"Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe"

Project acronym: **SurPRISE**

Collaborative Project

Grant Agreement No.: 285492

FP7 Call Topic: SEC-2011.6.5-2: The Relationship Between Human Privacy And Security

Start of project: February 2012

Duration: 36 Months

D 6.7 – Citizen Summits on Privacy, Security and Surveillance: Country report Spain

Lead Beneficiary: CSIC

Author(s): Vincenzo Pavone (CSIC), Elvira Santiago (CSIC)

Due Date: June 2014

Submission Date: October 2014

Dissemination Level: Public

Version: 1.1

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

This document was developed by the SurPRISE project (http://www.surprise-project.eu), co-funded within the Seventh Framework Program (FP7). SurPRISE re-examines the relationship between security and privacy. SurPRISE will provide new insights into the relation between surveillance, privacy and security, taking into account the European citizens' perspective as a central element. It will also explore options for less privacy infringing security technologies and for non-surveillance oriented security solutions, aiming at better informed debates of security policies.

The SurPRISE project is conducted by a consortium consisting of the following partners:

Institut für Technikfolgen-Abschätzung / Österreichische Akademie der Wissenschaften Coordinator, Austria	ITA/OEAW	
Agencia de Protección de Datos de la Comunidad de Madrid*, Spain	APDCM	
Instituto de Politicas y Bienes Publicos/ Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain	CSIC	
Teknologirådet - The Danish Board of Technology Foundation, Denmark	DBT	
European University Institute, Italy	EUI	
Verein für Rechts-und Kriminalsoziologie, Austria	IRKS	
Median Opinion and Market Research Limited Company, Hungary	Median	
Teknologirådet - The Norwegian Board of Technology, Norway	NBT	
The Open University, United Kingdom	OU	
TA-SWISS / Akademien der Wissenschaften Schweiz, Switzerland	TA-SWISS	
Unabhängiges Landeszentrum für Datenschutz, Germany	ULD	

*APDCM, the Agencia de Protección de Datos de la Comunidad de Madrid (Data Protection Agency of the Community of Madrid) participated as consortium partner in the SurPRISE project till 31st of December 2012. As a consequence of austerity policies in Spain APDCM was terminated at the end of 2012.

Table of Contents

Executive Summary

SurPRISE re-examines the relationship between security and privacy, commonly positioned as a "trade-off". Where security measures and technologies involve the collection of information about citizens, questions arise as to whether and to what extent their privacy has been infringed. This infringement of individual privacy is sometimes seen as an acceptable cost of enhanced security. Similarly, it is assumed that citizens are willing to trade off their privacy for enhanced personal security in different settings. This common understanding of the security-privacy relationship, both at state and citizen level, has informed policymakers, legislative developments and best practice guidelines concerning security developments across the EU.

However, an emergent body of work questions the validity of the security-privacy "trade-off". This work suggests that it has over-simplified how the impact of security measures on citizens is considered in current security policies and practices. Thus, the more complex issues underlying privacy concerns and public skepticism towards surveillance-oriented security technologies may not be apparent to legal and technological experts.

In response to these developments, the SurPRISE project consulted with citizens from nine[1] EU member and associated states on the question of the security-privacy "trade-off" as they evaluate different security technologies and measures.

In this report the results from Spain are presented.

Spain entered the European Union only in the mid-Eighties, after forty years of dictatorship and a short, though successful, transition to democracy. It is a parliamentary monarchy with a highly decentralized state architecture and some internal tensions produced by independents movements in the Basque Country, Catalonia and Galicia. It is a mid-size country with an economy that is undergoing a process of painful restructuring and adjustment, which started with the financial crisis and the collapse of the real estate “bubble”. Spanish economy, quite buoyant up to 2007, moved quickly into an alarming double recession, which produced a dramatic level of unemployment, worsened by local and national corruption, harsh and controversial welfare cuts and by the bank bailout obtained in 2012. Currently Spain is a country with a high level of immigration, inherited from the years of the economic growth, and an uncertain economic future, especially due to the lack of clear signs of a possible emergence of a new model of economic development.

Against this background, we can better understand the concept of security, as it is defined in the main legal and policy documents in Spain. Starting from the 1978 Constitution, it has been highlighted how the concept of security is a fundamental element of that constitution, which actually recognizes the “right to security”. The Spanish legal framework addressing the right to security has evolved with time, following two main directions: the introduction of new public authorities in charge with some specific aspects of public security and the regulation of a gradual and more exhaustive access, to progressively more integrated databases, to these authorities.

The main security and surveillance debates in the Spanish press have mainly emerged around CCTV and body-scanners. Spanish citizens are indeed concerned about security issues, but not only with those proceeding from terrorism or organized crime, because gender violence and sexual harassment are also considered important security issues. Due to the generally positive Spanish attitude towards new technologies, security technologies also receive a significant level of support. Spanish citizens, thus, welcome the introduction of new security technologies more than other EU citizens but they are especially concerned with how official institutions and commercial companies use their data. The increasing complexity of security technologies raises a sense of anxiety, generally connected with the risk of abuse that such a complexity may carry. Continuous information and public transparency about the ends and the reasons behind the choice of any given technology, thus, seem crucial to ensure the success of a process of legitimization of these technologies in the eyes of the citizens.

[1] Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland and United Kingdom

The Spanish national security strategy has been traditionally characterized by a strong support to the European Integration and the NATO as well as by a commitment to multilateralism. After 9/11 the Spanish approach, similarly to what happened in other western countries, shifted gradually to a more pro-active, pre-emptive and risk-based attitude towards security. The National Security Strategy approved in 2011, did not reject the legacy of multilateralism approach of the previous national defense directives, but incorporated them into a broader strategy where security is no longer a privileged ground for the state and the military establishment. Rather, it conceived and outlined a new strategy where public and private, military and civil, and the national and international domains are strictly intertwined, almost linked into a continuum with no clear demarcation. Moreover, the Spanish security strategy is characterized by the priority given to economic and energetic security, the emphasis on the risks of migratory flows and the importance of cyber-infrastructures, which are among the most interesting features of the Spanish national security strategy.

With regards to privacy, the Spanish regulatory landscape makes an important distinction between privacy and data protection. Whilst the right to privacy (which in Spanish is often conceptualized as intimacy) makes reference to the right that individuals enjoy to decide what to make public or keep private, the right to data protection is rather related to the articulation of legal guarantees that may exist in order to have individual information retrieved, stored and disclosed to third parties only under specific circumstances and conditions. Therefore, the right to privacy, as it is intended in the Anglo-Saxon normative framework, only emerges as a result of the combination of three different rights: the right to intimacy, the right to data protection and the right to anonymity, which includes the right to be forgotten and the right to access our own data at all times.

Spanish people can reach a consensus on the adoption of new technologies only in relation to specific cases and issues, generally related to terrorism, which does not come as a surprise, considering the impact of the Madrid terrorist attacks of March 2004. This acceptance however is normally granted only upon the condition that these technologies would be used for specific crimes, in specific contexts, in proportion to the gravity of the crimes, and for prevention purposes. Yet, some citizens question the appropriateness of using new SOSTs to address security problems. Although SOSTs are considered useful against terrorism, there exist concern that an over-emphasis on terrorism may come at the expense of other threats that citizens perceive as more imminent and familiar.

The Citizen Summit participants feel pretty secure in their daily life and consider that Spain is a safe place to live. While they support the introduction of SOSTs as a general measure to improve national security, they did not consider that these technologies actually improved their own individual security. In fact, the participants feel mostly secure in general terms but have worries and concerns when specific areas or domains, such as the cyberspace, are taken into account. This incongruence gives rise to an interesting paradox, where people feel generally safe but end up asking for more and more security measures and technologies. This paradox may be due to the fact that citizens are less willing to tolerate risks or threats. It seems that a desire for absolute security, which is obviously not attainable, is being gradually instilled in western societies. Second, only about half of the participants actually adopted a trade-off approach to consider the relationship between privacy and security: they explicitly affirmed that security and privacy stood in a zero-sum game, as SOSTs were perceived as both privacy infringing and security enhancing. However, this does not means that they were willing to trade privacy in exchange for security, as only a very small percentage of them was prepared to do so. Third, it is the possible use of these technologies in the future that generates important concerns, which negatively affects their acceptability. Looking at the prospected future the participants are worried that these technologies may be easily abused in order to match the interests of powerful political elites and/or commercial actors. Within this framework, it is easy to imagine how strongly the participants mistrust public authorities and security agencies using CCTVs and DPI. Nearly half of the participants believe that these institutions are not sufficiently competent. Most importantly, around eighty percent of the participants believe that security agencies do abuse their power when operating CCTVs and DPI.

Fourth, Smart CCTV systems are perceived in Spain differently depending on its private or public use. Citizens are more critical towards the private use of CCTV cameras, which are considered intrusive, while quite supportive of the use of cameras in public locations. Traditional CCTV receives more support than smart CCTV. Smart CCTV systems located in private residential areas, for instance, are considered typical examples of measures conceived to protect wealthy families and their belongings: these cameras are perceived to increase separation between rich and poor people, and increase social inequalities. While traditional CCTV systems are considered fairly equitable forms of surveillance, the fundamental lack of transparency and information around DPI raises serious concerns among citizens. The 'algorithmic' components of both smart CCTV and DPI also worry participants. It is not clear what are the rules establishing what it is defined normal or what is considered to be abnormal behavior. The autonomous decisions taken by algorithms also raise and leave unanswered important questions about fairness and equality.

The participants almost unanimously suggested that SOSTs should be regulated at European level to ensure fairness of treatment to all Europeans, even if national and regional peculiarities should contribute to shape overarching policies. Moreover, in order to combine effectiveness and legitimacy, participants asked for an institutional mediator, able to create a permanent and effective communication between security agencies and public authorities, on the one side, and civil society, on the other side. The technology mediator is expected to inform citizens about their rights and duties and make politicians and regulators aware of citizens' opinions, concerns and suggestions.

The participants did not neglect the causes and origins of crime, terrorism and insecurity. Though effective they may be security technologies do not eradicate the ultimate causes of crime and violence. In order to eradicate crimes, for instance, social differences should be reduced. Nor the participants neglected the bias of current security measures and technologies: it was, in fact, suggested to shift the focus of surveillance and observation from terrorism and petty criminality to fiscal frauds, tax havens and the multi-millionaire flows of money and resources hidden behind the bank secret codes and the fiscal tricks and boxes used to avoid tax enforcement.

Finally, citizens seem to be willing not only to contribute to bear the responsibility of the protection and preservation of their data, but they want also to collaborate in the design of public policies and new technologies. Social trust in the authorities responsible for the use of SOSTs is not a universal but a contextual value, which cannot be taken for granted and always needs to be renegotiated in relation to each technology, and maintained through the existence and correct function and clear rules, transparent information and effective participatory practices.

1 Introduction

This report summarizes and describes the initial findings from the Spanish citizen summits, held in Madrid on the 1st of February 2014. It begins by offering a brief overview of the Spanish national context, including information about its demographic make-up, economy, political, judicial and law enforcement systems. Then, an overview of its national security policy is presented. Controversies and public debates about security technologies are discussed to frame the preliminary data analysis. The debate about the implementation of new technologies in Spain is not especially lively in general and security technologies make no exception to this trend. However, the debate in Spain has been mostly focused on CCTVs and body-scanners. Nonetheless, the participants in the summit offered a wide range of views, opinions and suggestions, which reveal that, although the public debate is not especially lively, citizens have strong and often contrasting views on security technologies that simply do not find public spaces and opportunities to be voiced and discussed. Information about the citizen summits themselves is provided and then the descriptive statistical results are presented. It is revealed that the results as presented represent a similar range of opinions found in previous research. However it is also revealed that the Spanish participants were particularly concerned with the risk of future abuses of security technologies by public authorities and demanded new forms of democratic oversight in respect of this operation. Participants also demanded more information about who, how, when and where SOSTs were used. Significant differences in the way participants value DPI and CCTVs also emerged, which partially explain why CCTVs are more acceptable than DPI. Finally the citizen summit prompted citizens to consider their privacy much more carefully: although about half of the participants adopted the trade-off approach to security and privacy, only a very small percentage of them affirmed that would be willing to trade more of their privacy in exchange for security. Finally, important suggestion were made: from shifting the focus of security measures to fiscal fraud, tax havens and multi-millionaire flows to the reduction of social and economic differences, considered as responsible at least in part for crime and violence to better integration policy, from a more participatory data protection framework to a stricter control over the controllers. Although security technologies were supported as part of a general strategy towards an improved national security, they were explicitly considered only a partial solution to a broader and more complex problem that could not be addressed only by surveilling technologies and that, even when these technologies are necessary, need to be operated in a more transparent, clear and participatory framework.

2 Privacy, security and surveillance in the national context

2.1 General national context/ country profile of Spain

2.1.1 General description

Spain is a democracy organized in the form of a parliamentary government under a constitutional monarchy. It is a developed country with the 13th largest economy in the world. It is a member of the United Nations, NATO, OECD, and WTO. After the death of Francisco Franco in 1975, general elections were convened in 1977, with the purpose of electing Constituent Cortes (the Spanish Parliament, in its capacity as a constitutional assembly) for the purpose of drafting and approving the constitution of 1978. After a national referendum on 6 December 1978 approved the constitution and Spain was divided into 17 autonomous communities and two autonomous cities with varying degrees of autonomy. Spain is a constitutional monarchy, with a hereditary monarch and a symmetric bicameral parliament, the Cortes Generales ("General Courts"). The executive branch consists of a Council of Ministers of Spain presided by the Prime Minister, nominated and appointed by the monarch and confirmed by the Congress of Deputies following legislative elections. The legislative branch is made up of the Congress of Deputies ("Congreso de los Diputados") with 350 members, elected by popular vote on block lists by proportional representation to serve four-year terms, and a Senate ("Senado") with 259 seats of which 208 are directly elected by popular vote and the other 51 appointed by the regional legislatures to also serve four-year terms.

Spain is a decentralized country where all Autonomous Communities have their own elected parliaments, governments, public administrations, budgets, and resources. Health and education systems, amongst others services, are managed regionally. The distribution of powers, however, may be different for every community, as laid out in their Statutes of Autonomy, since devolution was intended to be asymmetrical. Only two communities—the Basque Country and Navarre—have full fiscal autonomy. Interestingly, the Basque Country, Catalonia and Navarre have police corps of their own: Ertzaintza, Mossos d'Esquadra and the Policía Foral respectively, which replace some of the State police functions.

2.1.2 Demographic data and migration movements

In 2008 the population of Spain officially reached 46 million people. Spain's population density is lower than that of most Western European countries and its distribution across the country is very unequal. With the exception of the region surrounding the capital, Madrid, the most populated areas lie around the coast. The population, however, has began to decrease after 2012, due to the emigration of both Spanish citizens and foreign residents, who are leaving the country as a result of the economic crisis, the high level of unemployment and the lack of opportunities.

Whilst native Spaniards constitute 88% of the total population of Spain, immigrants make up the remaining 12% of the population. Immigrants originate mainly in Latin America (39%), North Africa (16%), Eastern Europe (15%), and Sub-Saharan Africa (4%). The number of immigrants in Spain had grown up from 500,000 people in 1996 to 5.2 million in 2008 out of a total population of 46 million[2]. Another statistically significant factor is the large number of residents of EU origin typically retiring to Spain's Mediterranean coast. These immigrants are mostly British, French, German, Dutch, and Norwegian. They reside primarily on the Mediterranean coast and the Balearic Islands, where many choose to live their retirement.

[2] "Population in Europe in 2005" (PDF). Eurostat. Retrieved 13 August 2008.

2.1.3 Foreign policy and economic indicators

After the return of democracy following the end of Franco's dictatorship, Spain's foreign policy aimed at breaking out the diplomatic isolation experienced during Franco's regime aimed at entering the European Community, and define security relations with the West. During the first three decades of democracy, Spain's economy became the 14th largest worldwide[3] and the 5th largest in the European Union. However, even during the years of sustained economic growth Spain's economy suffered from high inflation, a large underground economy, and an education system, which OECD reports place among the poorest for developed countries, together with the United States and UK.[4]

The strong economic growth during the 1990s helped the government to reduce the government debt as a percentage of GDP and Spain's high unemployment began to drop steadily. With the government budget in balance and inflation under control Spain was admitted into the Eurozone in 1999. Since the 1990s some Spanish companies have gained multinational status, often expanding their activities in culturally close Latin America. Spain is the second biggest foreign investor there, after the United States. The adoption of the Euro in 2002 saw a marked reduction in interest rates to historic lows. The growth in the Spanish property market, which had begun in 1997, accelerated and within a few years had developed into a property bubble, financed largely by the Cajas (regional savings banks under the oversight of the regional governments) and fed by the historically low interest rates and a massive growth of immigration. The Spanish economy was credited for having avoided the virtual zero growth rate of some of its largest partners in the EU.[5] The bubble, however, imploded in 2008, causing the collapse of Spain's large property related and construction sectors, causing mass layoffs, and a collapsing domestic demand for goods and services. Today, unemployment is back at 24 percent of active population, second only to Greece and public debts stays at around 98 percent of GDP.[6]

At first, Spain's banks and financial services avoided the early crisis of their counterparts in the US and UK. This was particularly the case with Spain's international banks, Banco Santander and BBVA, that had diversified, international portfolios and had actively limited their exposure to housing mortgage risk. However, as the recession deepened and property prices slid, the growing bad debts of the smaller regional savings banks ("cajas") forced the intervention of Spain's central bank and government first through a stabilization and consolidation program, and finally acceding to a bank bailout from the European Central Bank in 2012.[7]

2.2 Science, technology and public attitudes

In Spain, science is very fragmented, with some areas of excellence, such as biomedicine, and, until austerity measures were introduced, was generously subsidized by public investments[8]. Scientists generally enjoy a high level of autonomy in their research strategy, and, in medical areas, some professional groups have more chances to influence both regulation and innovation policy than others[9]. Spanish society, in turn, shows remarkable levels of support for the scientific and medical professions but

---

3 http://en.wikipedia.org/wiki/List_of_countries_by_GDP_%28PPP%29

4 "A good bet?". *The Economist*. Business (Madrid). 30 April 2009

5 "OECD figures". http://stats.oecd.org/ViewHTML.aspx?QueryName=198&QueryType=View&Lang=en Retrieved 13 August 2008.

