with the mobile phones usage.
Indifference or reaction	
Awareness campaigns/ results	<p>http://www.elpep.info/mobil.htm</p> <p>Campaing from EDPAC association to inform young people about the</p>

	good practices using mobiles, about bad practices, giving advice, etc.
Good practises	Some companies like Movistar are working in offering mobile phone packs specially for children and young people. These packs have games, music, etc for children but also some mechanisms of control for parents (controlling costs, controlling the SMS and calls, ...).
Campaign to be led. On which themes?	Dissemination of good practices using mobiles, warn about bad practices, giving advice.
Others	
Conclusions	Mobile telephones is an ubiquitous ICT device that is always on and always on the pocket of youth, and it is being used as the basis for almost all communication acts (text, audio, chats, email, video, web).
Recommendations	Campaigning on the responsible and effective uses of these devices, informing about the risks.

M O B I L I T Y – T R A V E L C A R D S (P U B L I C T R A N S P O R T)

THEME	Mobility
Identification of technology	Travel Cards (Public Transport)
Technology used/tool (For each teams, a card pro tool)	RFID
Country/ use area	Spain
Frame of use	Urban transportation
Population concerned: target and age	Both sexes and all ages Spanish citizens (including young population)
% of users/of young users	Approximately, 55% of young people (data from RACC study, april 2009)
Trends (measured / supposed)	Until recently, the transportation cards were made of cardboard with magnetic stripe. Some cards also added some personal information such as passenger name and ID card number. But for some time now are being implemented in Spanish cities a new kind of transportation cards with RFID chip (Malaga, Madrid, Valencia and soon in Barcelona) under the unclear name of "smart cards". The fact that no mention officially the use of this technology gives us much to think and suspect.
Known or potentials dangers / Risks	Most people do not know yet what is the RFID technology and therefore remain oblivious to their potential risks, particularly as may be the monitoring and control of their movements.
others	...
Generated data bases	
Associated data base/ creation	User data files at transport companies
What justifies the inscription in the file /Risks?	To have the service offered by the company
Purposes /contents, main data included / Risks?	Formalism to access the service offered by the company. To control the service and payments. The data could be used by the transport company for other purposes: cession of data file to other related companies, monitoring the user's routes...
File masters? Risks?	The transport companies.
Who accesses the	Employees of these companies, users (and maybe Public

files/ Sharing of the data base? Access limits? /Risks	administration) Possible cession of data file between related companies??
Data retention delays/ risks Right to be forgotten	The law establish the conservation of some files during one year. Also the companies could not accomplish the law and keep the files as long as they want (In spanish law the companies has the right to keep some files/some data as historical information).
Rights to know or to modify data?	There are the rights established by the Spanish law of data protection, to access, rectify or cancel data. But sometimes it's difficult for people to find what they have to do, or where there are the forms to do it...
Covert purposes/ Risks/uncontrolled future evolution	Control the user's movements, commercial purposes...? This could evolve into a surveillance state too oppressive.
Others (interconnections...)	...
Legislation in application	
Law /rules / others	In Spain LOPD and LSSI are the laws controlling these type of services.
Risks for freedoms despite the law	Usually, the contracts are not clear and not well specified, so it's difficult for people to understand what they are signing (most users don't know anything about the RFID technology that they are going to use...)
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	...
Conformity with the European right (Charter of fundamental rights, directives...)	LOPD and LSSI are Spanish laws directly related with the European community directives
Implementation (or not) of the legislation? / Risks	In general companies are applying the law, but some practices are in the border line of the law.
Others	In general, people are really misinformed about their rights and suffer the abuses of companies without complaining.
This tools and young public or young adults	
How far are young people concerned?	They are absolutely not concerned with the possible dangers of their transportation cards, and specially with the new RFID technology.
Awareness of issues or of	In general, the whole population is unaware of the dangers behind the

risks	use of RFID technology.
Indifference or reaction	...
Awareness campaigns/ results	So far, nothing is known about campaigns or actions.
Good practises	It would be convenient to inform about the technology of the new transportation cards and explain clearly why it's used...
Campaign to be led. On which themes?	More information about the new transportation cards and RFID.
Others	...
Conclusions	Transportation cards differ very much among diverse areas, implementations are diverse and the information about them is fragmented, and not publicly available.
Recommendations	Investigate the issues related to private data in transport cards to let citizens know what personal information is used in each.

THEME	Biological Identity
Identification of technology	DNle (electronic national document of identity)
Technology used/tool (For each teams, a card pro tool)	Chips, digital certificates
Country/ use area	Spain
Frame of use	<p>All Spanish citizens have an oficial document to identify them, to accredit them physically. This document is given by the Interior Ministry of Spain and is used to identify each Spanish citizen and is needed for a lot of things (administration functions, bank operations, studies, shopping, home services -electricity, gas, water, phone).</p> <p>Since March-2006 DNI has a new format, it is a digital one (DNle). The new DNI has a chip that keeps inside the same information in the old one (name, surname, date of birth, place where you live, a unique number to identify you, your photo and your signature and your fingerprints) and two digital certificates (auth certificate, and digital signature certificate). The DNle accredits person in a physical and also in a digital way. It is mandatory by law to carry the identity card all the time.</p> <p>The DNle could be use for the same purposes of the old one, and also for doing diferent types of operations using electronic/telematic methods (operations related with goverment and administration, with the Treasure ministry/spanish Tax Authority « Hacienda Pública Española » , also for comercial operations using electronic methods (shopping in Internet,...- or operation with banks, ...</p> <p>The Authentication certificate serves to identify the owner of the card – DNle– in telematic communications. And the digital signature certificate serves to warranty the integrity and the procedence of the document as well as the autenticity of its origin.</p>
Population concerned: target and age	All spanish citizens.
% of users/of young users	All spanish citizens.
Trends (measured / supposed)	DNle started in March 2006 in the city of Burgos. Since then it has been spreading slowly to all the Spanish territory, Today it is given in all the regions and citizens could ask for change