6 http://www.datosmacro.com/deuda/espana

7 http://www.economist.com/media/pdf/QUALITY_OF_LIFE.pdf

8 Sanz Menéndez, L., & Cruz Castro, L. (2010). Análisis sobre ciencia e innovación en España.Siegrist, M y Cvetkovich G. (2000): "Perception of Hazards:The Role of Social Trust and Knowledge", Risk Analysis 20: pp. 713-720. Sanz-Menéndez, L., Muñoz, E., & García, C. E. (1993). The vicissitudes of Spanish science and technology policy: coordination and leadership. Science and Public Policy, 20(6), 370-380.

9 Pavone, 2010. "Genetic testing, geneticisation and social change: Insights from genetic experts in Spain" chapter 4 Assessing life : on the organisation of genetic pp104-132.

does not trust very much political and business actors[10]. Consumer culture and critical awareness is comparatively poor and the development and diffusion of civil society organizations is also quite limited[11].

Current advances of technology are perceived in contemporary Spain as an increasingly important element of daily life; and a clear indicator of such attitude is given by the strong positive values usually associated with the new technologies, generally described as a crucial element in the advance of progress and social welfare. In effect, the advancement of technology plays an important role in contemporary Spanish society, not only for its economic impact but also for its social implications and repercussions. As demonstrated by several enquiries conducted by the FECYT (1996, 2001, 2006) and by the Eurobarometer (2006) on the public perception of science and technology, the Spanish society seems to hold a benevolent and supportive attitude towards the development and application of new technologies. The positive attitude towards the new technologies has been also extended to the general research process behind their development, which has been especially approved because it constitutes a mechanism that allows reflection about unexpected or previously unconceivable situations. In this respect, the participants have considered the very process of technology assessment hereby carried out as a good example of the modality of participatory processes that should always be carried out in relation to the development and implementation of new security technologies.

This positive attitude also includes security and privacy technologies, which seem to be welcomed, at least in principle, because they are expected to improve citizens' security and the general protection of properties and goods. The level of support towards new security technologies, however, varies along with the perceived negative impact on citizen's privacy, in a sense that is higher when the perceived impact on privacy is lower. In spite of such a positive attitude, however, the increasing complexity of these technologies raised a sense of anxiety, generally connected with the risk of abuse that such a complexity may carry. Yet, it is often acknowledged that, with a proper control exercised by competent authorities these technologies may indeed improve the level of security in given areas of people's life. In this respect, continuous information and public transparency about the ends and the reasons behind the choice of any given technology would prove crucial to ensure the success of a process of legitimization of these technologies in the eyes of the citizens.

2.3 Security issues, policy and strategies

2.3.1 The concept of security in Spain: from the 1978 constitution to date

The Spanish Constitution of 1978 regulates and configures fundamental rights and public liberties, the rights and duties of citizens, and the principles governing social and economic policy. Moreover, as Spain is a decentralized State, all the territorial entities are involved in security policies, each exercising its own competences: State, Autonomous Communities and Local Entities.

The Constitution emphasizes the term "security" already in the preamble. Table 1 shows some of the articles establishing relevant principles in terms of security. It is interesting to highlight that the Constitution established a "right to freedom and security".

[10] Pavone, V., Osuna, C., & Degli Esposti, S. (2010). Invertir en ciencia y tecnología en tiempos de austeridad económica:¿ Qué opinan los ciudadanos?. FECYT (2011) Percepción Social de la Ciencia y la Tecnología, 115-136.

[11] Torcal and Montero 1999

Preamble: The Spanish Nation, desiring to establish justice, liberty, and security, and to promote the well being of all its members, in the exercise of its sovereignty (…)
Article 17.1 Every person has the right to freedom and security. No one may be deprived of his or her freedom except in accordance with the provisions of this section and in the cases and in the manner provided for by the law.
Article 104.1 The Law enforcement agencies serving under the Government shall have the duty to protect the free exercise of rights and liberties and to guarantee the safety of citizens.
Article 149.1.29 The State shall have exclusive competence over public safety, without prejudice to the possibility of Self-governing Communities creating police forces, as provided for in their respective Statutes of Autonomy and within the framework to be laid down by an Organic Act.

Table 1: Articles establishing relevant principles in terms of security

In these articles, security is mainly conceived in terms of territorial integrity and public safety. However, the Constitution also speaks of security in different terms, such as when it refers to legal security (Article 9.3), security measures related to punishments entailing imprisonment (Article 25.2), compliance with health and safety at work (Article 40.2), security related to defense of consumers and users (Article 51.1), the liability of the members of the Government for crimes against State security (Article 102.2), and lastly, several principles that refer to the Law Enforcement Agencies.

The main objective of the Act 2/1986 on Law Enforcement establishes the basic principles of action that are common to them all and setting their fundamental statutory criteria. Making reference to the Constitution itself, it suggests that public security constitutes a competence that is difficult to split up, as it does not allow delimitation or definition with the rigor and precision that are admissible in other matters. That is the case because the rules that organize public security do not consider tangible physical realities, but rather events that are merely foreseen in the future, with regard to which one ignores the moment, the place, the importance and, in general, the circumstances and conditions of appearance thereof.

Addressing specifically citizens' security, the Act 1/1992 emphasizes that the protection of citizens' protection and the exercise of public liberties constitute an inseparable binomial, and both concepts are basic requisites of cohabitation in a democratic society. However in order to protect citizens' security, it is considered necessary to establish the scope of responsibility of the administrative responsibilities in matters such as manufacturing, commerce, holding and use of weapons and explosives; public gatherings for spectacles; personal documentation of nationals and foreigners in Spain; as well as to regulate certain activities of special interest and responsibility for the Law enforcement agencies.[12] This Act, written two decades ago, in way foresaw the progressive expansion of the security agenda and relevance to several societal domains, including the economic ones. Moreover, Act 23/1992 considers that public and civil securities are also deeply intertwined with private security. Although security remains primarily and essentially a public prerogative, the Act acknowledges the existence of private security services, and tries to regulate the sector. Its main goal is to ensure that those citizens, who wish to access private security services, may be provided with services following the same principles of public authorities.

[12] Organic Act 1/1992, of 21st February, on Protection of Citizens' Security.

2.3.2 Security, technology and surveillance: legal and institutional changes

The year after the attack on the Twin towers, the Spanish Parliament approved the Act 2/2002, which created the CNI, whose main task is to prevent, detect and enable the neutralization of activities of foreign services, groups or individuals that may endanger, threaten or violate the constitutional order, the rights and freedoms of Spanish citizens, sovereignty, integrity and security, stability of its institutions, national economic interests and welfare of the population. Interestingly, the Act also establishes an a priori judicial control of activities by the CNI likely to affect fundamental rights recognized in the Spanish Constitution.

In the following years, new organizations and institutions were also created. First, in 2006, the Intelligence Centre against Organized Crime (CICO) was assigned to the Secretariat of State for Security as an advisory and supporting body, whose aim was to prepare strategic intelligence in combating all kinds of organized crime, as well as, when appropriate, establishing operating co-ordination criteria for the services acting in the event of coinciding or concurrent investigations. Second, the National Anti-terrorist Co-ordination Centre (CNCA) was created by Resolution by the Council of Ministers on 28th May 2004. Among its functions there is assessment of terrorist threats, the design of future scenarios, the integration and analysis of the information supplied, and the operational co-ordination. Finally, the National Centre for Protection of Critical Infrastructures was created in 2011 in order to protect critical infrastructures, according to Act 8/2011 (measures to protect critical infrastructures) and the European Union Directive 2008/114. It coordinates and supervises all activities assigned to the Secretariat of State for Security in relation to protection Critical Infrastructures nationwide.

The legislative modifications and reforms following 9/11 were not limited to the introduction of new public bodies and institutions as they also affected the legislative framework. The Organic Act 14/2003 on the rights and liberties of foreigners in Spain and their social integration, for instance, was introduced to "[…] reinforce and, definitively, to improve the means and instruments for penalization foreseen in Organic Act 4/2000, amended by Organic Act 8/2000, to combat illegal immigration and trafficking human beings". In that sense, the act encourages collaboration with transport companies in order to obtain greater information on the persons to be transported to Spanish territory. That information shall improve and strengthen the available instruments to guarantee the security of international transport, especially by air. The act also reinforces the procedures to return foreigners who enter our country illegally and extend the conduct classified as severe offences to cover all those who – for profit, induce or favor – promote or facilitate clandestine immigration by people in transit or with Spain as their destination, or encourage them to remain in our country. [13]

As a result of the aforementioned reform, an Additional Provision Seven was introduced to Act 7/1985, which now allows the Directorate General of Police to access to the Municipal Census of Inhabitants. Given the sensible nature of this information and the potential for discrimination and function creep, the act specifies: "in order to assure strict fulfillment of the legislation on personal data protection, the access shall be performed with the maximum security measures. To these ends, a record of each access shall be kept at the Directorate General of Police, identifying the user, date and time at which it took place, as well as the data consulted".

In this way the Spanish legislator tried to ensure that unacceptable and unjustified use of this information could at least be tracked back to the moment and the author of the access, in order to ensure transparency and accountability. Yet, in order to keep the census inscription data on aliens on the municipal census up to date, the Directorate General of Police shall report monthly to the National Institute for Statistics, to exercise its competences, on the data annotated at the Central Register of Aliens.

As stated in the section of purposes of the Organic Act 14/2003, the reforms introduced by the Act are not motivated merely by security reasons, for migration and integration also have important economic and social implications. The Act, therefore, not only establishes a framework of rights and liberties of foreigners to guarantee them all full exercise of the fundamental rights (art. 1), it also tries to improve the system of orderly legal channeling of migratory labor flows, reinforcing the link between the capacity to

[13] Organic Act 14/2003, of 20th November, on Reform of Organic Act 4/2000, of 11th January, on rights and liberties of foreigners in Spain and their social integration, amended by Organic Act 8/2000, of 22nd December; by Act 7/1985, of 2nd April, that Regulates the Bases of the Local Regime; of Act 30/1992, of 26th November, on the Juridical Regime of Public Administrations and the Common Administrative Procedure, and Act 3/1991, of 10th January, on Competition.

receive immigrant workers and the needs of the labor market (art. 2). On the one hand, the act tries to increase the effectiveness of combating irregular immigration (art. 3), but, on the other hand, it also tries to reinforce integration as one of the central axes of the immigration policy in order to achieve to achieve a framework of cohabitation of identities and cultures (art. 4). Moreover, the act tries, first, to coordinate the work and action of both the central state and the regional authorities, especially in relation to the release of work permits, and, second, to establish the correct level of competences in and between the different layers of administrative action (art. 5). Finally, it also tries to establish a collaborative relation with the immigrant organizations and other organizations with an interest and establishment in the field of migration including, among such, the most representative Trade Union and employers' organizations (art. 6).

Legislative changes were later extended to cybersecurity and money laundering, too.

The Act 10/2010 on Prevention of Money Laundering and Terrorist Financing14, consistently with the for Directive 2005/60/EC of the European Parliament and the Council, implements measures related to the definition of "politically exposed person" and the technical criteria for simplified customer due diligence procedures and for the exemption on grounds of a financial activity conducted on an occasional or very limited basis, in addition to establishing the penalization regime of the Regulations (EC) No. 1781/2006 of the European Parliament and Council, of 15th November 2006, on information on the payer accompanying transfers of funds. More recently Act 8/2011 establishes measures to protect critical infrastructures, transposing to Spanish law the Council Directive 2008/114/EC, of 8th December, on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection.

To sum up, after 9/11 legislative reforms were oriented, on the one hand, to the introduction of new public bodies and institutions as the CICO, oriented to combating organized crime, or CNCA, oriented to assessment of terrorist threats, and, on the other hand, the reforms also affected the legislative framework in the context of border security and migration, -Act 14/2003-, cybersecurity –Act 5/2010-, money laundering Act 10/2010, and protection of critical infrastructures –Act 8/2011-. These measures explicitly oriented towards the implementation of a new security legal framework, which focuses on the protection of individuals and of the state, had the consequence of a clear decrease of privacy data subjects.

2.3.3 The Spanish National Security Strategy

Before 9/11, The Spanish national security strategy was based on a series of national security directives. Among the most important ones, The National Defense Directive 1/1996 firstly adopted the new concept of security and defense, developed by the NATO, which made the initiatives of co-operation and approach to former adversaries compatible with maintaining adequate military capacity. The NATO strategy was based on the conviction that western security was strictly linked to that of our neighboring countries, to that of those sharing our model of society and that of those located in areas in which the NATO states have a strategic interest. Spain, thus, made an explicit commitment to achieve a more stable, secure international order, based on peaceful cohabitation, defense of democracy and human rights and respect for international rule of law. That commitment was then made evident by Spain's presence and determined participation in peacekeeping operations.

According to that Directive, the purpose of the defense policy was to provide Spain an effective instrument for dissuasion, prevention and response to permanently guarantee its sovereignty and independence, its territorial integrity and constitutional organization, as well as to protect the life, peace, liberty and prosperity of Spaniards and the national strategic interests wherever these may be located. This directive also represented the beginning of a new political stage, with new orientation criteria for defense policy. The major changes in the international situation, following the end of the Cold War, were then more consolidated and with better profiled trends for the future; and the coming completion of the processes of adaptation of the Atlantic Alliance to the new strategic realities, made it advisable to orient Spanish defense policy toward three basic objectives of action:

[14] This act transposes the Directive 2005/60/EC by the European Parliament and the Council, of 26th October 2005, on prevention of the use of the financial system for the purpose of money laundering and terrorist financing, developed by Directive 2006/70/EC of the Commission, on 1st August 2006.

1) The consolidation of the presence of Spain in international security and defense organizations, fully undertaking the responsibilities and commitments arising from participation therein.

2) The improvement of the efficiency of the Spanish Armed Forces, to enable them to carry out their constitutional missions, to contribute with the allies, to the extent of national possibilities, to the collective security and defense, and to collaborate in keeping the international peace and stability, particularly in our geographic and cultural environment.

3) A better connection with the Spanish society, in order to ensure that the latter may understand, support and participate with greater intensity in the task of maintaining a defense device adapted to Spanish strategic needs, responsibilities and interests.

Spanish national security strategy took a different path after 9/11. Whereas before the terrorist attack on the Twin Towers was mainly oriented towards peacekeeping, peace building and aid to development, after 9/11 the Spanish approach, similarly to what happened in other western countries, shifted very gradually to a more pro-active, pre-emptive and risk-based attitude. This is already visible in the National Defense Directive 1/2004 but it became more pronounced with the last change in government. The National Defense Directive 1/2012 states: "Spain must be ready to deal with the risks of a world in which interconnection, the quality and speed at which information flows, electronic management of transaction, freedom of movement and commercial exchange, the benefit of which is so evident to society, do not give rise to a scenario in which these are taken advantage of by terrorist groups and organized crime, with the capacity to severely damage social peace, citizens' security, political stability and general prosperity.

The first document to explicitly endorse the shift from a defense strategy to a security strategy is the 2011 Spanish national security strategy. This document does not reject the legacy of multilateralism and aid to development approach of the previous national defense directives, but incorporates them into a broader strategy where security is no longer a privileged ground for the state and the military establishment. Rather, it conceives and outlines a new strategy where public and private, military and civil, and the national and international domains are strictly intertwined, almost linked into a continuum with no clear demarcation. The strategy takes its start from the acknowledgement of a bleak and worrisome scenario, which is characterized by the worst economic crisis since 1929 and the gradual shift of economic power towards East Asia. In this scenario, globalization has made it possible for new and traditional security threats to become more and more interconnected within and across national borders, rendering national security strategies and policies insufficient and inadequate to deal with such threats. We quote:

"We face transversal, interconnected and transnational threats and risks. Preserving security requires co-ordination, both international and internal, as well as contribution by society overall. The limits between interior and exterior security have become faded. National policies in the traditional fields of security are no longer sufficient to safeguard this in the 19th Century. Only an integral focus, that conceives security amply and in an interdisciplinary manner, at national, European and international level, may rise to the complex challenges we are facing".