	they DNI for a DNle or otherwise when the DNI expires it is automatically changed by the DNle.
Known or potentials dangers / Risks	<p>Is it secure enough?</p> <p>The DNle has a microprocessor that performs internally all the cryptographic operations (key generation, electronic signature). To use the chip the PIN has to be introduced. The future will tell depending on the attacks.</p> <p>What more information could be kept in?</p> <p>There is room for additional information on the chip.</p> <p>Is it possible for someone to steal your digital identity?</p> <p>The PIN can be obtained when used in fraudulent readers or keyloggers in PC.</p>
others	If the DNle is lost or stolen the citizen has to revoke the electronic certificates included.
Generated data bases	
Associated data base/ creation	Files containing all the data in the DNle.
What justifies the inscription in the file /Risks?	To identify physically and digitally every citizen. It is compulsory by law in Spain the carry and be identified by a DNI.
Purposes /contents, main data included / Risks?	To identify citizens
File masters? Risks?	<p>The National Police is the authority that is in charge of the DNI and DNle.</p> <p>The National Police is the one who controls the data files, who gives the DNle, who is in charge of renewals, of helping citizens with this subject, etc.</p>
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Only the National Police
Data retention delays/ risks	Always
Right to be forgotten	
Rights to know or to modify data?	The National Police has the tools needed to renew, recover, to make corrections on data, etc.
Covert purposes/ Risks/uncontrolled future evolution	
Others (interconnections...)	
Legislation in application	

<p>Law /rules / others (?)</p> <p>(implemented for this data base or this technology)</p>	<p>These are the laws which regulates the DNIE:</p> <ul style="list-style-type: none"> - Spanish organic law on protection of citizen security: Ley Orgánica 1/1992, de 21 de febrero, on „Protección de la Seguridad Ciudadana“ (<i>BOE núm. 46, de 22 de febrero</i>), en su redacción dada por la Disposición Adicional Cuarta de la Ley Orgánica 4/1997, de 4 de agosto (<i>BOE núm. 186, de 5 de agosto</i>) y por la Ley 10/1999, de 21 de abril (<i>BOE núm. 96, de 22 de abril</i>). - Spanish law on expedition of DNI: Ley 84/1978, de 28 de diciembre, por la que se regula la tasa por expedición del Documento Nacional de Identidad (<i>BOE núm. 11, de 12 de enero de 1979</i>), en su redacción dada por la Ley 11/2007, de 22 de junio (BOE núm. 150, de 23 de junio) y por la Ley 2/2008, de 23 de diciembre (BOE núm. 309, de 24 de diciembre). - Spanish law on electronic signature: Ley 59/2003, de 19 de diciembre, de firma electrónica, artículos 15 y 16 (BOE núm. 304, de 20 de diciembre). - Spanish law on expedition of electronic DNI: Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica (BOE núm. 307, de 24 de diciembre). - Spanish order on the practices and policies for certification: Orden INT/738/2006, de 13 de marzo, por la que se aprueba la declaración de prácticas y políticas de certificación del Ministerio del Interior (BOE núm. 64, de 16 de marzo).
<p>Risks for freedoms despite the law</p>	
<p>If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)</p>	
<p>Conformity with the European right (Charter of fundamental rights, directives...)</p>	
<p>Implementation (or not) of the legislation? / Risks</p>	

Others	
This tools and young public or young adults	
How far are young people concerned?	
Awareness of issues or of risks	
Indifference or reaction	
Awareness campaigns/ results	
Good practises	
Campaign to be led. On which themes?	
Others	
Conclusions	The DNle extends the traditional DNI card with additional data in digital format.
Recommendations	Inform citizens about practices in other countries to let them compare. Inform on the added risks induced by the digital information contained in the card.

BIOLOGICAL INFO – FINGERPRINT DATABASES

THEME	Biological Identity
Identification of technology	Fingerprint (access to gyms)
Technology used/tool	Biometric data
Country/ use area	Spain/Catalonia/BCN
Frame of use	Each time a user wants access to gyms with this kind of access technology.
Population concerned: target and age	Both sexes and mainly young people and adults.
% of users/of young users	A high percentage of young people often go to gyms & sports centers.
Trends (measured / supposed)	Many gyms (Ubae, DIR...) have changed in recent times the old mechanisms of access with biometric technology systems.
Known or potentials dangers / Risks	Most people still don't know what biometric technology is or how it works, so they remain oblivious to their potential risks, particularly as may be the monitoring and control of their habits and movements, the transfer of data to other entities or commercial purposes.
others	...
Generated data bases	
Associated data base/ creation (a line pro database)	Files containing all the personal data of users in the gym's databases.
What justifies the inscription in the file /Risks?	To identify the users and to have the service offered by the gyms.
Purposes /contents, main data included / Risks?	Formalism to access the service offered by the gyms. Presumably, to control the access more effectively and safely. The data could be used by the companies for other purposes: cession of data file to other related companies, monitoring the user's habits...
File masters? Risks?	The managers of the gyms. They should: <ul style="list-style-type: none"> - Register the file in the Data Protection Agency. - Notify the owner of the fingerprint that their data will be stored in a database and purpose. They must also communicate their right of access, rectification, cancellation and opposition. - If they transfer the data to other people, will also need written permission from the owner of the data.

Who accesses the files/ Sharing of the data base? Access limits? /Risks	Employees of the gyms and the users themselves.
Data retention delays/ risks Right to be forgotten	The law establish the conservation of some files during one year. Also the companies could not accomplish the law and keep the files as long as they want (In spanish law the companies has the right to keep some files/some data as historical information).
Rights to know or to modify data?	There are the rights established by the spanish law of data protection, to access, rectify or cancel data.
Covert purposes/ Risks/uncontrolled future evolution	Control the user's habits and movements. Transfer data. Commercial purposes... This could evolve into a surveillance state too oppressive.
Others (interconnections...)	...
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	In Spain LOPD and LSSI are the laws controlling these type of services (the fingerprint is included in the LOPD, like for example a photo; both are personal data).
Risks for freedoms despite the law	Excessive control and monitoring of users without informing enough.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	...
Conformity with the European right (Charter of fundamental rights, directives...)	The Spanish laws are directly related with the European community directives
Implementation (or not) of the legislation? / Risks	...
Others	...
This tools and young public or young adults	
How far are young people concerned?	They are absolutely not concerned with the possible risks or dangers of the biometric data technology.

Awareness of issues or of risks	In general, the whole population is quite uninformed and unaware of the risks behind the use of biometric data.
Indifference or reaction	...
Awareness campaigns/ results	So far, nothing is known about campaigns or actions about biometric data in our country.
Good practises	It would be convenient to inform about this type of technology and its risks and explain clearly why it's used.
Campaign to be led. On which themes?	More information about the new access systems.
Others	...
Conclusions	Growing use of these cards among youth
Recommendations	Inform on the info stored in these cards, uses and risks of them.

B I O L O G I C A L I N F O – E L E C T R O N I C P A S S P O R T

THEME	Biological Identity
Identification of technology	Electronic Passport
Technology used/tool	RFID, biometric data
Country/ use area	Spain/World
Frame of use	Extra-UE travels (since august 2006 Spanish passport has a new format: electronic one)
Population concerned: target and age	Both sexes and all ages Spanish citizens (including young population)
% of users/of young users	All Spanish citizens traveling to destinations outside EU.
Trends (measured / supposed)	Electronic passport started in Spain in august 2006. Just as the DNIe, since then it has been spreading slowly to all the Spanish territory.
Known or potentials dangers / Risks	Most people do not know yet what is the RFID technology and therefore remain oblivious to their potential risks, particularly as may be the monitoring and control of their movements, or the falsifications.
others	...
Generated data bases	
Associated data base/ creation (a line pro database)	Files containing all the personal data in the electronic passports.
What justifies the inscription in the file /Risks?	To identify physically and digitally the citizen. Risks: Falsifications, "phishing"...
Purposes /contents, main data included / Risks?	To identify citizens.
File masters? Risks?	The National Police is the authority that is in charge of the electronic passport and DNIe. The National Police is the one who controls the data files, who gives the new passport, who is in charge of renewals, etc. Possible risks: monitoring of citizens without informing/respecting the presumption of innocence...
Who accesses the files/ Sharing of the data base? Access limits? /Risks	The members of National Police. The citizen's personal data can easily be shared with police and security personnel from other countries...

Data retention delays/ risks	Always.
Right to be forgotten	
Rights to know or to modify data?	The National Police has the tools needed to renew, recover, to make corrections on data, etc...
Covert purposes/ Risks/uncontrolled future evolution	Control the citizen's movements, surveillance. Identity falsifications. This could evolve into a surveillance state too oppressive (as is already happening in the U.S. ...)
Others (interconnections...)	...
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	Ley Orgánica 1/1992 , de 21 de febrero, sobre Protección de la Seguridad Ciudadana (<i>BOE núm. 46, de 22 de febrero</i>) <i>Modificaciones : LO 4/1997 -BOE 186, de 5 de agosto. Ley 10/1999 -BOE núm. 96, de 22 de abril.</i> Real Decreto 896/2003 , de 11 de julio, por el que se regula la expedición del pasaporte ordinario y se determinan sus características (<i>BOE núm. 166, de 12 de julio</i>).
Risks for freedoms despite the law	Excessive control and monitoring of citizens without informing/respecting the presumption of innocence.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	...
Conformity with the European right (Charter of fundamental rights, directives...)	The Spanish laws are directly related with the European community directives.
Implementation (or not) of the legislation? / Risks	...
Others	...
This tools and young public or young adults	
How far are young people concerned?	They are absolutely not concerned with the possible risks of their biometric passports, and specially with the new RFID technology.
Awareness of issues or of risks	In general, the whole population is unaware of the risks behind the use of RFID technology.

Indifference or reaction	...
Awareness campaigns/ results	So far, nothing is known about campaigns or actions...
Good practises	It would be convenient to inform about the technology of the new biometric passports and explain clearly how the digital information is used in different situations and countries.
Campaign to be led. On which themes?	More information about the privacy implications of the implications of digital data included in the passport (RFID).
Others	...
Conclusions	The ePassport contains information in digital format that is not clearly visible to the citizens and that they may ignore its presence and how it is used.
Recommendations	Need for strong limitations at EU level on the use of biometric passports, especially with regards to children and with regards to centralized databases.

THEME	Social Networks - Tuenti
Identification of technology	Internet connection, web services, mail services, instant mail,
Technology used/tool	Web, instant messaging
Country/ use area	Spain <->world
Frame of use	<p>Personal communications, Social relations, friendship, obtaining information, groups of interest, job, comercial uses, activism ?</p> <p>Data from INTECO, uses of social networks by spanish users (date of the study = october 2008)</p> <p>upload/share photos = 70,9%</p> <p>Send private messages = 62,1%</p> <p>Comments on friends's photos = 55%</p> <p>profile update = 52,1%</p> <p>send public messages = 50,2%</p> <p>gossip = 46,2%</p> <p>Label friends at photos = 34,8%</p> <p>Search for information = 25%</p> <p>downloading software = 19,3%</p> <p>downloading games = 9,5%</p> <p>Search for job = 8,5%</p>
Population concerned: target and age	<p>A wide range of ages, important number of young people.</p> <p>Data from INTECO – national institute of communications technologies-</p> <p>In Spain 44,6% of internauts are using Social networks (which represents more or less 7.850.000 people)</p>
% of users/of young users	<p>Data from INTECO</p> <p>Use of the social networks by age:</p> <p>36,5% are users between 15 to 24 years old</p> <p>32,5% are users between 25-34 years old</p> <p>Data from IDESCAT (Institute of Stadistics fo Catalonia), use fo Internet in Catalonia by age:</p> <p>→ 16-24 years = 93,5%</p> <p>→ 25-34 years = 84,9%</p> <p>Data from IDESCAT (Institute of Stadistics fo Catalonia), frequency in</p>