Globalization, as they say, is expected to amplify and exacerbate current risks and threats, although it may also considered as a provider of solutions and tools to tackle these risks and threats (p. 32). This is why the preservation of national security may imply action far away from national borders. The Spanish security strategy identifies, then, a number of potential threats that are (more or less) likely to affect Spanish security, and it lists and addresses them in chapter 3. Essentially, along with the traditional threats represented by armed conflicts, terrorism, the proliferation of weapons of mass destructions and organized crime, the document, for instance, speaks of as "economic and financial security", which marks a difference with EU security strategy. Economic security, which is considered an essential element of Spanish security, is portrayed as threatened by macroeconomic imbalances, financial volatility, economic speculation, poor performance of supervisory agencies and competition for common resources. These threats may cause macroeconomic imbalances and contagious systemic crises, which are likely to produce higher income inequality and depletion of resources. National states have limited capacity to solve these problems. As a result, the document suggests implementing a better supervision of the markets, a stricter regime of punishment for economic crimes and an improvement of the EU governance.

The emphasis on energetic security and energy vulnerability is another Spanish peculiarity, due to high dependence of fossil fuels. Whilst it is necessary to improve independence, efficiency and reduce consumption whilst investing in national renewable energy, the document prioritizes the security of supplies and diversification of providers, as well as the liberalization of the market. Other traditional security issues, like cyber security and migration, are also present in the document, although they are framed in their own interesting terms. Cyber security, for instance, is framed in terms of a virtual space of infrastructures that we need to protect and monitor for more and more economic, social and political activities nowadays occur in the cyberspace. As attacks to cyberspace may paralyze activities and events in real space, there is need to protect this space by improving the legislation and the resilience of the infrastructures, and by enhancing cyber-intelligence and the public-private cooperation.

Uncontrolled migratory flows are also framed in terms of social conflict, rather than in terms of direct security threat. Massive migration likely produces social conflict, generates ghettos and lack of integration, which, in turn, favors economic exploitation and encourages criminality, terrorism and ideological radicalization. The Spanish strategy, thus, recognize on equal terms the social and the criminal nature aspects of uncontrolled and poorly integrated migratory flows, which, is addressed by a strategy based on both more effective social integration policies and more efficient border control. Terrorism and organized crime are framed, more or less, in the same terms as in the EU security strategy. In these areas, the risk-assessment pre-emptive approach is more explicit that in other areas: the plan and strategy is essentially based on the anticipation, prevention and, when the previous have failed, protection of potential victims. Interestingly, the strategy crucially acknowledges technology as a potentially multiplying factor: technology can solve problems, they say, but it also produces new threats and risks (p. 35). The same technology that allows financial or transport coordination can be used to disrupt these very services: cyber-security is an illustrative example of this double edge situation.

In order to tackle these security issues, the document promotes a comprehensive approach, which allows the development of security policies capable of addressing the threats systematically. While it insists on the efficient use of existing and emerging resources, it also promotes a better coordination between the State and the society, hinting at a state of security that is the result of a shared collaboration (together with shared responsibility) between public authorities, private citizens, civil society organizations and business companies. As a result, anticipation of threats and risks is emphasized as a crucial part of the strategy itself: "The Anticipation or prevention of conflicts should always be the first objective. Investments in creating stability and security before crises erupt are not only less costly but also more effective." (p. 42) Imagining the potential threats their future developments and trends and the likelihood of their materialization becomes a key element of a security strategy, along, of course, with an improvement of the resilience of systems and instruments. Finally, it recommends a better and more responsible interdependence with UN and allies.

In conclusion, the shift towards a more risk-based, pre-emptive and proactive approach to security; the emphasis on increasingly blurred boundaries between the private and the public, the civil and the military, and the national and the international; the prominence of economic and energetic security, the emphasis on the risks of migratory flows and the importance of cyber-infrastructures are among the most interesting features of the Spanish national security strategy. These changes, claims the document, urge all of us, including lay citizens to develop what is defined a "greater security culture":

"The threats and risks our country faces have changed drastically in the last two decades and their origins are multiple and heterogeneous, from jihadist terrorism to networks of organized crime, ranging through cyber-attacks. Living in a modern company requires attitudes, skills and knowledge at a level unknown up to present. It is necessary to promote a greater security culture and encourage education of professionals in highly diverse sectors and, in general, that of citizens, in such matters."

2.4 Privacy in the Spanish context: issues, regulations and debates

The Spanish regulatory landscape makes an important distinction, which, as we argue, should rather constitute the starting point of current debates on privacy and data protection. On the one hand the

Spanish legislation considers that privacy and data protection constitute, effectively, two different rights, which are related to each other but are nonetheless conceptually different. Whilst the right to privacy (which in Spanish is often conceptualized as intimacy) makes reference to the right that individuals enjoy to decide what to make public or keep private, the right to data protection is rather related to the articulation of legal guarantees that may exist in order to have individual information retrieved, stored and disclosed to third parties only under specific circumstances and conditions. The proper function of data protection legislation and procedures, of course, reinforces and improves the right to intimacy, as it prevents illegitimate intrusions to existing data and information, but it cannot be considered as an alternative to the right to intimacy, which precisely identifies and regulates those circumstances and purposes that enable data retrieval to be carried out in the first place.

In fact, in the Spanish constitutional framework the right to privacy, as it is generally understood in the Anglo-Saxon world, does not exist. Only specific aspects of this generic right may be considered to exist, such as the above-mentioned right to intimacy (art. 18, comma 1), which is strictly related to any information associated with the data subject and their family. However, the right to privacy could be considered to emerge as a result of the combination of three different rights: the right to intimacy, the right to data protection and the right to anonymity. Apart from the Spanish constitution, these three rights are regulated by three specific legislative Acts: The Ley Orgánica 1/1982, which regulates the right to intimacy, the Ley Organica 2/1984, which regulates the right to modify and control the data, including the right to anonymity, as explained later in this chapter, and, finally, the Ley orgánica 15/1999, which regulates data protection.

2.4.1 The right to intimacy

The right to intimacy is the closest legal concept in the Spanish legislation to the Anglo-Saxon right to privacy, however it has a much more limited extension and it is also conceptually different. In a few words, intimacy could be defined as the right to be protected from third party curiosity; however, it is not related to the protection of our private life (in the sense of the way we use to live and act) but rather to the right individual have to decide what they want to make public and what the want to keep protected from an external gaze[15]. In this sense, we could say that privacy is somewhat configured as the outcome of a full exercise of the right intimacy, combined with the right to data protection and anonymity. This definition of the right to privacy, however, is the result of a conceptual development intrinsically associated with the idea that the basic rights of expression, associations and information could only be exercised in physical spaces well defined and delimited, in a world where it was still largely possible to conceptually separate the private sphere from the public one.

However, the increasing diffusion of social interactions in the cyberspace, whether through social networks, blogs, Internet, and cyber-forums makes these traditional definitions and delimitations blurred and, often, no longer meaningful. It is increasingly difficult to decide whether participation to social networks is a public or a private activity or whether the cyberspace is a public or a private space. Yet, a much important part of our social, intimate and professional life occurs in the cyberspace. Effectively, we would no longer be the same if we could not express ourselves and operate in the cyberspace. Interestingly, however, the virtual spaces of interactions, whether social networks, websites or personal blogs, are designed in such a way that, while we are operating in the cyberspace, we often have the feeling of being protected, of being involved and interconnected in a space that is respectful of our right to intimacy and it is opaque to the rest of the world. In fact, this is far from true. Unfortunately, this feeling of false intimacy encourages incautious behaviors and may foster a gradual release of even the most intimate information about us.

The point is that the cyberspace and the use of social networks affects the right to intimacy in the sense that it makes very difficult for the data subject to decide autonomously, and effectively, what to make public and what to keep as private information. In this sense, the legislation makes a distinction between territorial and informational intimacy, depending on the physical space where information is located and shared (physical reality or virtual cyberspace). Recent legal doctrine (STC 173/2011) has established that Art.18, thus, does not guarantee the right to a private life but the right to make sure that personal

[15] Menéndez, I. V. (2013). LA INTIMIDAD, ESE "TERRIBLE DERECHO" EN LA ERA DE LA CONFUSA PUBLICIDAD VIRTUAL. Espaço Jurídico: Journal of Law [EJJL], 14(3), 57-72.

information is not shared unless this is the will of the data subject, which indirectly enables the citizen to have a private life. In sum, it is the citizen who must always be in the condition of deciding, in complete autonomy, what is meant to be private and what is not. Yet, this does not prevent the State or its security agencies or its judicial organs to discipline and regulate, even delimitate, such right[16].

As a result of this specific understanding of what is privacy, the Spanish debate, though not very lively, has mainly focused on how new security technologies, especially DPI but not only, affect and possibly curb the individual right to decide what to share and what to keep private. The Spanish emphasis on the "right to be forgotten", which has been recently accommodated into European legislation, has to be understood in this specific context. If we consider that the right to decide what to share implies the right to decide when to withdraw consensus to share our own information, the logical consequence is that, once the consensus has been withdrawn, the related information also needs to be made inaccessible.

2.4.2 The right to data protection and anonymity

In many ways, the specific aspects of intimacy above mentioned constitute the foundation of another right, the right to data protection. One of the main characteristics of the cyberspace is that, whether we like it or not, much of the information that we share over the social networks or the web as such is collected and stored on private servers. This happens anyway; even if we have clearly selected that this information could only be shared with specific persons or group of persons. Once collected and stored, this information need to be protected and made inaccessible or otherwise the data subject right to intimacy would be irremediably affected. This is why data protection is crucial, especially when we deal with privacy in the virtual space: without an appropriate data protection policy, the right to intimacy is lost.

To be precise, the sharing of messages and information on the social networks does not constitute per se a threat or an infringement of the right to intimacy. Yet, the analysis of this apparently innocuous information in collective and systematic terms reveal so much about individual preferences and intimate characteristics that, effectively, it makes the right to intimacy impossible to enforce. This specific aspect of the right to intimacy in the cyberspace is rendered even more problematic by the fact that personal information is shared, sold and made accessible by the internet providers or servers to third parties for commercial reasons and produces enormous benefits[17].

The right to data protection is, thus, especially important in the Spanish context and it is regulated by the Article 18.4 of the Spanish Constitution, the Ley orgánica 15/1999 and, more recently by the 2007 Royal Decree on data protection. There exist four data protection agencies, one is national and three of them operate at regional level, in Catalonia, Basque Country and Madrid[18]. The right to data protection enables the data subject to a) decide what to share and with whom b) know who possesses his data and why and c) deny or consent their use and/or obtain modification or removal. The Data protection agencies are public institutions, independent from the government, that not only ensure the correct implementation of the law; they also produce additional executive normative guidelines and offer consultation on the implementation of the norms. The objects of data protection are all those personal information that allow the identification of data subjects, including picture, addresses, phone numbers, sound records, medical registries etc. According to current legislation, whenever a database with such information is created the data protection authorities needs to be informed, in order to ensure that the data retrieval and data storage has been conducted in accordance to the law and that the database will be adequately and legitimately accessed according to the criteria also established by the law.

There exist three levels of data protection, which apply to different types of data. The first and most basic level of protection applies to traditional individual data (address names, date of birth etc.) and it establishes a series of mostly administrative procedures to be implemented to regulate who, how, when and to what extent these data can be accessed. A second and stricter level is established for more personal

---

16 Amitai Etzioni, 2012 "Los limites de la privacidad", Edisofer, Madrid

17 Tello Diaz, Lucía. 2013. "Intimacy and «Extimacy» in Social Net-works. Ethical Boundaries of Facebook." Comunicar, Vol. 21, 205-213.

18 The Data Protection Agency of Madrid (APDCM) was terminated in 2012 as a result of the austerity measures adopted by the Regional Authority of the Madrid Community. Its competences and functions, as well as part of its staff, have been transferred to the Spanish Data Protection Agency.

and sensitive data, such as financial data, criminal records, and Internet data connected to email and communications. In this second level, a data protection officer is required, who becomes responsible of the data protection and access procedures and stricter rules of who can access and when, how and to what extent is possible to access these data. For instance, the physical or digital space where these records are stored and accessed need to be protected through rigid procedures of identification of those who access, when and how. Both the IC technologies used to manage these data and the buildings where these data are handled need to be audited every two years. The third and highest level of security is mandatory for data related to ideology, religion, health, sexual orientation, as well as data related to police investigations and sexual harassment. This level impose further restriction to the access of the data and keep a very detailed registry of all accesses, which need to be authorized individually and in advance. The data related to the registry of access will be kept for two years. Moreover, the circulation of these data will always be realized through a system of encryption. Finally, the data protection legislation in Spain insists that all data need to be true, relevant and up-to-date. This implies that a) the data need to be updated whenever possible and b) they must be destroyed if they are false and/or irrelevant. It also implies that, unless they are considered necessary by security agencies, the judges and/or the police, personal data also must be made inaccessible or destroyed if so is required by the data subject.[19]

The Spanish legislation, thus, protects equally the right to intimacy and the right to data protection, as both rights are considered crucial to protect citizens from illegitimate intrusions and guarantee their privacy, as the Spanish legislation frames it. It ensures, for instance, that virtual communications to specific individuals, such as emails, are protected as much as physical communication but does not grant a similar protection to web searches and general communications made on the web. This is why the growing amount of intimate information shared in social networks, apparently shared only with selected individuals or groups, but effectively stored and made accessible to third parties constitutes a powerful threat to the right to privacy. Villaverde, again, proposes to consider and regulate a new right to complement and integrate the right to intimacy and the right to data protection, which is the right to "anonymity". This right would be both a passive right (the right not to be identified by third parties whilst operating on the web, or elsewhere) and an active right (the right to be forgotten, in fact). This right would be, allegedly, the only way to ensure that Internet comes to constitute a safe, transparent and protected space. At the moment, it is only falsely safe and private, and most citizens are not entirely aware of it.

It is important to consider that, from the Spanish perspective, the protection of the right to intimacy and data protection over the cyberspace is a priority, as these rights constitute an essential component of human dignity and contribute directly to the development of human personality. As a result, this grants the State the right to intervene and regulate the cyberspace in order to ensure the respect for these rights, even if and when individuals decide to renounce to the exercise of these rights. The State can, thus, impose limits to Internet providers and social networks owners, even if individuals are willing to renounce to let these actors trespass these limits (STC 144/1999). However, more recent perspectives have suggested that we define ourselves not only through what we keep private and what we share with specific subjects, but also through what we share in the web, through what we need to share of our intimacy, that it is so important that sharing it contributes to help construct ourselves. This new understanding of intimacy is often referred to as "ex-timacy" [20].

2.5 Public discourses on surveillance-oriented security technologies and related practices

The current advances of technology play an important role in contemporary Spanish society, not only for its economic impact but also for its social implications and repercussions. The Spanish society seems to hold a benevolent and supportive attitude towards the development and application of new technologies, as demonstrated by the relevant surveys conducted by the FECYT (1996, 2001, 2006) and by the Eurobarometer (2003, 2005, 2006, 2012). Spanish citizens, however, have a critical attitude towards

[19] López Roman y J. Mora, 2009, Un análisis de la estructura institucional de protección de datos en España, Indret, No. 2/2009, pp. 1-34. See also Cristina Gomez Piqueras, Spanish Data Protection Agency, presentación en power point accessible at: http://www.faisscv.es/4jornadasxativa/1conferenciacristina/confidencialidad.pdf .

[20] Tello Diaz, Lucía. 2013. "Intimacy and «Extimacy» in Social Net-works. Ethical Boundaries of Facebook." Comunicar, Vol. 21, 205-213.

their political and administrative institutions (Eurobarometer, 2008a, 2008b, 2009) and show perplexity towards a few situations usually associated with the implementation of some of these technologies, which are often perceived as more plausible in the context of a science-fiction novel – with all the dehumanizing and impersonal implications – than in a context of ordinary daily life. For example, Luján and Todt[21] show how Spanish people are aware that scientists may be influenced by economic interests and also consider the social and ethical values should play a significant role in making decisions in science and technology. These new interpretations have placed the concept of ambivalence at the core of social representations of science and technology in Spain[22] as a result of the integration of the deficit and contextual models.

Within this positive and yet occasionally ambivalent framework, security technologies receive a significant level of support, as they are expected to improve the level of personal protection as well as the protection of goods and properties. In general, however, the lower is the perceived negative impact of these technologies on personal privacy the higher would the level of support be. In some cases, however, Spanish citizens have shown perplexity, such as towards the body scanner or the face-recognition cameras. In this respect, continuous information and public transparency about the ends and the reasons behind the choice of any given technology would prove crucial to ensure the success of a process of legitimization of these technologies in the eyes of the citizens. More specifically, Spanish citizens have traditionally expressed deep concern that these technologies may be used for commercial purposes and/or for political control. This benevolent yet cautious attitude towards security technologies, especially those that are surveillance oriented[23], could partially be explained by, on the one hand, the familiarity of Spanish citizens with terrorist actions, and the other hand by the relatively recent legacy of Franco's fascist regime.

As a matter of fact, Spain has a history of terrorist attacks from the ETA organization (only a year ago ETA finally announced the ultimate rejection of violence and terrorism). Madrid, additionally, was struck in 2004 by a serious terrorist attack with bombs on a number of trains. Spanish citizens, therefore, are in many ways familiar with the threat of terror and may be expected to have a special craving for security. The PRISE project in 2008, however, demonstrated that this is not always the case. Spanish citizens are indeed concerned about security issues, but not only with those proceeding from terrorism or organized crime, because gender violence and sexual harassment do represent an important issue in the Spanish society. Spanish citizens, moreover, may well be more flexible than other EU citizens, when it comes to the introduction of new security technologies but they are especially concerned with how official institutions and commercial companies use their data, which occasionally leads to high levels of mistrust in new security technologies. As the PRISE report suggested, Spanish citizens tend to mistrust the people in direct control of the technologies, not only on technological grounds but also in relation to human errors. On the one hand, the increasing complexity of these technologies raise a sense of anxiety, generally connected with the risk of abuse that such a complexity may carry. On the other hand, it is generally acknowledged that, with a proper control exercised by competent authorities, these technologies might indeed improve the level of security in given areas of people's life[24]. The debate around many of the security technologies needs to be considered against this specific background.

In the following, we have recollected some of the debates on specific technologies that have been hosted by the main Spanish newspapers. It is important to consider that some of the discussions concerning security and surveillance in Spain have concentrated on activities related to terrorism and crime. Other

---

21 Luján López, J. L. (2007): "El principio de precaución y la imagen social de la ciencia", en Fundación Española para la Ciencia y la Tecnología (FECYT), Percepción Social de la Ciencia y la Tecnología en España 2006, pp. 65-80.

22 Luján, J. L. y Todt O. (2000): "Perceptions, attitudes and ethical valuations: the ambivalence of the public image of biotechnology in Spain, Public Understanding of Science 9: pp. 383-392.
Luján López, J. L. (2007): "El principio de precaución y la imagen social de la ciencia", en Fundación Española para la Ciencia y la Tecnología (FECYT), Percepción Social de la Ciencia y la Tecnología en España 2006, pp. 65-80.
Torres 2005.

23 Pavone, V. and S. Degli Esposti (2012) "Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security " Public Understanding of Science 21(July): 556-572.

24 PRISE Spanish National Report, 2008.

issues, such as the use of the National Identity Document or the use of biometric data (fingerprints for instance are included in that National Identity Card and are also used as a presence control device for employees) have not been especially controversial in Spain.

Surveillance cameras, though extensively used, have raised interesting debates. In one specific case, cameras had been installed in a sauna, in Madrid. Customers were not informed, and when it was discovered some customers complained to the Police and the data protection authority fined the Sauna owner[25]. More recently, however, some supportive voices invoked more surveillance cameras, especially after the theft of the Calixstus Code. El Pais reported: "But the theft of the Codex of Calixtus in the summer of 2011 alerted the responsible of many small temples in which, over the years, proliferated the thefts. This growing fear in Galician was benefited a young businessmen from Melide, Javier Mouriño, since 17 years old is dedicated to bring the wireless Internet connection to Galician countryside"[26]. This new craving for surveillance cameras somehow spread across the country, and more and more town councils introduced cameras to deter crime and violence, as in the case of Barcelona[27] and the city of Salt, in the province of Girona[28].

In a small town close to Madrid, more cameras were also requested by the inhabitants, but with a specific provision, which requires the tapes to be destroyed after one month if nothing has, in the meanwhile, happened: "The City of Pozuelo de Alorcón (82,400 habitants) is to install surveillance cameras to monitor sensitive areas of the city. The Department of Safety has submitted a project to the Government Delegation in Madrid to install 12 electronic eyes in the central streets working 24 hours a day (...) The images of the local police will be destroyed after a months, if not required by the judicial authorities"[29]. However, the Regional Committee of Surveillance rejected this request because it did not consider fully justified the proposal to place 12 electronic eyes that record for 24 hours a day to control the crime[30].

Concerns about cameras have also been raised among the bar and club owners in Chueca, the gay neighborhood of Madrid, famous for its nightlife. There is a risk, as it has been argued, that the presence of surveillance cameras may inhibit and condition people's behavior, making Chueca less attractive to people, who simply want to enjoy life and night entertainment. Yet, success of cameras in other areas, however, is reducing fear and reluctance even in Chueca: "There is a fear that Chueca success die because the major propose the use of surveillance cameras that have been successful in the Plaza Mayor, Sol, and Montera. Experience in these areas, where the all-seeing eye has managed to reduce the number of crimes, is dissipating the initial reluctance to violate the privacy and turn the city into a big brother. It seems that most people prefer to feel safe in the streets even with the risk of being seen in full divertimento "[31].

More controversies have been generated by the installation of a number of CCTV cameras in Lavapiés, the multiethnic neighborhood of Madrid[32]. Although the camera have been introduced to improve the security and the safety of the local residents, in fact, they have been mainly criticized as an instrument of racial discrimination, given the specific ethnic composition of the neighborhood[33]. In fact, among the strongest critics of the system, we can find precisely the local residents, regardless of their ethnic background[34].

25 El Pais (2010): Newspaper article from June 3, 2010.
26 El Pais (2012): Newspaper article from July 26, 2012.
27 El Pais (2012): Newspaper article from July 11, 2012
28 El Pais (2011): Newspaper article from Feb.16, 2011
29 El Pais (2010): Newspaper article from June 19, 2010.
30 El Pais (2010) Newspaper article from July 30, 2010.
31 El Pais (2010): Newspaper article from January 9, 2010.
32 El País (2009): Newspaper article from 23 December 2009.
33 Publico (2008): Newspaper article from 21 October 2008.
34 El Pais (2012): Newspaper article from 24 March 2012.

Surveillance cameras have also been considered from a different perspective, which focuses more on self-segregation than on active discrimination. This was, for instance, the case of residential communities that have installed surveillance cameras to protect, segment and isolate their territory from external intrusion. In this case, El Pais spoke of "mixophobia", that is the fear of cultural diversity and multi-ethnic social blends: "Recently, the High Court of Justice of Catalonia (TSJC) authorized the City Council to Sitges install surveillance cameras and barriers at the entrances of seven urbanizations (...) Residential communities have become commodities and signs of status, social segmentation trend seems unstoppable if the market is flow free. The pursuit of diversity, which was the major driving force of cities as places that made us feel more open, now seems the opposite symbol. There are many people who do not like to mix. And if their pocket permits, they show mixophobia. And so, without realizing it, we build more and more borders and walls in a globalized world only for the money and for consumption"[35].

Street crime, petty crime and violence are not the only reasons to encourage the installation of surveillance cameras, they can also be used to prevent and combat fires, or at least to identify those who cause them: "The Council of Castilla y León has already begun the installation of surveillance cameras in the region of Sanabria (Zamora) to detect forest fires and person that cause it."[36]. Finally, a special mention deserves Google Street view, which has been criticized for it does not comply with Spanish Data Protection laws: "Now that Google Street View cars are roaming through Spanish streets, the firm 'ePrivacidad' complained to the Data Protection Agency (AEPD), that Google's way of taking pictures is based on the practice of taking pictures indiscriminately, while Spanish legislation to install cameras in public places is very strict"[37].

Body scanners have also been a quite contested technology. In 2010, the then Minister of Development, José Blanco, announced in Congress that provisional and experimental "body scanners" would soon be implemented in some Spanish airports to see how they work and how the passengers respond (...). Facing a growing movement of protest for the discomfort that these scanners may produce to passengers, actually Blanco had to specify that he had not received pressure from the US to introduce such scanners[38]. The main issue with these scanners is personal and bodily privacy. Civil liberties supporters argue that this type of scanners invades the privacy of travellers. The Aviation authorities, however, keep insisting that "passengers' privacy is guaranteed by the application of a filter so that is not possible identify the people and the images are purged immediately once viewed and are never stored."[39]. Almost inevitably the debate has been framed as a confrontation between security and privacy advocates: "The controversial installation of body scanners at airports to prevent terrorist attacks, that the Government of Spain considers "inevitable", had divided the experts on those who support security should take precedence over the right to privacy of travellers and vice versa. While some advocate the installation of these devices to necessary, others believe that there are alternative measures and the use of scanners is an invasion of privacy"[40]. As a result, pretty much like surveillance cameras, the debate has been almost always conceived as a trade-off between privacy and security, although some actors have rather insisted on the availability of alternative and more efficient, more privacy friendly practices, solutions and measures, such as urban design and new architectonic solutions against crime.

In conclusion, whilst Spanish citizens generally agree that security is indeed necessary and must be increased, they question, to a certain extent, the appropriateness of using new SOSTs to address security problems and prefer to restrict the adoption of new SOSTs only to specific crimes, in specific contexts and always under specific legal and institutional guarantees. Their main concerns were to avoid political abuses and a deterioration of the democratic framework of law and rights. While acknowledging that

35 El Pais (2008): Newspaper article from September 18, 2008.
36 EL Mundo (2012): Newspaper article from May 7, 2012.
37 EL Mundo (2012): Newspaper article from May 7, 2012.
38 El Mundo (2012): Newspaper article from March 12, 2012.
39 El Mundo (2010): Newspaper article from March 5, 2010.
40 El Mundo (2010): Newspaper article from January 17, 2010.

SOSTs may be useful against terrorism, they express concern that an over-emphasis on terrorism may come at the expense of other threats that they perceive as more imminent and familiar[41].

[41] Pavone, V. and S. Degli Esposti (2012) "Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security " Public Understanding of Science 21(July): 556-572.

3 Process design – the citizen summit in Spain

The Spanish Surprise Citizen Summit was held in Madrid, on Saturday the 1st of February 2014, in the Holiday Inn Hotel close to Santiago Bernabeu Football stadium. Out of 220 people, who had confirmed their attendance the day before the event, 185 effectively took part in the event.

Spanish participants received the Spanish version of the Surprise booklet, with information about three SOSTs: Smart CCTV, Smartphone Location and Deep Packet Inspection (DPI). The day of the event, participants were grouped into heterogeneous groups – in terms of gender, education and age – of 8 people per group, and seated around round tables. At each table a facilitator was present to help people feel comfortable, answer questions by using clickers and share their views in a respectful manner. The head facilitator, Dr. Elvira Santiago, guided citizens throughout the event from the main stage. As part of the introduction, Elvira introduced the clickers (wireless audience response system) and explained how citizens had to use them to answer questions appearing on the three screens positioned around the stage.

Clickers not only registered anonymous responses from each participant, they also made these responses instantly available: aggregated results were displayed on a big screen at the center of the venue after each question. These aggregated statistics helped participants to get an impression of what were other people's opinions. The Spanish summit ran smoothly throughout the afternoon with a coffee break organized in a room opposite to the main venue almost halfway through the event.

3.1 Description of the Event

Time	Activity
14:45	Registration
15:20	Introduction given by Elvira Santiago and Vincenzo Pavone
15:40	1st round of questions – general questions
15:50	Emilio Aced's, Head of the Support Unit of the Spanish Data Protection Authority
16:20	2nd round of questions – questions on smart CCTV
16:25	Smart CCTV Film
16:35	Questions on Smart CCTV – questions on smart CCTV
16:45	45-min Discussion Round on Smart CCTV
17:30	3rd round of questions – questions on smart CCTV
17:50	Coffee break
18:20	4th round of questions – questions on DPI
18:25	DPI Film
18:35	5th round of questions – questions on DPI
18:45	45-min Discussion Round on DPI
19:40	6th round of questions – questions on DPI
19:50	Recommendation round
20:35	7th round of questions – general questions
20:50	8th round of questions – demographic questions
20:55	9th round of questions – evaluation of the event

Table 2: Program of the Spanish Citizen Summit

The registration process was simple: respondents were identified, and then received an empty nametag, and their table number. Mr. Emilio Aced, Head of the Inspection Unit at Spanish Data Protection Agency,

opened the summit. As he was a bit late, his speech (a PowerPoint presentation) followed Elvira's introduction and welcome speech.

Cadena Ser, the biggest private radio network in Spain was present throughout the event and prepared an extensive report on the event. A few days later, Cadena Ser invited Elvira Santiago and Vincenzo Pavone to a half-hour radio program, called Punto di Fuga. Meanwhile both Elvira Santiago and Vincenzo Pavone were interviewed by Radio Ecca, Radio Galega, Onda Cero, Radio Cope and Radio Extremadura, and also by the EFE press agency.

During the citizen Summit, the initial phase was followed by a series of general questions related to security, such as the use of technology to tackle security problems or the level of anxiety perceived by people with regard to their safety. Once participants finished answering this set of questions, the host explained that the discussion would focus on three specific surveillance-orientated security technologies (SOSTs), which were then introduced by a short documentary film, lasting about 7 minutes each. Participants had received detailed information about each technology through the booklet they received when they decided to register to participate to the citizen summit. When the film ended, the host handed over the discussion to table moderators who facilitated both exchange of opinions and deliberation at tables.

Summit participants worked on formulating recommendations for those who are in charge of choosing, using and deploying the technology. The table moderator or, in her absence the table secretary, took notes of participants' comments and remarks. A standardized template was available to table participants to help their work as a group. After having the chance of commenting advantages, disadvantages and alternatives to the SOST at the center of the discussion, participants were then asked to answer another set of questions. This time questions referred specifically to the SOST presented in the films. The same structure was repeated two times, for two different SOSTs (Smart CCTV and Deep Packet Inspection). At the end of the day, participants had a chance to provide comments and suggestion in order to evaluate the day, their experience and their overall satisfaction with the citizen summit. At the finalization of the event, participants were given a gift card, a value of EUR 50, which included reimbursement of travelling and was handed by the table moderators in return for the clickers.

3.2 Recruitment Strategy

The chosen method for the SurPRISE citizen summit was "on site recruitment". Once the target population was defined the subcontracting company identified the appropriate composition of the participants. Then, according to the required characteristics, the company elaborated a brief recruiting questionnaire that reports about:

- Socio-demographics variables:
  - Age
  - Gender
  - Geographical zone (rural, urban and metropolitan)
  - Educational level
  - Occupation
  - Household income
- Attitudinal profile
- Use and availability of new technologies
  - Computer, laptop, ...
  - Tablet, eBooks, ...
  - Smartphone
  - Other gadgets
- Time availability
- Contact details.

The recruitment company recruited participants through a random process, operating directly in those places where it was feasible to find the required profile. Each person has been approached and explained what the participation is about and the gratification obtained. If they agreed to participate, they were asked to complete the recruiting questionnaire and, in case they matched the required profile, they were included in a list of potential participants for the citizen summit. If the candidate profile was appropriated, and his/ here profile necessary, he/she was contacted to confirm the time availability and the willingness to participate. If they were still interested in attending, the company communicated them the dates and times, sent the information material and got in touch with them two more times, a week before and two days before the event.

The same company also recruited table moderators among qualitative research professionals with expertise in focus group moderation and master students in social research techniques. All moderators and note-takers attended two sessions of training: the first meeting was held two weeks before the event with a duration of three hours in which they got acquainted with the different parts and content of the event, the films were shown and they put together different tools for moderating groups. The second (two-hours meeting) was held during the morning of the event, and they reviewed the content and the agenda of the day, and became familiar with the rooms.

3.3 Structure of the citizen panel

Out of 220 confirmed participants on the day before the event, only 185 were finally present. Most people who had confirmed their attendance but ultimately did not show up were young (under 30 years). Distribution by gender was balanced (52% females, 46% males) (fig. 2). With regards to age, those under 30 and over 60 were slightly under-represented, and those in their thirties and forties were slightly overrepresented (fig. 1). The rate of ethnic minority was 9%. Whilst the different educational levels were represented in a balanced way (fig. 3), the unemployed were slightly over-represented (fig. 4), and so were the professionals and the clerical workers (fig.5).