	<p>the use of Internet in Catalonia by age:</p> <ul style="list-style-type: none"> → 16-24 years = 73,6% every day → 25-34 years = 66,2% every day → 16-24 years = 21,1% once or more a week → 25-34 years = 27,3% once or more a week <p>Data from INTECO, use of social networks by ages (date fo the study = july 2008):</p> <ul style="list-style-type: none"> → people from 14-20 years Tuenti = 31% → people from 21-30 years Tuenti = 18% → people from 31-40 years Tuenti = 2%
Trends (measured / supposed)	<p>Fast increasing in a short time period.</p> <p>And the tendency is to continue increasing rapidly. In the case of Tuenti specially between young people in Spain and Latinamerica (spanish language countries).</p>
Known or potentials dangers / Risks	<p>Too many personal and private data available on the network</p> <p>Data accesible by lots of people</p> <p>loss of the privacy</p> <p>loss of the control of your own data</p> <p>illegal / not specified use of the data</p> <p>possibility of control of a people</p> <p>spying</p> <p>getting information of people from the job (control by boss, avaiable data of possible employees...)</p> <p>bullying</p> <p>harasement</p> <p>receiving spam and comercial messages or adds. In general it's a specific spam, so implies that th net is using the information recolleted to choose the adds people could be interested in.</p> <p>international transfer of data (some networks have their servers in third countries,).</p> <p>Installation of cookies without the consent/approval of the user to recover/ control information and activities and use of the net by the user</p>

	<p>identity theft</p> <p>difficulties to delete accounts and data related</p> <p>possibility of indexing contents/data by search engines</p>
others	<p>Poor control of privacy by users</p> <p>default profiles with very low security and protection of data</p> <p>missing information about uses of data, rights of users,...</p> <p>not clear contracts (not easy to read, too long, too specific language...)</p> <p>problems to cancel/delete data</p> <p>people is not conscious about all the possible problems and situations that can occur using a social network</p> <p>people don't know the law and the possible faults they are committing uploading third person data to a social network</p>
Generated data bases	
Associated data base/ creation (a line pro database)	<p>Users files (with all the data upload by the users)</p> <p>Use files (logs, list of users and access data..)</p>
What justifies the inscription in the file /Risks?	To be part of the network and to access the services available
Purposes /contents, main data included / Risks?	<p>In general this files are created and maintained in order to give the services.</p> <p>These files keeps user's data necessary to register in the social network, data uploaded/published by users</p> <p>Possible risks: they could be use for more purposes than the ones specifically needed to give the service. They could be sent to other companies for other purposes (advertisements, sending information to the users, studying trends, having statistic information,...). The data could be used by the social network company for other activities and they can obtain benefits from the user's data (normally the legal conditions signed to enter a social network imply the cession of all their data and contents they upload to the network)</p>
File masters? Risks?	Files are controlled by companies owning the social networks
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Employees of these companies
Data retention delays/ risks Right to be forgotten	The law establish the conservation of some files during one year. But there is no specifications for other files. Also the companies could not accomplish the law and keep the files as long as they want. In spanish

	<p>law the companies has the right to keep some files/some data as historical information.</p> <p>It seems that there are some contradictions between rights/obligations of the companies.</p>
Rights to know or to modify data?	Depending on the network
Covert purposes/ Risks/uncontrolled future evolution	?
Others (interconnections...)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	<p>In Spain LOPD and LSSI are the laws controlling these type of services.</p> <p>Tuenti has signed recently the european agreement about social networks (see on: http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm)</p> <p>On July-2009 AEPD (Spanish protection data agency) has subscribed some agreements with Tuenti in order to delete all under 14 years old people profiles. And also to improve methods for controlling the registration/acces at the network from young people and children.</p> <p>Spanish laws for protection of honour, personal and family privacy and personal image are also competent for these subjects.</p> <p>At international level are also competent the «human rights declaration »(1948), International pact for civil and politic rights (1966)», International pact for economic, social and cultural rights (1966)</p>
Risks for freedoms despite the law	<p>Social networks use to have contracts really abusive in order to have total rights over all the data/contents uploaded by users.</p> <p>The contracts are not clear and not well specified, so it's difficult for people to understand what they are signing. In general they are too long, with very confusing redaction, specialized terminology...</p> <p>There are not enough security mesures available in the social networks, the implementation of new mesures, and moreover, the implementation of control methods for avoiding young people under aged could register/use these social networks.</p>
If revision of the regulation: reasons? Result: improvement or aggravation (compared to	Some revisions of the law could be needed, but the most important thing is to apply the law in the cases it is being not accomplished.

the protection of the DP)	
Conformity with the European right (Charter of fundamental rights, directives...)	LOPD and LSSI are spanish laws directly related with the european community directives
Implementation (or not) of the legislation? / Risks	Tuenti is applying the spanish laws and is collaborating with AEPD and administrations in improving its network.
Others	
This tools and young public or young adults	
How far are young people concerned?	<p>They are not concerned with the dangers of these social networks, or with the possible faults they can commit uploading certain type of contents (for exemple photos of friends without permission, or data of other people without permission...). It's easy for them to use the technology but they need to learn how to use it in a safer way and also they need to learn about the law (what can be done and what cannot be done).</p> <p>They are unaware of the use that these companies can do with their data.</p> <p>They are unaware of the dangerous consequences that the loss of their privacy could imply now and in the future (information could be available on the Internet during a lot of time, information it's available for people who can use it for ilegal activities)</p> <p>Data from INTECO, security of profiles in social networks (date october-december 2007)</p> <p>48% have a profile accesible by friends, and friends of friends</p> <p>43% have a profile accesible by everybody</p> <p>6% have a private profile</p> <p>3% don't know what type of profile they have</p> <p>In Tuenti's blog you can read some comments of the Tuenti' users about privacy and data protection, and it's clear reading these that the most of them have no clear idea of what privacy is and dangers of loosing it. (http://blog.tuenti.com/)</p>
Awareness of issues or of risks	<p>In general children and young adults are unaware of the dangers behind the use of social networks and their services.</p> <p>Also parents ans teachers are not so good in theses technologies and are incapble to help children with these subject.</p>
Indifference or reaction	?
Awareness campaigns/ results	APD, goverment, local administrations are doing some campaigns to show children and young people how to use safely these services, and