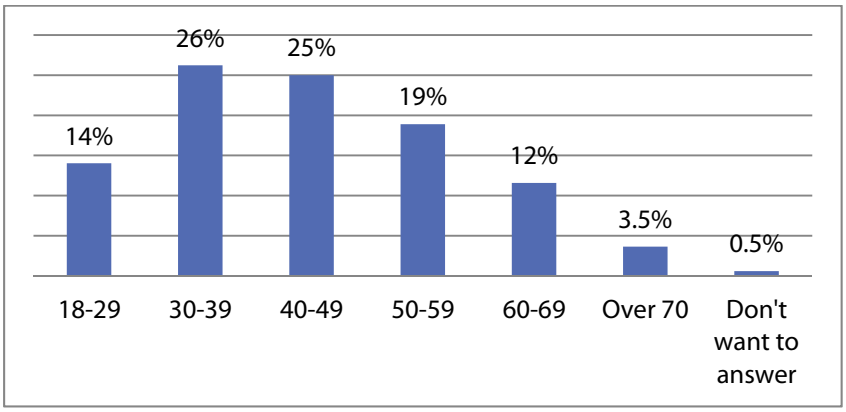


Figure 1: Age (Percentages)

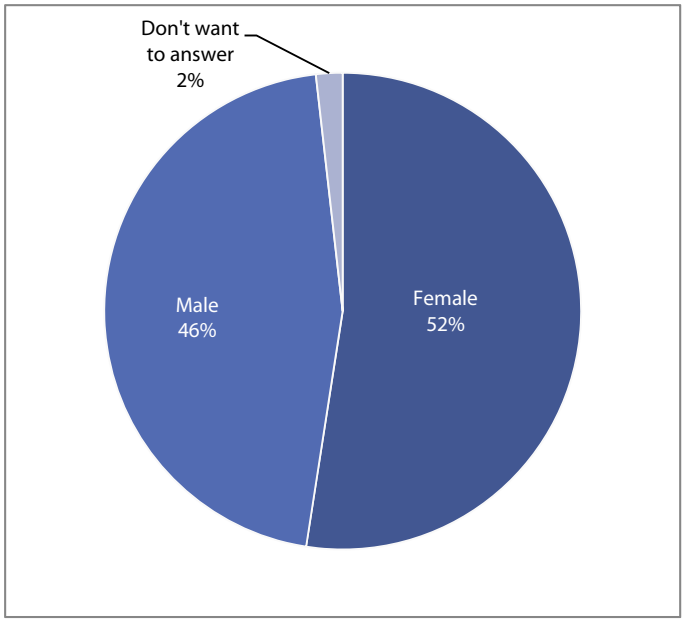


Figure 2: Gender (Percentages)

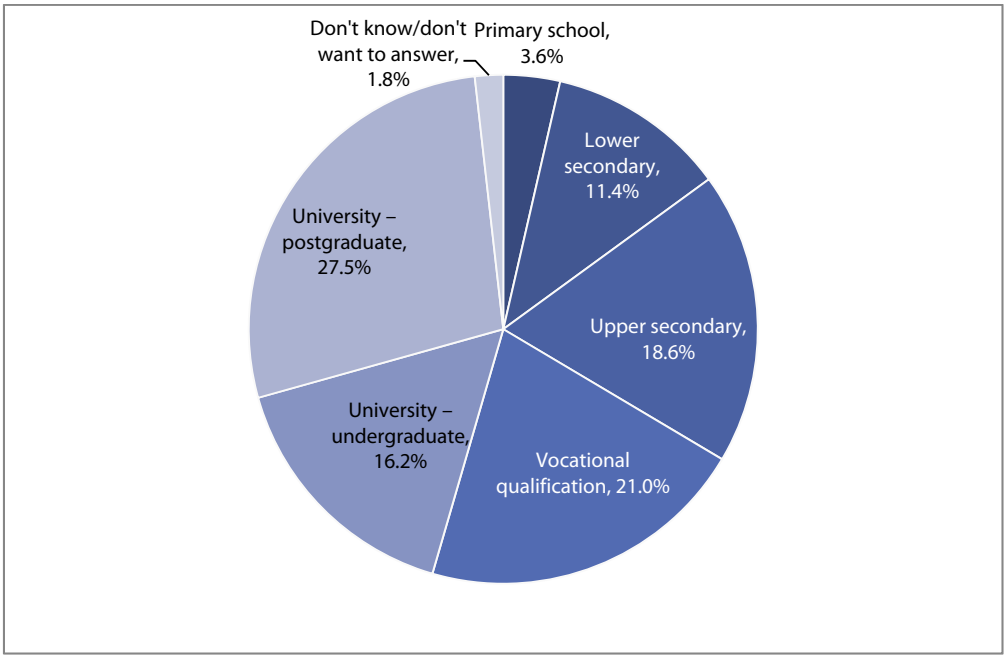


Figure 3: Level of studies (Percentages)

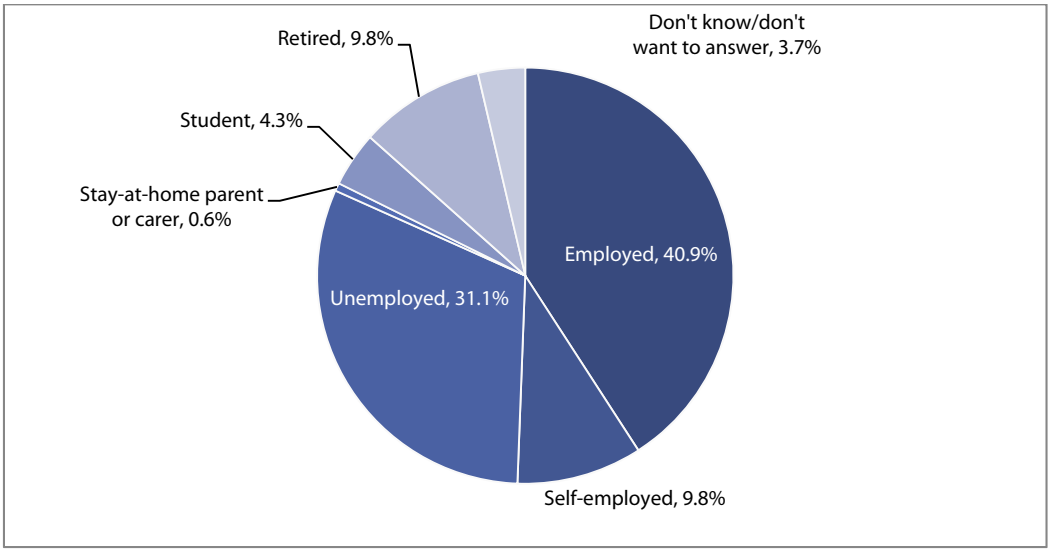


Figure 4: Occupation A (Percentages)

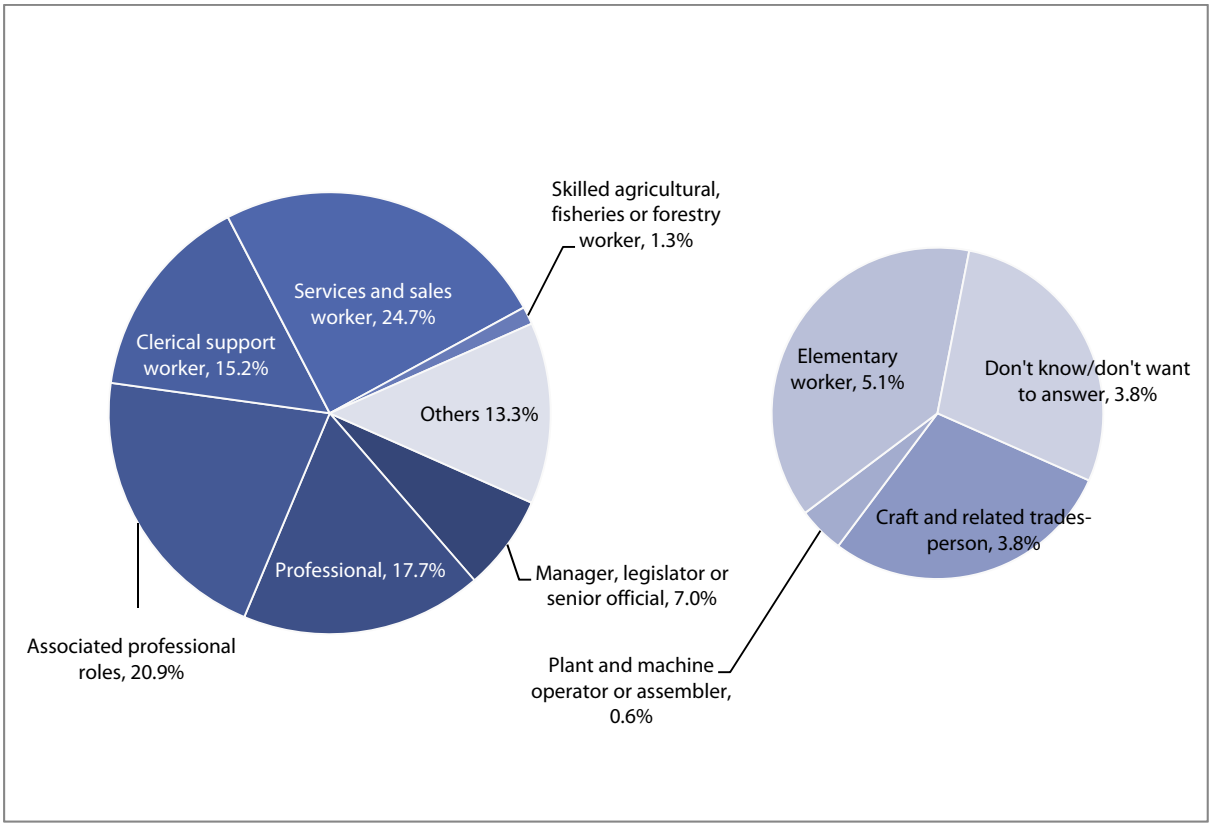


Figure 5: Occupation B (Percentages)

3.4 How citizen assessed the summit

The atmosphere was friendly and fun during the citizen summit. Both the participants and the moderators enjoyed the day. Elvira, the head facilitator led the event in a smooth and relaxed way, it had an atmosphere of a TV quiz show. She read all the answers to the questions only at the beginning, until participants were getting familiar with the clickers. It was crucial not to weary the participants.

Participants offered a very positive attitude toward the organization of the participation process feedback. They considered themselves fortunate to have been involved in this experience, they will be happy to participate in similar future events and to receive information about the results. A 77% of the participants felt that they gained a new perspective (fig. 6). The 65% agree or strongly agree with the sentence "this event produce a valuable knowledge for politicians" (fig. 7).

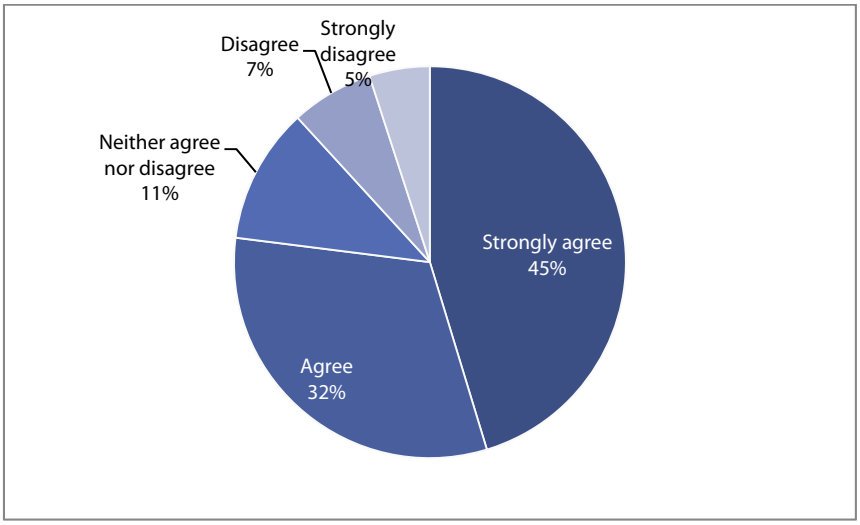


Figure 6: Evaluation question - I have gained new insight by participating in the citizen summit (Percentages)

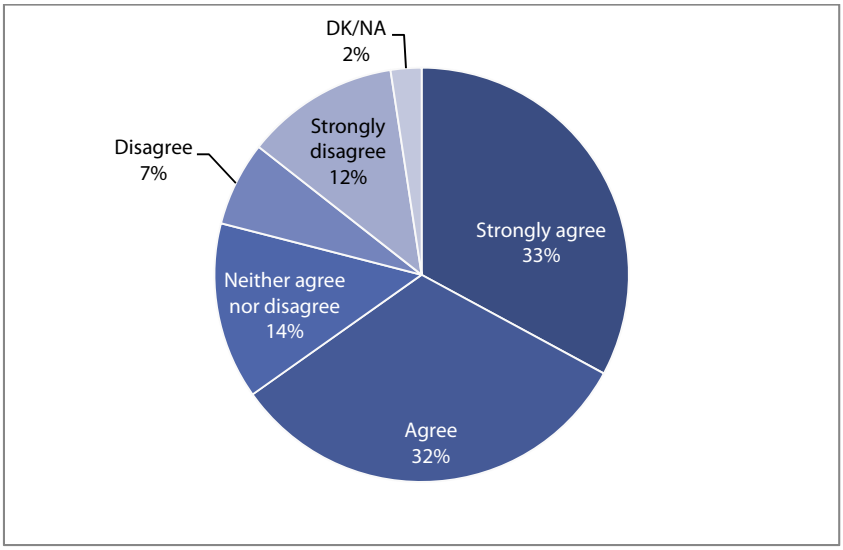


Figure 7: Evaluation question - I believe the citizen summit has generated valuable knowledge for the politicians (Percentages)

Overall, 42% of participants did not change their attitude towards SOSTs while 16% had a more positive and 39% had a more negative attitude after participating in the event (fig. 8). Yet, the general attitude towards the implementation of SOST is comparatively more negative at the end of the event. However, it is important to consider that this change in attitude, though remarkable it may look, has been less significant compared to the average change registered in the other citizen summits. In fact, in Spain the amount of participants who changed their attitudes negatively at the end of the event was 15 percent less than in the other countries of the consortium.

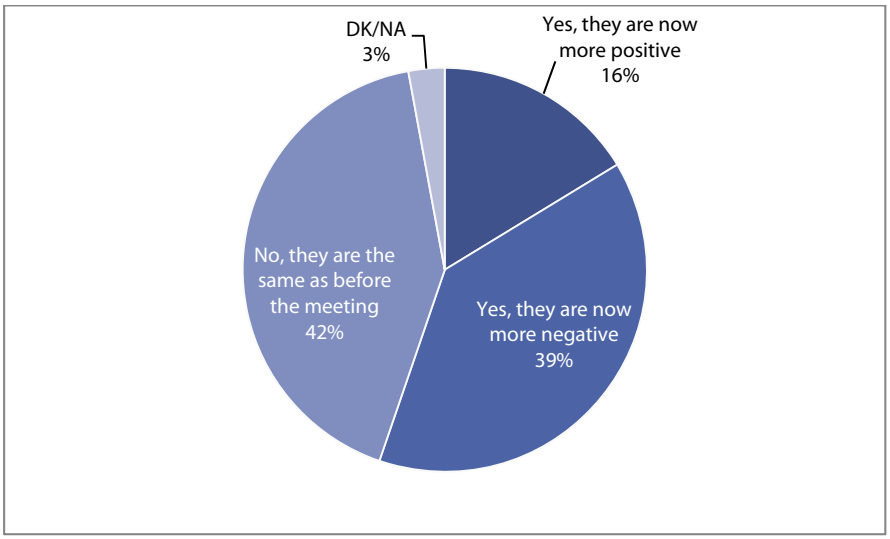


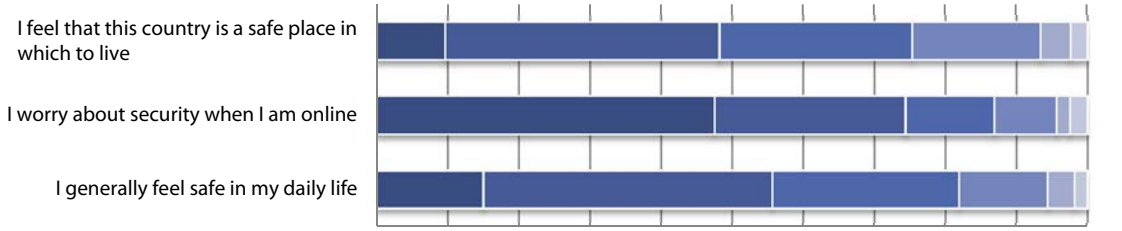
Figure 8: Evaluation question - Has this experience changed your attitudes regarding security oriented surveillance technology? (Percentages)

4 Empirical results of the citizen summit

4.1 General attitudes on privacy and security

It would be impossible to understand the level of acceptance of SOSTs without taking into account the seriousness of those threats that these technologies try to address and prevent. However, this project was not meant to measure objective level of threat - by means of crime statistics or equivalent figures -but to assess how people perceive threats around them.

In this respect, it is important to consider that the majority of the participants to the summit feel pretty secure in their daily life and consider that Spain is a safe place to live (fig. 9). Yet, this data are significantly lower than the ones retrieved in other citizen summits conducted elsewhere in Europe, where often more than two thirds of participants felt secure and safe. As a matter of fact, when we look at specific questions around the perception of security, for instance how safe participants felt in the cyberspace, the perception of security is much lower than expected. As a result, it seems that participants feel mostly secure in general terms but have worries and concerns when specific areas or domains, such as the cyberspace, are taken into account (fig. 9). This incongruence gives rise to an interesting paradox, where people who feel generally safe end up asking for more and more security measures and technologies. This paradox may be due to a number of factors, as we discuss in this report later one, and yet it may also have cultural roots. It may well be the case that our societies are indeed safe, certainly safer than they were decades or centuries ago, but citizens have changed and are less willing to tolerate risks or threats, and do not accept the feeling of being unable to act in order to reduce insecurity more and more. It seems that a desire for absolute security, which is obviously not attainable, is being gradually instilled in western societies. This would explain very well why citizens keep asking for more security even if they feel generally secure and the security of the society as objectively improved over the past twenty years.



	I generally feel safe in my daily life	I worry about security when I am online	I feel that this country is a safe place in which to live
Strongly agree	15,0	47,5	9,6
Agree	40,6	26,9	38,6
Neither agree or disagree	26,3	12,5	27,1
Disagree	12,5	8,8	18,1
Strongly disagree	3,8	1,9	4,2
Don`t know/don't want to answer	1,9	2,5	2,4

Figure 9: Perceived level of threat (Percentages)

It is again interesting to note that the attitudes towards these technologies, especially with regards to their role in improving national security, are more positive at the beginning than at the end of the event. At the beginning, 63.4 percent considered positively the role of SOSTs in improving national security, whilst at the end only 58.5 shared this idea. Meanwhile the amount of skeptical participants jumped from

19.5 to 24.5. The difference may not look very relevant, but it is the outcome of the radicalization of extreme positions: the percentage of those who radically approved of or opposed these technologies increased at the end of the event.

This process of polarization can be observed in the following figure (fig. 10):

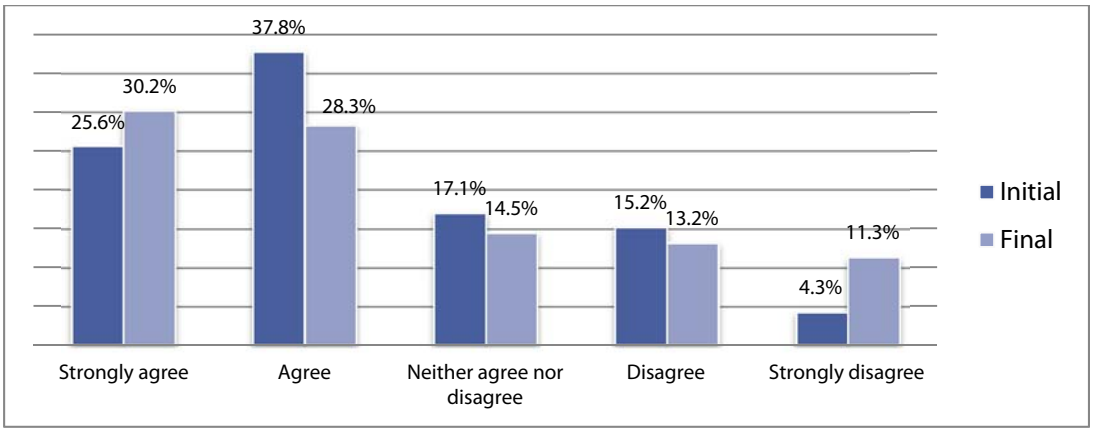
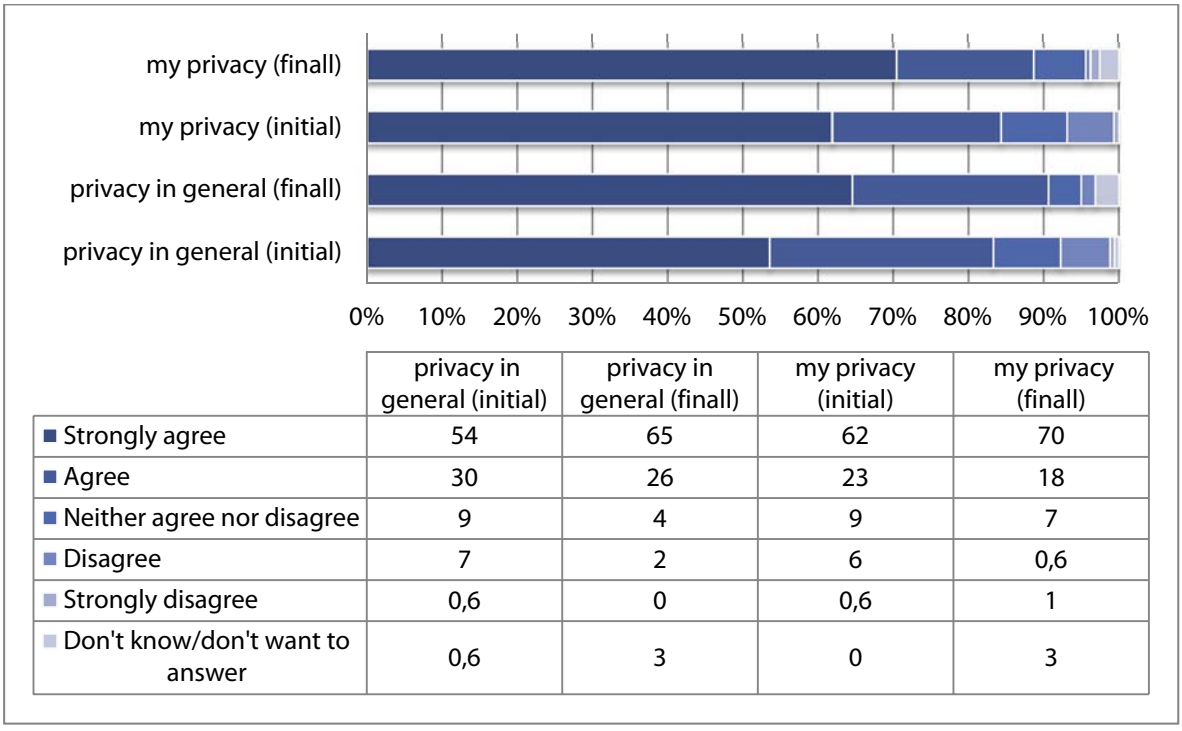


Figure 10: Changes in the security attitudes - Overall I believe surveillance-oriented security technologies should be routinely implemented to improve national security (Percentages)

A similar shift can be observed with regards to whether these technologies are perceived as intrusive and privacy infringing, in both personal and collective terms. In both cases, at the end of the event, the participants felt more concerned with privacy erosion than at the beginning (fig. 11).



	privacy in general (initial)	privacy in general (finall)	my privacy (initial)	my privacy (finall)
Strongly agree	54	65	62	70
Agree	30	26	23	18
Neither agree nor disagree	9	4	9	7
Disagree	7	2	6	0,6
Strongly disagree	0,6	0	0,6	1
Don't know/don't want to answer	0,6	3	0	3

Figure 11: Change in the security attitudes (B) - Concerned that SOSTS usage erodes... (Percentages)

4.2 How do participants perceive the use of surveillance-oriented security technologies?

4.2.1 General attitudes

Smart CCTVs (Closed Circuit Television) systems are perceived in Spain differently depending on its private or public use. Citizens are more critical towards the private use of CCTV cameras, which are considered intrusive, while quite supportive of the use of cameras in public locations. Security cameras in private establishments protect the owners of eventual theft and assault, but not ordinary citizens. The main purpose of private cameras seems to be controlling consumers' purchasing habits rather than the security of either objects or people. DPI is perceived as a measure more used to pursue economic goals than to increase public security. Traditional CCTV receives more support than smart CCTV. Smart CCTV systems located in private residential areas are considered typical examples of measures conceived to protect wealthy families and their belongings: these cameras are perceived to increase separation between rich and poor people, and increase social inequalities.

While traditional CCTV systems are considered fairly equitable forms of surveillance, it is not clear when, by whom, and for what reasons people are monitored by means of DPI. The fundamental lack of transparency and information around DPI raises serious concerns among citizens. The 'algorithmic' components of both smart CCTV and DPI also worry participants. It is not clear what are the rules establishing what it is defined normal or what is considered to be abnormal behavior. The autonomous decisions taken by algorithms also raise and leave unanswered important questions about fairness and equality. Certainly, this preliminary recognition of Surprise citizen Summit results leaves many questions open and ask for a more in-depth analysis of both quantitative and qualitative results.

Familiarity

The presence of CCTV systems in European cities' public spaces is nowadays no longer perceived by citizens as seriously intrusive or particularly annoying[42]. Citizens are familiar with this surveillance technology (fig. 12): "Surveillance of the street is not annoying as it is not an intimate space, I do not bother to see surveillance cameras in public spaces" (Group Discussion 1), which could lead us to think that their acceptability will be high based on previous studies related the effect of the familiarity increasing acceptability[43]. However, the processes by which citizens accept or reject a controversial technology are more complex and need further inquiry into the social discourse surrounding it.

In the area where you live, how often do you see CCTV cameras?				I understand what smart CCTV is		
	Frequency	Percent			Frequency	Percent
Never	26	14.4%		Strongly agree	86	47.8%
Rarely	34	18.9%		Agree	64	35.6%
Sometimes	53	29.4%		Neither agree nor disagree	11	6.1%
Often	23	12.8%		Disagree	3	1.7%
All of the time	34	18.9%		Strongly disagree	5	2.8%
Total	170	94.4%		Total	169	93.9%

Figure 12: Familiarity with CCTV

[42] Hempel and Töpfer, 2004.
[43] Slovic et al, 1986.

As far as CCTVs are concerned, the first consideration to keep in mind is that even though the cameras are familiar to the citizens (60% of the participants in the event see cameras sometimes, often or all the time; and more than the 80% understand well what CCTVs are), the participants make a clear distinction between public cameras (streets, and public buildings) and private cameras (shops and private neighborhoods). As a result, the first step to discuss the acceptability of video surveillance is to establish a clear contextualization of the use and practices. The video surveillance cameras in public places are more accepted than in privately owned ones. Participants considered that the cameras located in public spaces exert an equal and universal untargeted surveillance, which led them to define CCTV as an unbiased Surveillance Oriented Security Technology:

"The CCTVs have a function of "objective observation" of abnormal situations, whose images could go over to posteriori to have accurate information and help in clarify situations and identify suspects. Cameras are a reliable witness who provides truthful and not misleading information" (Group Discussion 1)

In a way, it is commonly accepted that the recordings of these cameras offer a real and indisputable picture of possible criminal acts, and these images can work as "objective evidences". The ability to provide such evidences is considered the cameras' main advantage, but citizens are aware that its ultimate utility is always dependent on the existing law and in what is considered as legitimate recordings.

"The CCTV are mere witnesses silent and inert of criminal situations, provided pictures as evidence, but the actual consequences of using them depend entirely on the judicial system and criminal law" (Group Discussion 15).

Despite this generally positive view of CCTVs, citizens also highlighted the inability of the camera to act in the immediate time "Although the offense committed will be serious, the aid comes from the use of the cameras is not immediate" (Group Discussion 16) and therefore they only can be considered as a useful technology to complement more sophisticated security systems: "The cameras are good because they can monitor all sites and guarantee surveillance, that doesn't mean they always watch you ... but if something bad happens…, it is a complement to security" (Group Discussion 21).

It is interesting to highlight that, in spite of the fact that 82 percent of the participants are used to navigate on the internet (a figure that is only slightly lower than the average of the consortium, i.e. 88 percent), only about 60 percent actually understand what DPI is about, which is significantly lower than the 74 percent registered for CCTVs (fig. 13). Contrary to smart CCTVs, DPI is perceived to act in the immediate time, in the present of the "here and now". As a result, the participants admitted that DPI might be useful to contrast serious crimes like terrorism or child pornography. Doubts, however, also emerged, not only because terrorists are perceived to be more sophisticated than how they are generally described: "Is not an effective tool to stop terrorists because they are more sophisticated and are not so foolish as to talk about the crimes through internet" (Group Discussion 1) but also because many participants were not really sure that DPI could help catch so many terrorists as generally believed: "How many terrorists have been caught using DPI? [This technology] questions the privacy of all to detect one" (Group Discussion 2)

How often do you use the Internet?				I understand what DPI is		
	Frequency	Percent			Frequency	Percent
Never	11	6.8%		Strongly agree	38	23.6%
Rarely	2	1.2%		Agree	57	35.4%
Sometimes	15	9.3%		Neither agree nor disagree	33	20.5%
Often	28	17.4%		Disagree	17	10.6%
All of the time	104	64.6%		Strongly disagree	13	8.1%
DK/DA	1	0.6%		DK/DA	3	1.9%
Total	161	100%		Total	161	100%

Figure 13: Familiarity with DPI

Perceived effectiveness vs. intrusiveness of SOSTs

According to the risk-benefit framework, the more beneficial and less risky a technology is perceived, the higher will be the level of acceptance and acceptability. In the context of this study, perceived risks are enclosed in the variable "perceived intrusiveness", while perceived benefits are covered by the variable "perceived effectiveness". Following Sanquist (2008), both constructs have four constitutive dimensions each.

Perceived intrusiveness is composed by:

- Risk of Disclosure – The likelihood that private information about you or some aspect of your life (such as your financial or medical records) would be disclosed without your knowledge or permission.
- Risk of Embarrassment – The likelihood that the application of the security system would lead you to feel ill-at-ease, uncomfortable, self-conscious or ashamed.
- Intrusiveness – The extent to which the security is forced upon you without invitation or permission.
- Risk of Civil Liberties Infringement – The extent to which you believe the security system might violate human rights.

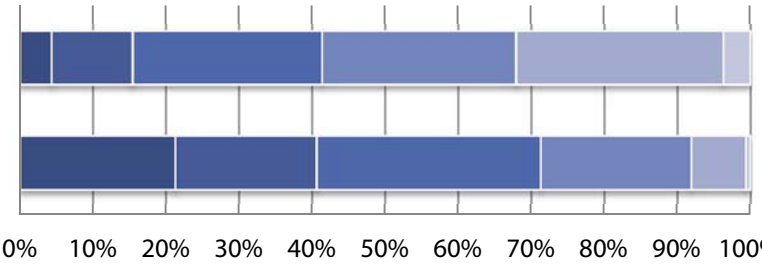
Perceived effectiveness is formed by:

- Perceived security as a personal benefit – The extent to which there is a desirable outcome, such as feeling more secure or protected, that follows as a result of applying the security system.
- Public Security – Perception that the security system is able to reduce risks of terrorist or criminal activities.
- Accuracy – The extent to which the security system properly detects and identifies risks, or contains error-free records of your personal information.
- Validity – The extent to which the security system actually addresses a real threat, and uses appropriate data to identify that threat.

While perceived intrusiveness is expected to negatively influence acceptability, perceived effectiveness should have a positive effect on acceptability. In other words, the more SOST is perceived as intrusive and risky, the less acceptable it will appear. In contrast, the more effective, accurate, and capable of enhancing personal and public security SOST is perceived, the more acceptable it will be considered.

Dimension 1: Perceived security as a personal benefit

"I feel more secure…

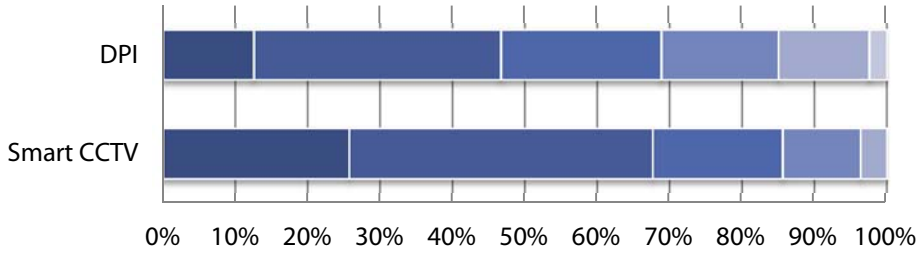


	… when Smart CCTV is in operation"	… because DPI is in use
Strongly agree	21	4
Agree	19	11
Neither agree nor disagree	31	26
Disagree	21	27
Strongly disagree	8	28
Don't know/don't want to answer	0,6	4

Dimension 2: Accuracy

"In my opinion, … is an effective national security tool."

(Percentages)

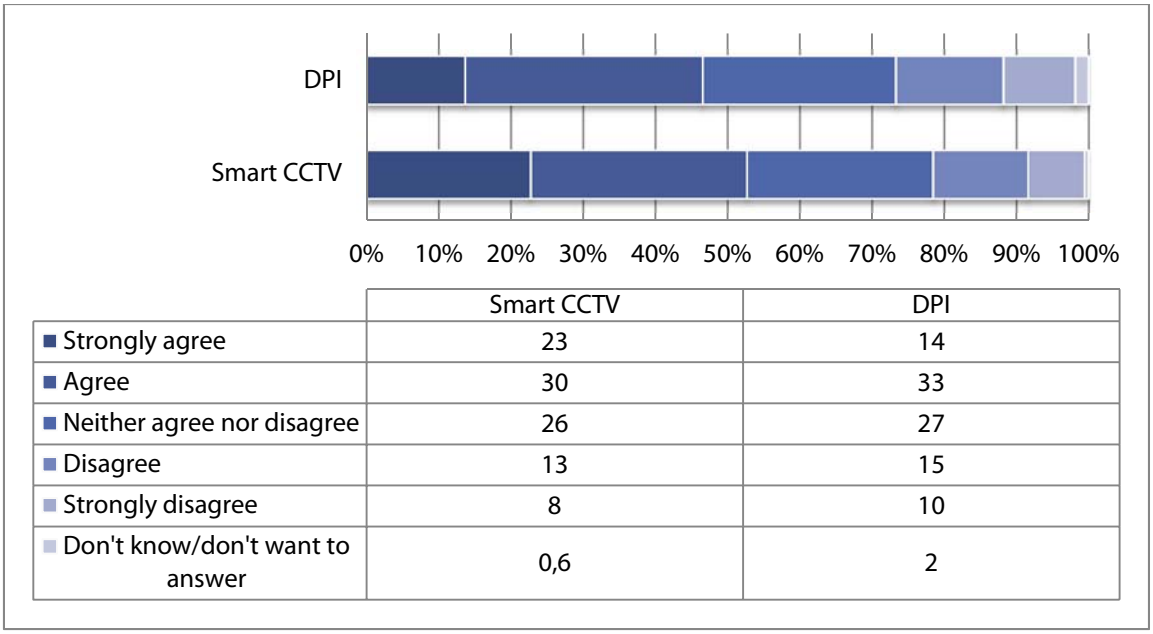


	Smart CCTV	DPI
Strongly agree	26	13
Agree	42	34
Neither agree nor disagree	18	22
Disagree	11	16
Strongly disagree	4	13
Don't know/don't want to answer	0	2

Dimension 3: Validity

"… is an appropriate way to address national security threats"

(Percentages)