	<p>the dangers hidden behind them.</p> <p>APD and government are doing important accords with social networks to improve their good practices and to protect specially children under age.</p> <p>APD and regional APD offices are preparing studies and materials to conscience different publics about th use of social networks (good practices, protecting themselves, risks, dangerous uses...).</p> <p>In addition to these, some universities are starting to do some courses about positive and negative aspects of social networks. For example this summer University of Barcelona is doing a course about « control/uncontrol » of privacy in the net/social networks during their summer special academic activities.</p>
Good practises	<p>Some social networks are modifying their attitude in front of the protection of children and they are applying new measures of protection and improving their networks to accomplish with the Spanish law (for example the case of Tuenti, deleting all the profiles suspicious to be of underage children or making private all the network contents – they could not be indexed from search engines)</p>
Campaign to be led. On which themes?	<p>More campaigns between children are needed. Also it is important to have campaigns for parents and teachers to help them to learn the dangers of these technologies and to show how they can help their children.</p>
Others	
Conclusions	<p>In Spain social networks are the phenomenon of the moment. They have experienced a big increase in a short period of time, and the main users of these networks are children and young adults.</p> <p>In general these users are very good at using technology but they are unaware of all the dangers it could imply and how to have a safer use.</p> <p>But, it's true that Tuenti (it's a Spanish enterprise) is showing a more receptive behaviour to protect children and to collaborate with APD. Perhaps just because being Spanish they have to apply LOPD and LSSI laws, while Facebook or others no.</p>
Recommendations	<p>Going on with more campaigns addressed to children, but also new ones addressed to parents and teachers.</p> <p>Working on the politicians to be conscious of all these problems and work to improve the situation</p> <p>implementing new security measures</p> <p>implementing control mechanisms in the networks</p> <p>controlling the indexing of profiles by searchers (Google, Yahoo, ...)</p>

SOCIAL NETWORKS – FACEBOOK

THEME	Social Networks - Facebook
Identification of technology	Internet connection, web services, mail services, instant mail,
Technology used/tool	Web, email, instant messaging
Country/ use area	Spain <->world
Frame of use	<p>Personal communications, Social relations, friendship, obtaining information, groups of interest, job, comercial uses, activism ?</p> <p>Data from INTECO, uses of social networks by spanish users (date of the study = october 2008)</p> <p>upload/share photos = 70,9%</p> <p>Send private messages = 62,1%</p> <p>Comments on friends's photos = 55%</p> <p>profile update = 52,1%</p> <p>send public messages = 50,2%</p> <p>gossip = 46,2%</p> <p>Label friends at photos = 34,8%</p> <p>Search for information = 25%</p> <p>downloading software = 19,3%</p> <p>downloading games = 9,5%</p> <p>Search for job = 8,5%</p>
Population concerned: target and age	<p>A wide range of ages, important number of young people.</p> <p>Data from INTECO – national institute of communications technologies-</p> <p>In Spain 44,6% of internauts are using Social networks (which represents more or less 7.850.000 people)</p>
% of users/of young users	<p>Data from INTECO</p> <p>Use of the social networks by age:</p> <p>36,5% are users between 15 to 24 years old</p> <p>32,5% are users between 25-34 years old</p> <p>Data from IDESCAT (Institute of Stadistics fo Catalonia), use fo Internet in Catalonia by age:</p> <p>→ 16-24 years = 93,5%</p>

	<p>→ 25-34 years = 84,9%</p> <p>Data from IDESCAT (Institute of Statistics of Catalonia), frequency in the use of Internet in Catalonia by age:</p> <p>→ 16-24 years = 73,6% every day</p> <p>→ 25-34 years = 66,2% every day</p> <p>→ 16-24 years = 21,1% once or more a week</p> <p>→ 25-34 years = 27,3% once or more a week</p> <p>Data from INTECO, use of social networks by ages (date of the study = July 2008):</p> <p>→ people from 14-20 years</p> <p>Facebook = 6%</p> <p>→ people from 21-30 years</p> <p>Facebook = 19%</p> <p>→ people from 31-40 years</p> <p>Facebook = 16%</p>
Trends (measured / supposed)	<p>Fast increasing in a short time period.</p> <p>And the tendency is to continue increasing rapidly.</p> <p>Data from INTECO, use of the main social networks at the world:</p> <p>Facebook: 14,1% → 2006 52,2% → 2007</p>
Known or potential dangers / Risks	<p>Too many personal and private data available on the network</p> <p>Data accessible by lots of people</p> <p>loss of the privacy</p> <p>loss of the control of your own data</p> <p>illegal / not specified use of the data</p> <p>possibility of control of a people</p> <p>spying</p> <p>getting information of people from the job (control by boss, available data of possible employees...)</p> <p>bullying</p> <p>harassment</p> <p>receiving spam and commercial messages or ads. In general it's a specific spam, so implies that the net is using the information collected to choose the ads people could be interested in.</p> <p>international transfer of data (some networks have their servers in third</p>