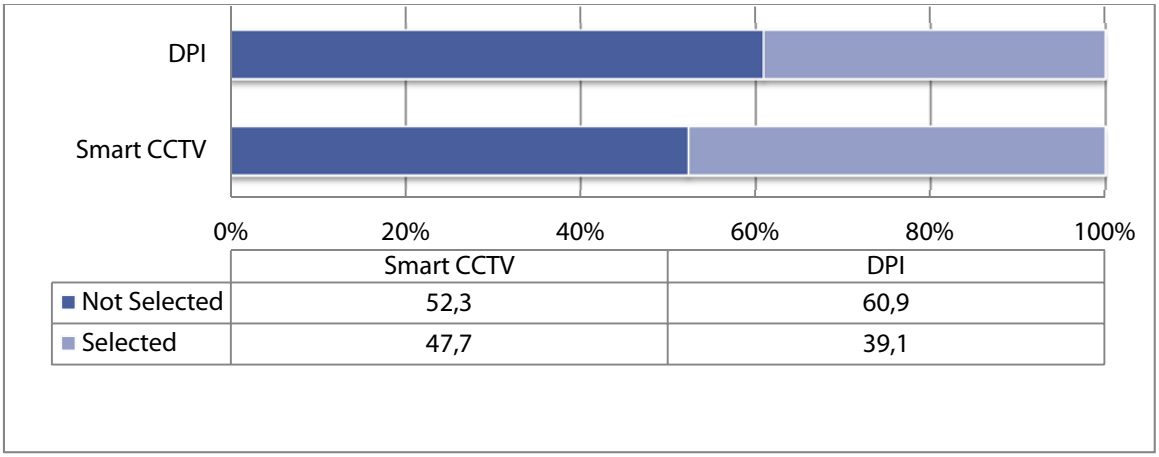


	Smart CCTV	DPI
Strongly agree	23	14
Agree	30	33
Neither agree nor disagree	26	27
Disagree	13	15
Strongly disagree	8	10
Don't know/don't want to answer	0,6	2

Dimension 4: Public security

"I believe … improves national security"

(Percentages)



	Smart CCTV	DPI
Not Selected	52,3	60,9
Selected	47,7	39,1

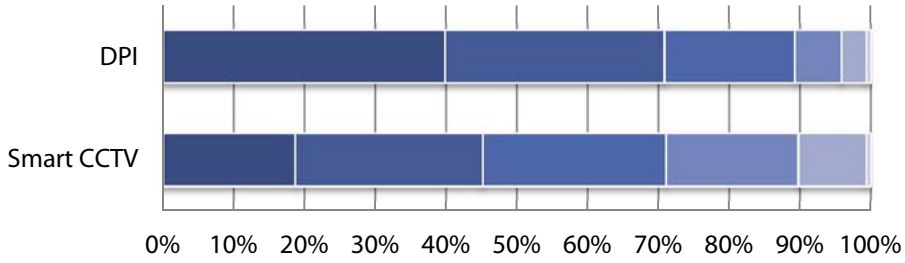
Figure 14: Perceived effectiveness (Percentages)

Although DPI and CCTVs are generally considered good tools to improve security (fig. 14), when participants were asked to consider whether such tools actually improve security, only 47.7 percent in the case of CCTVs and 39 percent in the case of DPI actually believed so. In fact, if we look at the same question this time focused in personal security the percentages are even lower: only 15.4 percent feel more secure when DPI is operated and 40.7 percent when CCTVs are at work.

Dimension 1: Risk of embarrassment

"The idea of… makes me feel uncomfortable"

(Percentages)

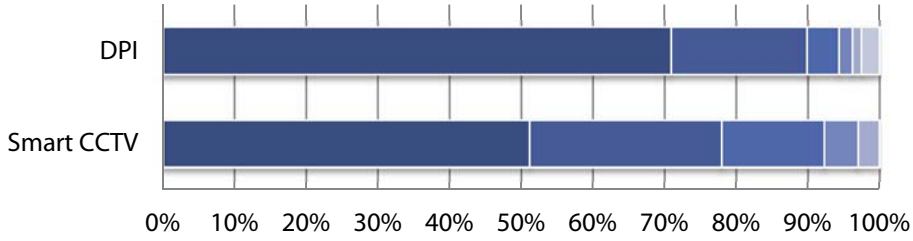


	Smart CCTV	DPI
Strongly agree	19	40
Agree	27	31
Neither agree nor disagree	26	18
Disagree	19	7
Strongly disagree	10	4
Don't know/don't want to answer	0,6	0,6

Dimension 2: Intrusiveness in terms of forcing it upon someone

"I feel … is forced upon me without my permission"

(Percentages)

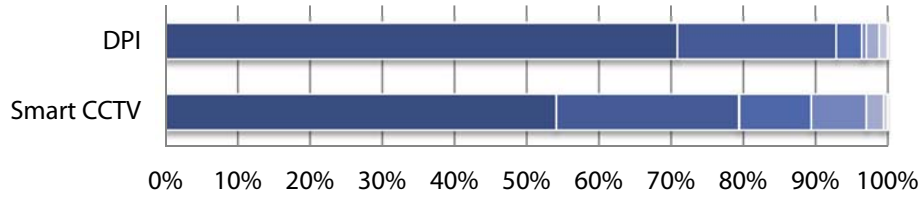


	Smart CCTV	DPI
Strongly agree	51	71
Agree	27	19
Neither agree nor disagree	14	4
Disagree	5	2
Strongly disagree	3	1
Don't know/don't want to answer		3

Dimension 3a: Risk of civil liberties infringement-individual aspect

"…worries me because it could violate my fundamental rights"

(Percentages)

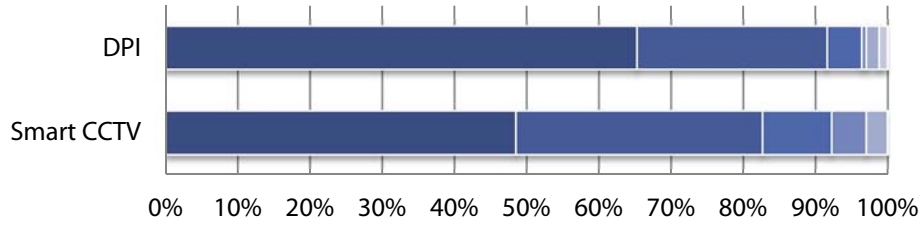


	Smart CCTV	DPI
Strongly agree	54	71
Agree	25	22
Neither agree nor disagree	10	4
Disagree	8	0,6
Strongly disagree	2	2
Don't know/don't want to answer	0,6	1

Dimension 3b: Risk of civil liberties infringement-collective aspect

"worries me because it could violate everyone's fundamental human rights"

(Percentages)



	Smart CCTV	DPI
Strongly agree	49	66
Agree	34	27
Neither agree nor disagree	10	5
Disagree	5	0,6
Strongly disagree	3	2
Don't know/don't want to answer	0	1

Figure 15: Perceived intrusiveness (percentage)

The point is that the participants consider both technologies very intrusive, with DPI perceived as more intrusive than CCTVs. The reason is, first, that participants insist that both technologies operate without their consent: this is the case for 78 percent of participants in the case of CCTVs and 90 percent in the case of DPI (Figure 15). But also the risk of embarrassment is higher in the case of DPI, as DPI makes citizens feel more uncomfortable than CCTV (70.9% of participants agree or strongly agree with the statement vs. 45.5% in the case of CCTV). Secondly, as confirmed by the debates at the tables, participants agree that both technologies violate their own fundamental rights at the social level and at the individual level, but insist that DPI could be more intrusive in this dimension than CCTVs.

In the round of group debates, the participants affirmed that the effectiveness of cameras could be appreciated in the "here and now" but, rather 'before' the criminal action is perpetrated, due to their dissuasive power or 'after' the crime has occurred, since recordings can be helpful both to look for portrayed criminals or as evidences in a trial. Nonetheless, they were also aware of the potential misuses of this technology including commercial purposes and manipulation of images "Images can be hacked or manipulated (...) there may also be a market for images" (Group Discussion 1). Misinterpretation of individual behaviors was also a matter of serious concern: 79% of participants agreed or strongly agreed the statement "Smart CCTV worries me because it could result in my behavior being misinterpreted". CCTVs were also questioned on the ground of basic civil rights such as privacy and freedom: "With the use of video surveillance cameras our privacy is trampled and our privacy is violated (…) Smart CCTV undermines the right of the individuals to be free" (Group Discussion 1). Such a statement is by no means confined to one table discussion: 79% of participants strongly agree or agree with the statement "Smart CCTV worries me because it could violate my fundamental human rights".

Compared to smart CCTVs, Deep Packet Inspection (DPI) was welcomed with even greater distrust and criticism, as it was generally considered a more intrusive technology whose implementation and modalities of operation raised remarkable concerns. The participants were especially concerned with the high degree of arbitrariness when it came to who, what, where and why DPI operators choose to monitor and track. DPI was understood as a technology that clearly requires a prior value judgment to define what are the communications, actions, words or images that may be associated to risky behaviors: "Who decides what behavior is suspicious and on what basis? (Group Discussion 21). In addition monitoring through DPI implies targeted surveillance, which is mostly oriented towards private spaces of communications and virtual interactions on the web. This specific aspect of DPI not only triggered extensive debate, it also encouraged the participants to claim that citizens should take some degree of responsibility for their self- performance while in the web: "It is our responsibility to learn how DPI works" (Group Discussion 7).

Privacy concerns

In our concise typology of privacy dimensions and functions[44], we have claimed that general privacy can be divided into information and physical privacy. Physical privacy is then partitioned into four dimensions, which are: intimacy, solitude, anonymity and reserve. Each dimension identifies a portion of personal space, which needs to be protected from intrusion. In detail: Intimacy refers to the protection of an individual's body and feelings; Solitude concerns the defense of one's geographical location; Anonymity implies the safeguard of social relationships and social behavior; Reserve is about guarding communications from prying.

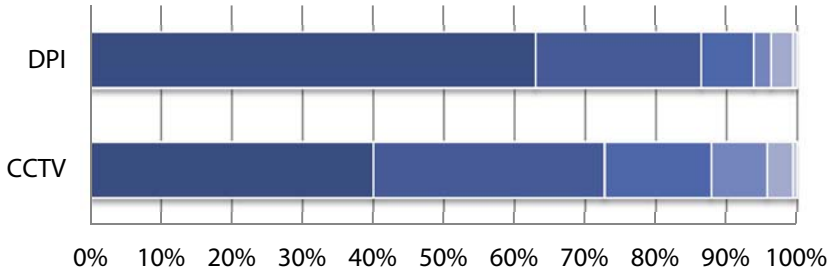
In general, the participants expressed concerns that the implementation of SOSTs may infringe their intimacy, as the concept is described and embodied in Spanish law, and reveal sensitive information about them. This was especially the case for DPI, which worried more than 86 percent of the participants, who agreed or strongly agree with the statement "DPI worries me because it could reveal sensitive information about me" (figure 16). Though not as high, 73 percent, still a very high percentage of participants were worried about CCTV. People were especially worried that DPI and CCTVs could reveal their position, but they were also concerned that the use of these technologies may cause a misinterpretation of their behavior.

[44] See Deliverable 2.2, p. 94

Dimension 1: Intimacy

".. worries me because it could reveal sensitive information about me"

(Percentages)

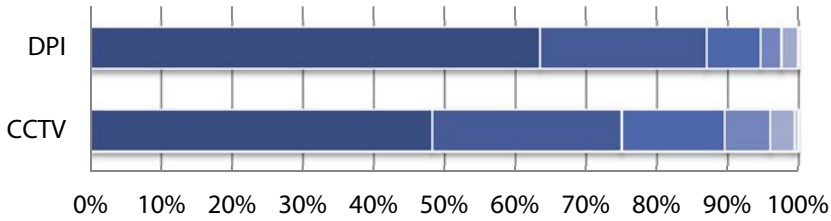


	CCTV	DPI
Strongly agree	40	63
Agree	33	23
Neither agree nor disagree	15	7
Disagree	8	2
Strongly disagree	4	3
Don't know/don't want to answer	0,6	0,6

Dimension 2: Solitude

"…worries me because it could let strangers know where I am"

(Percentages)

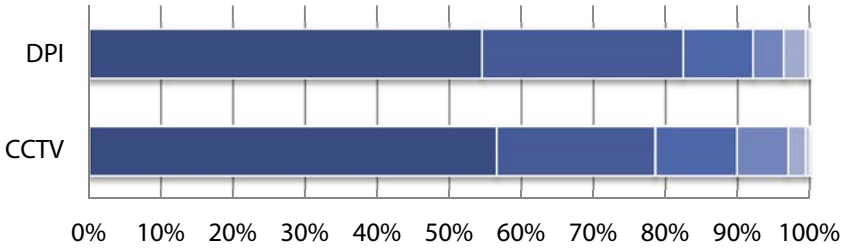


	CCTV	DPI
Strongly agree	48	64
Agree	27	24
Neither agree nor disagree	15	8
Disagree	6	3
Strongly disagree	3	2
Don't know/don't want to answer	0,6	0

Dimension 3: Anonymity

"worries me because it could result in my behavior being misinterpreted"

(Percentages)



	CCTV	DPI
Strongly agree	57	55
Agree	22	28
Neither agree nor disagree	11	10
Disagree	7	4
Strongly disagree	2	3
Don't know/don't want to answer	0,6	0,6

Figure 16: Privacy concerns (Percentages)

In the case of DPI, the major privacy concern was that DPI was perceived as monitoring and tracking what participants considered as their fundamentally private space. The participants stated clearly that their online communications should be protected exactly in the same way their mail communications were protected. Moreover, being ubiquitous and beyond reach as to when it operates, where and for how long, DPI affected citizens' private space and privacy in a way that does not allow anyone to choose whether to be monitored or not. In the table discussions, this was often contrasted to smart CCTVs whose location and operation in both public and private spaces is always announced, giving citizens the possibility to avoid places and buildings where CCTVs are installed, if they wish to do so.

Moreover, participants were especially concerned with the destination and use of their own personal information: "We do not know where all this information goes" (Group Discussion 7). As a consequence, the participants explicitly asked for a better management of private information, suggesting it was necessary to manage these data in a more transparent way, always allowing people to have access to their own data: "it should be possible to have access to our own stored data and the right to delete them or withdraw consensus to use it any time" (Group Discussion 4). In fact, some participants even suggested the creation and implementation of a law of transparency that could regulate in a clear and accessible way the retrieval, storage and use of personal information: "We need a law of transparency, as much as we have a law on data protection" (Group Discussion 5) "

Apart from the specific privacy concerns provoked by these technologies, the group debates revealed some more general concerns about information privacy. Information privacy was meant to be observed and analyzed through three main dimensions: 1) Unauthorized secondary use, 2) Improper access and 3) Errors: anxieties about accidental errors in personal data due to poor data handling, inaccurate records. If we look at both qualitative and quantitative data, Spanish participants expressed a special concern for information privacy. 91.5 percent of participants, for instance, expressed concern for the amount of personal information collected and even more, 95.7 percent, were worried about this information being shared with third parties without consent. Slightly lower percentages could be observed when it was asked about worries that this information could be used against them or that this information could be

wrong or not updated (fig. 17). These figures are significantly higher than the average of the consortium, which are around 60-70 percent on collection, errors and improper access but reach a similar 91 percent unauthorized secondary use. As a matter of fact, Spain represents the country where most concerns have been expressed about information privacy.

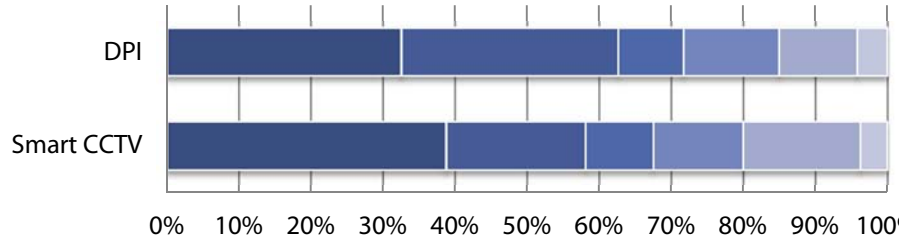
	N	Strongly agree/ Agree	Neither, nor	Disagree/ Strongly disagree	NA	Total
		Percentages				
"I am concerned that too much information is collected about me"	163	91.5%	4.8%	3.6%	-	100%
Unauthorized secondary use						
"I am concerned that my personal information may be shared without my permission"	165	95.7%	1.2%	1.2%	1.8%	100%
Improper access						
"I am concerned that my personal information may be used against me"	154	92.9%	3.2%	3.2%	0.6%	100%
Errors						
"I am concerned information held about me may be inaccurate"	165	87.9%	6.1%	5.4%	0.6%	100%

Figure 17: Information privacy concerns

Proximity

Proximity is composed of three dimensions: social proximity, space proximity and time proximity. The first one refers to the ambivalence associated with the acceptability of some SOSTs: for instance, if video surveillance focuses on criminals and not on common citizens it comes to be considered more acceptable than when it does not make distinction between criminals and common citizens. As the NIMBY[45] syndrome suggests, space proximity is also relevant when it comes to establish where it is more acceptable to have surveillance-oriented security technologies (public spaces) and where it is not acceptable (private homes, private spaces). Finally, temporal proximity focuses on the possibility of misuses in the future, that is, the lack of trust about the future use of the information retrieved through SOSTs, which may negatively affect the acceptability of them.