	<p>countries,).</p> <p>Installation of cookies without the consent/approval of the user to recover/ control information and activities and use of the net by the user</p> <p>identity theft</p> <p>difficulties to delete accounts and data related</p> <p>possibility of indexing contents/data by search engines</p>
others	<p>Poor control of privacy by users</p> <p>default profiles with very low security and protection of data</p> <p>missing information about uses of data, rights of users,...</p> <p>not clear contracts (not easy to read, too long, too specific language...)</p> <p>problems to cancel/delete data</p> <p>people is not conscious about all the possible problems and situations that can occur using a social network</p> <p>people don't know the law and the possible faults they are committing uploading third person data to a social network</p>
Generated data bases	
Associated data base/ creation (a line pro database)	<p>Users files (with all the data upload by the users)</p> <p>Use files (logs, list of users and acces data..)</p>
What justifies the inscription in the file /Risks?	To be part of the network and to access the services available
Purposes /contents, main data included / Risks?	<p>In general this files are created and mantained in order to give the services.</p> <p>These files keeps user's data necessary to register in the social network, data uploaded/published by users</p> <p>Possible risks: they could be use for more purposes than the ones specifically needed to give the service. They could be sent to other companies for other purposes (advertisments, sending information to the users, studying trends, having stadistic information,...). The data could be used by the social network company for other activities and they can obtain benefits from the user's data (normally the legal conditions signed to enter a social network imply the cession of all their data and contents they upload to the network)</p>
File masters? Risks?	Files are controlled by companies owning the social networks

Who accesses the files/ Sharing of the data base? Access limits? /Risks	Employees of these companies
Data retention delays/ risks Right to be forgotten	<p>The law establish the conservation of some files during one year. But there is no specifications for other files. Also the companies could not accomplish the law and keep the files as long as they want. In spanish law the companies has the right to keep some files/some data as historical information.</p> <p>It seems that there are some contradictions between rights/obligations of the companies.</p> <p>There are problems with companies not based in Spain, who act according laws of third countries (which could be less strict).</p>
Rights to know or to modify data?	Depending on the network
Covert purposes/ Risks/uncontrolled future evolution	
Others (interconnections...)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	<p>In Spain LOPD and LSSI are the laws controlling these tye of services. These laws are only for spanish companies but it's not clear that others accomplish these laws.</p> <p>Some articles of the law are concerning to obligations for companies based in European community countries. But they don't affect to companies based in USA for example.</p> <p>Government and APD are working intensively to extent the application of the laws to all the companies, and to sign different contracts in other to protet young people and children mainly.</p> <p>Facebook has signed recently the european agreement about social networks (see on: http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm)</p> <p>On July Facebook has presented to AEPD (Agencia Española de Proteccion de datos) some new mesures they are implementing in order to improve the privacy and the protection of data. They are preparing mesures in order their users have to decide who can access their contents, and also new mesures for controlling the</p>

	<p>registration/acces of under 14 years old people (they are considering to adapt this limit age to the convinience of spanish laws).</p> <p>Spanish laws for protection of honour, personal and family privacy and personal image are also competent for these subjects.</p> <p>At international level are also competent the «human rights declaration »(1948), International pact for civil and politic rights (1966)», International pact for economic, social and cultural rights (1966)</p>
Risks for freedoms despite the law	<p>Social networks use to have contracts really abusive in order to have total rights over all the data/contents uploaded by users.</p> <p>The contracts are not clear and not well specified, so it's difficult for people to understand what they are signing. In general they are too long, with very confusing redaction, specialized terminology...</p> <p>There are not enough security mesures avalaible in the social networks, the implementation of new mesures, and moreover, the implementation of control methods for avoiding young people under aged could register/use these social networks.</p>
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	<p>Some revisions of the law could be needed, but the most important thing is to apply the law in the cases it is being not accomplished. Specially with not spanish companies.</p>
Conformity with the European right (Charter of fundamental rights, directives...)	<p>LOPD and LSSI are spanish laws directly related with the european comunity directives</p>
Implementation (or not) of the legislation? / Risks	<p>Spanish enterprises are applying the law but is not the case of another companies, mainly the ones not based in Spain or European comunity countries.</p>
Others	
This tools and young public or young adults	
How far are young people concerned?	<p>They are not concerned with the dangers of these social networks, or with the possible faults they can commit uploading certain type of contents (for exemple photos of friends without permission, or data of other people without permission...). It's easy for them to use the technology but they need to learn how to use it in a safer way and also they need to learn about the law (what can be done and what cannot be done).</p> <p>They are unaware of the use that these companies can do with their data.</p>

	<p>They are unaware of the dangerous consequences that the loss of their privacy could imply now and in the future (information could be available on the Internet during a lot of time, information it's available for people who can use it for ilegal activities)</p> <p>Data from INTECO, security of profiles in social networks (date october-december 2007)</p> <p>48% have a profile accesible by friends, and friends of friends</p> <p>43% have a profile accesible by everybody</p> <p>6% have a private profile</p> <p>3% don't know what type of profile they have</p>
Awareness of issues or of risks	<p>In general children and young adults are unaware of the dangers behind the use of social networks and their services.</p> <p>Also parents ans teachers are not so good in theses technologies and are incapble to help children with these subject.</p>
Indifference or reaction	?
Awareness campaigns/ results	<p>APD, goverment, local administrations are doing some campaigns to show children and young people how to use safely these services, and the dangers hidden behind them.</p> <p>APD and goverment are doing important accords with social networks to improve their good practices and to protect specially children under age.</p> <p>APD and regional APD offices are preparing studies and materials to conscience different publics about th use of social networks (good practices, protecting themselves, risks, dangerous uses...).</p> <p>In addition to these, some universities are starting to do some courses about positive and negative aspects of social networks. For example this summer University of Barcelona is doing a course about « control/uncontrol » of privacy in the net/social networks during their summer special academic activities.</p>
Good practises	<p>Facebook is mantening contacts with AEPD and making an effort for improving their network in some aspects related with privacy and protection, in order to accomplish spanish laws. AEPD is doing periodically meetings with facebook to work on these subjects.</p>
Campaign to be led. On which themes?	<p>More campaigns between children are needed. Also it is important to have campaigns for parents and teachers to help them to learn the dangers of these technologies and to show how can they help their children.</p>

Others	
Conclusions	<p>In Spain social networks are the phenomenon of the moment. They have experienced a big increase in a short period of time, and the mainly users of these networks are children and young adults.</p> <p>In general these users are very good at using technology but they are unaware of all the dangers it could imply and how to have a safer use.</p>
Recommendations	<p>Going on with more campaigns addressed to children, but also new ones addressed to parents and teachers.</p> <p>Working on the politicians to be conscious of all these problems and work to improve the situation</p> <p>implementing new security measures</p> <p>implementing control mechanisms in the networks</p> <p>controlling indexing of profiles by search engines (google, yahoo, ...)</p>

THEME	Social Networks (Facebook, Tuenti, mySpace,...)
Identification of technology	Internet connection, web services, mail services, instant mail,
Technology used/tool	Web, email, instant messaging
Country/ use area	Spain <->world
Frame of use	<p>Personal communications, Social relations, friendship, obtaining information, groups of interest, job, comercial uses, activism ?</p> <p>Data from INTECO, uses of social networks by spanish users (date of the study = october 2008)</p> <p>upload/share photos = 70,9%</p> <p>Send private messages = 62,1%</p> <p>Comments on friends's photos = 55%</p> <p>profile update = 52,1%</p> <p>send public messages = 50,2%</p> <p>gossip = 46,2%</p> <p>Label friends at photos = 34,8%</p> <p>Search for information = 25%</p> <p>downloading software = 19,3%</p> <p>downloading games = 9,5%</p> <p>Search for job = 8,5%</p>
Population concerned: target and age	<p>A wide range of ages, important number of young people.</p> <p>Data from INTECO – national institute of comunications technologies- In Spain 44,6% of internauts are using Social networks (which represents more or less 7.850.000 people)</p>
% of users/of young users	<p>Data from INTECO</p> <p>Use of the social networks by age:</p> <p>36,5% are users between 15 to 24 years old</p> <p>32,5% are users between 25-34 years old</p> <p>Data from IDESCAT (Institute of Stadistics fo Catalonia), use fo Internet in Catalonia by age:</p> <p>→ 16-24 years = 93,5%</p>

→ 25-34 years = 84,9%

Data from IDESCAT (Institute of Statistics of Catalonia), frequency in the use of Internet in Catalonia by age:

→ 16-24 years = 73,6% every day

→ 25-34 years = 66,2% every day

→ 16-24 years = 21,1% once or more a week

→ 25-34 years = 27,3% once or more a week

Data from INTECO, use of social networks by ages (date of the study = July 2008):

→ people from 14-20 years

MySpace = 21%

Facebook = 6%

Hi5 = 21%

Tuenti = 31%

Fotolog = 33%

Xing/Neurona = 1%

Linkedin = 0%

→ people from 21-30 years

MySpace = 21%

Facebook = 19%

Hi5 = 13%

Tuenti = 18%

Fotolog = 11%

Xing/Neurona = 4%

Linkedin = 2%

→ people from 31-40 years

MySpace = 17%

Facebook = 16%

Hi5 = 12%

Tuenti = 2%

Fotolog = 4%

Xing/Neurona = 7%

Linkedin = 3%

Trends (measured / supposed)	<p>Fast increasing in a short time period.</p> <p>And the tendency is to continue increasing rapidly.</p> <p>Data from INTECO, use of the main social networks at the world:</p> <p>MySpace: 66,4% → 2006 114,1% → 2007</p> <p>Facebook: 14,1% → 2006 52,2% → 2007</p> <p>Hi5: 18,1% → 2006 28,2% → 2007</p> <p>Friendster: 14,9% → 2006 24,7% → 2007</p> <p>Orkut: 13,6% → 2006 24,1% → 2007</p> <p>Bebo: 6,7% → 2006 18,2% → 2007</p>
Known or potentials dangers / Risks	<p>Too many personal and private data available on the network</p> <p>Data accesible by lots of people</p> <p>loss of the privacy</p> <p>loss of the control of your own data</p> <p>illegal / not specified use of the data</p> <p>possibility of control of a people</p> <p>spying</p> <p>getting information of people from the job (control by boss, avaiable data of possible employees...)</p> <p>bullying</p> <p>harasement</p> <p>receiving spam and comercial messages or adds. In general it's a specific spam, so implies that th net is using the information recolleted to choose the adds people could be interested in.</p> <p>international transfer of data (some networks have their servers in third countries,).</p> <p>Installation of cookies without the consent/approval of the user to recover/ control information and activities and use of the net by the user</p> <p>identity theft</p> <p>difficulties to delete accounts and data related</p> <p>possibility of indexing contents/data by search engines</p>
others	<p>Poor control of privacity by users</p> <p>default profiles with very low security and proteccion fo data</p> <p>missing information about uses of data, rights of users,...</p>

	<p>not clear contracts (not easy to read, too long, too specific language...)</p> <p>problems to cancel/delete data</p> <p>people is not conscious about all the possible problems and situations that can occur using a social network</p> <p>people don't know the law and the possible faults they are committing uploading third person data to a social network</p>
Generated data bases	
Associated data base/ creation (a line pro database)	<p>Users files (with all the data upload by the users)</p> <p>Use files (logs, list of users and acces data..)</p>
What justifies the inscription in the file /Risks?	To be part of the network and to access the services available
Purposes /contents, main data included / Risks?	<p>In general this files are created and mantained in order to give the services.</p> <p>These files keeps user's data necessary to register in the social network, data uploaded/published by users</p> <p>Possible risks: they could be use for more purposes than the ones specifically needed to give the service. They could be sent to other companies for other purposes (advertisments, sending information to the users, studying trends, having stadistic information,...). The data could be used by the social network company for other activities and they can obtain benefits from the user's data (normally the legal conditions signed to enter a social network imply the cession of all their data and contents they upload to the network)</p>
File masters? Risks?	Files are controlled by companies owning the social networks
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Employees of theses companies
Data retention delays/ risks Right to be forgotten	<p>The law establish the conservation of some files during one year. But there is no specifications for other files. Also the companies could not accomlissh the law and keep the files as long as they want. In spanish law the companies has the right to keep some files/some data as historical information.</p> <p>It seems that there are some contradictions between rights/obligations of the companies.</p> <p>There are problems with companies not based in Spain, who act</p>

	according laws of third countries (which could be less strict).
Rights to know or to modify data?	Depending on the network
Covert purposes/ Risks/uncontrolled future evolution	
Others (interconnections...)	
Legislation in application	
Law /rules / others (?) (implemented for this data base or this technology)	<p>In Spain LOPD and LSSI are the laws controlling these type of services. These laws are only for spanish companies but it's not clear that others accomplish these laws.</p> <p>Some articles of the law are concerning to obligations for companies based in European community countries. But they don't affect to companies based in USA for example.</p> <p>Government and APD are working intensively to extent the application of the laws to all the companies, and to sign different contracts in other to protet young people and children mainly.</p> <p>Spanish laws for protection of honour, personal and family privacy and personal image are also competent for these subjects.</p> <p>At international level are also competent the «human rights declaration »(1948), International pact for civil and politic rights (1966)», International pact for economic, social and cultural rights (1966)</p>
Risks for freedoms despite the law	<p>Social networks use to have contracts really abusive in order to have total rights over all the data/contents uploaded by users.</p> <p>The contracts are not clear and not well specified, so it's difficult for people to understand what they are signing. In general they are too long, with very confusing redaction, specialized terminology.</p> <p>There has been identified some specdific moments of risk. One is the moment of registering, when the user has to read all the use conditions, and decide ehat kind of personal information he is going to publish. Other moment is the general use of the social network, depending of the use person is doing the risks could be different. Both moments risks depend on the consciousness the person has of his rights, the dangers, etc.</p> <p>There are not enough security mesures avalaible in the social networks, the implementation of new mesures, and moreover, the implementation of control methods for avoiding young people under</p>

	aged could register/use these social networks.
If revision of the regulation: reasons? Result: improvement or aggravation (compared to the protection of the DP)	Some revisions of the law could be needed, but the most important thing is to apply the law in the cases it is being not accomplished. Specially with not spanish companies.
Conformity with the European right (Charter of fundamental rights, directives...)	LOPD and LSSI are spanish laws directly related with the european community directives. Rome agreement from 1950 and European Union fundamental rights chart from 2000. are also competent in these subjects. Spanish laws take them into consideration.
Implementation (or not) of the legislation? / Risks	Spanish enterprises are applying the law but is not the case of another companies, mainly the ones not based in Spain or European community countries.
Others	
This tools and young public or young adults	
How far are young people concerned?	<p>They are not concerned with the dangers of these social networks, or with the possible faults they can commit uploading certain type of contents (for exemple photos of friends without permission, or data of other people without permission...). It's easy for them to use the technology but they need to learn how to use it in a safer way and also they need to learn about the law (what can be done and what cannot be done).</p> <p>They are unaware of the use that these companies can do with their data.</p> <p>They are unaware of the dangerous consequences that the loss of their privacy could imply now and in the future (information could be available on the Internet during a lot of time, information it's available for people who can use it for ilegal activities)</p> <p>Data from INTECO, security of profiles in social networks (date october-december 2007)</p> <p>48% have a profile accesible by friends, and friends of friends</p> <p>43% have a profile accesible by everybody</p> <p>6% have a private profile</p> <p>3% don't know what type of profile they have</p>
Awareness of issues or of risks	<p>In general children and young adults are unaware of the dangers behind the use of social networks and their services.</p> <p>Also parents ans teachers are not so good in theses technologies and are incapable to help children with these subject.</p>

Indifference or reaction	
Awareness campaigns/ results	<p>APD, government, local administrations are doing some campaigns to show children and young people how to use safely these services, and the dangers hidden behind them.</p> <p>APD and government are doing important accords with social networks to improve their good practices and to protect specially children under age.</p> <p>APD and regional APD offices are preparing studies and materials to conscience different publics about th use of social networks (good practices, protecting themselves, risks, dangerous uses...).</p> <p>In addition to these, some universities are starting to do some courses about positive and negative aspects of social networks. For example this summer University of Barcelona is doing a course about « control/uncontrol » of privacy in the net/social networks during their summer special academic activities.</p>
Good practises	<p>Some social networks are modifying their attitude infront the protection of children and they are applying new mesures of protection and improving their networks to accomplish with the spanish law (for exemple the case if Tuenti, deleting all the profiles suspicious ti be of underage children).</p> <p>Some social networks have some forms available to complaint about some contents or about calumnies, lies, haressement suffered on the network... In some cases, there are grouops of voluntnteer users that make a kind of surveillance of the contents in the network in order them to be good.</p>
Campaign to be led. On which themes?	<p>More campaigns between children and young people are needed. Also it is important to have campaigns for parents and teachers to help them to learn the dangers f these technologies and to show how can they help their children.</p>
Others	
Conclusions	<p>In Spain social networks are the phenomenon of the moment. They have experimented a big increase in a short periord of time, and the mainly users of these networks are children an young adults.</p> <p>In general these users are very good at using technology but they are unaware of all the dangers it could imply and how to have a safer use.</p> <p>We haven't done a differentiation between networks, because all of them have more or less the same kind of issues.</p>
Recommendations	<p>Going on with more campaigns adressed to children, but also new ones adresses to parents and teachers.</p> <p>Working on the politicians to be conscious of all theses problems and work to improve the situation</p>

implementing new security measures

implementing control mechanisms in the networks

control indexing of profiles by search engines (google, yahoo, ...)