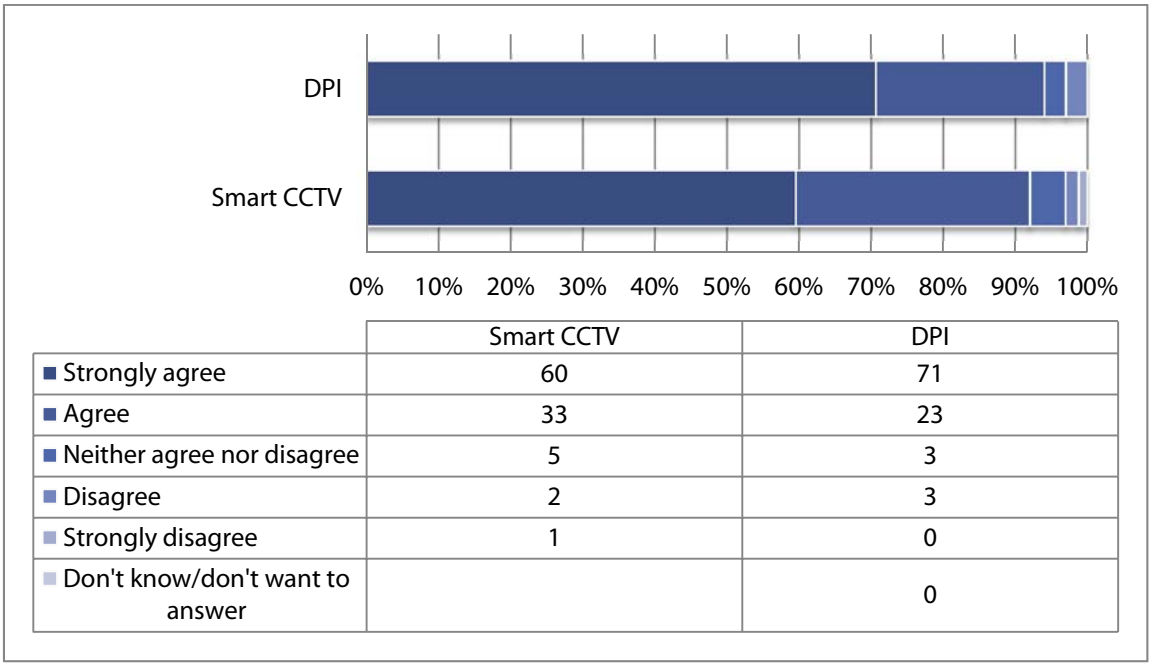
[45] Not In My Back-Yard: in the litearature of public understanding of science and risk studies, this is the acronym used to denote the typical attitude of those citizens who are in favor of given technologies to be introduced but only insofar these are implemented far from their meaningful life spaces, i.e. home, work etc…



	Smart CCTV	DPI
Strongly agree	39	33
Agree	19	30
Neither agree nor disagree	9	9
Disagree	13	13
Strongly disagree	16	11
Don't know/don't want to answer	4	4

Figure 18: *Social Proximity* "… does not bother me as long as it only targets criminals"(Percentages)

Figure 18 shows clearly how the participants would be less worried about the implementation of SOSTs if the latter were consistently and exclusively oriented towards targeted criminals (58% agree or strongly agree with the statement in the case of Smart CCTV vs. 48% average of the consortium, and 63% in the case of DPI vs. 54 percent average of the consortium). The difference between DPI and CCTVs is possibly due to the fact that the latter are mostly installed in public spaces, which makes it more difficult to configure them in such a way that they may target exclusively criminals or suspects. However, the participants proposed clear criteria to operate these technologies: "DPI should only be used to monitor specific people, who have criminal records and only after judicial consent; CCTVs should only be operated in public spaces" (Group Discussion 1). Nonetheless, the participants expressed some skepticism about the real capability of these technologies to help catch the most serious criminals, who are considered to be able to use sophisticated tools and procedures to avoid DPI surveillance: "It may not be so effective, considering that terrorists are more sophisticated and not so careless as to use the internet to organize their activity and communicate with each other" (Group Discussion 1).

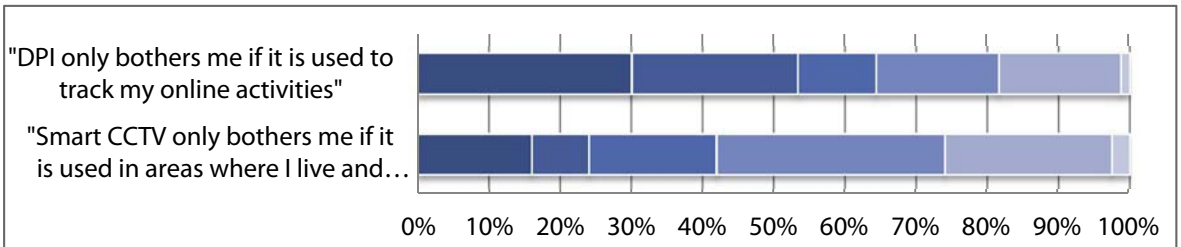


	Smart CCTV	DPI
Strongly agree	60	71
Agree	33	23
Neither agree nor disagree	5	3
Disagree	2	3
Strongly disagree	1	0
Don't know/don't want to answer		0

Figure 19: *Temporal Proximity* "I worry about how the use of… could develop in the future"(Percentages)

As figure 19 shows, the possible use of these technologies in the future also generates important concerns, which negatively affects their acceptability. A staggering 93 percent of the participants are concerned the future use of CCTVs (agree or strongly agree with the statement) and an even more disquieting 94 percent is worried about the future use of DPI. These figures are especially high and above the average found in the consortium, which stay at 67 percent for CCTVs and 87 percent for DPI. Yet, it can also be observed that they come close to the German figures for CCTVs and to the Austrian figures for DPI.

Looking at the prospected future, and even in the case SOSTs are currently used in an acceptable and controlled way, the participants are worried that these technologies may be easily abused in order to match the interests of powerful political elites and/or commercial actors. "The use of SOSTs can be good when used well, the problem is when they are used without control" (Group Discussion 5). The participants, thus, expressed clear interest in knowing not only how technologies are used and regulated today, but also how are they likely to be used and regulated in the future and how likely is that they can be abused. That is why citizens demanded that clear limits on what are the frameworks for action for this kind of surveillance-oriented security technologies, what are the parameters under which surveillance acts.



	"Smart CCTV only bothers me if it is used in areas where I live and work"	"DPI only bothers me if it is used to track my online activities"
Strongly agree	16	30
Agree	8	23
Neither agree nor disagree	18	11
Disagree	32	17
Strongly disagree	23	17
Don't know/don't want to answer	2	1

Figure 20: Spatial proximity (Percentages)

It is interesting to highlight that the spatial proximity not only is perceived very differently in the cases of DPI and CCTVs, it is also affects the acceptability of these technologies in opposite directions (fig. 20). This is probably due to the fact that CCTVs are only generally used in public spaces and people in Spain are used to their presence in these spaces, which are not perceived as especially private. The opposite is true for DPI, which is used to monitor our communications and social interactions on the internet, which is perceived as a much more private space of interaction: "The surveillance of a public street does not bother me too much because that is not an intimate space. […] In contrast, DPI infringes my right to intimacy completely…I mean it is inside my house!" (Group Discussion 1).

Trade-off

Only those people who believe that SOSTs are privacy infringing and security enhancing at the same time can be considered to adopt the trade-off approach[46]. However, other approaches are also theoretically possible:

- People may consider SOSTs as useful in terms of security and with no risk for their privacy. This group, characterized by a high level of confidence in the context implementing SOSTs, considers security the main issue.
- Alternatively, they may consider SOSTs as a useless solution to enhance security, but as a very risky option for their privacy. This group, characterized by an overall concerned attitude towards SOSTs, gives priority to the protection of privacy as the fundamental issue at stake.
- Finally, they can consider SOSTs both useless to increase security and innocuous in terms of privacy. These people can either find the debate uninteresting or they could use alternative, unexplored categories to frame the relationship between privacy and security.

[46] Pavone and Degli Esposti, 2012.

In the Spanish Citizen Summit, half of the participants – 51% in CCTVs (fig. 21) and 56.2% in DPI (fig. 22)– actually adopted this specific frame to consider the relationship between privacy and security: they explicitly affirmed that security and privacy stood in a zero-sum game, as SOSTs were perceived as both privacy infringing and security enhancing. However, this does not mean that they were willing to trade privacy in exchange for security, as only a very small percentage of them were prepared to do so. The other half of the participants did not adopt the trade-off approach, and believed that these technologies are either highly intrusive but not really effective (21.1% for CCTV and 28.4% for DPI), or, quite to the contrary, considered these technologies very effective in terms of improving security but not really privacy infringing (23.5% for CCTV and 11% for DPI). Finally, a very small group of participants believes that SOSTs do not increase security levels but do not infringe privacy either (1.2% for CCTVs and 2.5 % for DPI).

	Useful	Useless
Highly intrusive	51.2%	21.1%
Not very intrusive	23.5%	1.2%

Figure 21: Trade- off Smart CCTV

	Useful	Useless
Highly intrusive	56.2%	28.4%
Not very intrusive	11%	2.5%

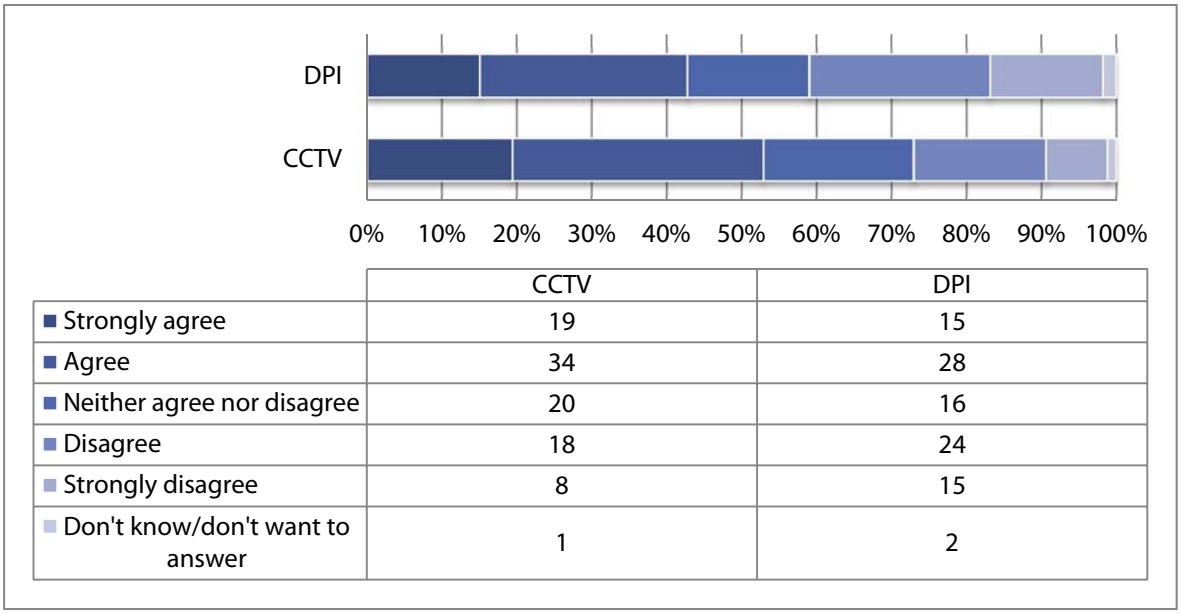
Figure 22: Trade- off DPI

Some participants, who insisted that privacy and security could co-exist, explicitly challenged the trade-off approach. The traditional approach based on the trade-off is based on the idea that citizens trade (voluntarily) part of their privacy in exchange for more security, as if they were buying goods in the market. In this summit, some participants made it clear that there is no exchange at all: whilst they feel forced to renounce to part of their privacy, it is not clear what they get in exchange for it and what are the rules that regulate this (forced) exchange: "There is no trade-off between privacy and security, we have to provide our personal information but there is no control and it is not clear what happens afterwards" (Group Discussion 11). In this context, it is easy to understand why there is a general attitude of mistrust, which, however, is not directed so much towards the security technology per se but rather to its use and implementation: "Whilst the use of these technologies may be good when it used correctly and for the right purposes, the problem arises when these technologies are used without control" (Group Discussion 5)

Another problem is that the risks that such technologies are intended to prevent are often specific risks that may affect individual citizens differently. For example, most ordinary people are concerned about terrorism and consider it one of the major problems of the contemporary world, yet very few citizens believe they may be victims of a terrorist attack. Therefore the cost of using these technologies may be perceived very differently, even when is commonly believed that these technologies may be very effective. Most of the times, considering the risk-benefit balance of many of these technologies, they are considered excessive, especially when the threat to democratic values and human rights they constitute is taken into account. In many cases, the risks and benefits in the use of these technologies are accounted for at different levels, because benefits are most often considered at individual level whilst the risks are usually assessed at the level of social structures and values. Obviously, individual experiences may affect this general posture, for someone who has been victim of a terrorist attack or has some family who experienced it, will tend to evaluate both risks and benefits at the individual level and be more prone to accept any limitation of rights and freedoms in order to increase security and be protected from these threats.

Acceptability

A technology is considered acceptable when it is capable or worthy of being accepted, which means that it is received favorably or with approval, and also capable of being endured, because it is tolerable, adequate, and conforms to approved standards. In the pursuit of a difficult balance between acceptable and inacceptable uses of CCTV, citizens clearly believe that only public authorities should implement, control and operate smart CCTVs in order to guarantee of the effectiveness and the correct use of CCTV. Public authorities should also control and manage the storage of the images recorded using a transparent protocol. "Citizens need more justification and transparency in relation to who is managing your images recorded by CCTVs" (Table Discussion 15). This action protocol must collect in detail the procedure to be followed to inform citizens about their rights and the ability to retrieve their recordings if it is needed for security or privacy purposes: "Responsible authorities should ensure access to the stored data itself and the right to delete or revoke consents" (Discussion Group 2).



	CCTV	DPI
Strongly agree	19	15
Agree	34	28
Neither agree nor disagree	20	16
Disagree	18	24
Strongly disagree	8	15
Don't know/don't want to answer	1	2

Figure 23: Overall I support the adoption of SOSTs as a national security measure (Percentages)

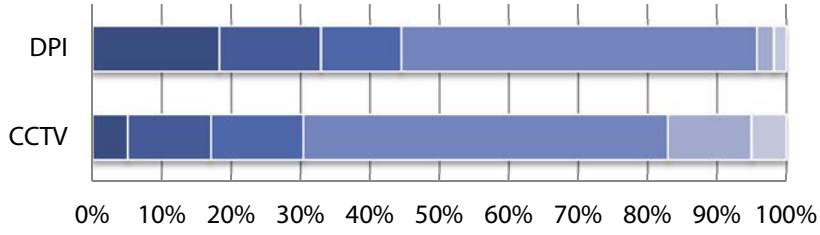
As figure 23 shows, DPI as a security measure is only accepted by 43 percent and rejected by 39 percent of the participants, whilst CCTV is more accepted, as nearly 53 percent supports its adoption and only 26 percent rejects it. In general, Spanish participants are less inclined to support the adoption of these technologies, compared to the participants in the other countries, but it is important to consider that there is a significant amount of participants, 20 percent, that is undecided; this percentage is similar to Germany but the amount of people explicitly in favor of the adoption of CCTVs there only reaches 15 percent.

Engaging in interesting comparisons between DPI and smart CCTVs, participants were also involved in relevant discussions on the general political and social context in which these technologies are implemented and operated. Participants criticized the fear-based approach used not only to increase their feeling of insecurity but also to manipulate their opinion in order to make these SOSTs more acceptable. A participant from group 11 compared the ubiquitous use of DPI to an indiscriminate use of antibiotics, even for minor illnesses: "With DPI, it is used the same fear approach that is ill used in the case of the use of antibiotics" (Group Discussion 11).

4.3 Avoidance and resistance against surveillance

The participants showed very different attitudes towards the two technologies discussed and assessed in the summit. For instance, only about five percent of the participants would actively engage in any activity that may effectively reduce the use of CCTVs whilst this percentage rises to 18 percent in the case of DPI (fig. 24). It is clear that DPI, for the reasons mentioned above, mobilizes more resistance and opposition then CCTVs. The point is that DPI is considered definitely more intrusive than CCTVs. However, it is also important to point out that the Spanish participants expressed more resistance towards DPI than the rest of the participants in the other countries and that the difference between resistance to DPI and CCTVs is higher in Spain than elsewhere. In spite of their higher acceptance in Spain, CCTVs are not opposed only by 12 percent (fig. 24), whereas the acceptance, or non-opposition, is 28 percent on average in the rest of the countries. The same applies to DPI: non-opposition to DPI reaches only 2 percent in Spain (fig. 24), but increases to 11 percent, on average, in the rest of the countries organizing the citizen summit and evaluating these technologies.

One of the main reasons behind resistance and active opposition to SOSTs in Spain is that these technologies are considered to advance too rapidly, in such a way that this generates mistrust and concern. As a matter of fact, both in the cases of CCTVs and DPI, several participants considered that these technologies advance more rapidly than the society (Group Discussion 11). In both cases, the majority of the participants asked for more information on both the advances of the technologies and about the ways in which it may be still possible to protect their privacy: "There must be public campaigns to inform citizens on what are the implications of using internet" (Group Discussion 16). In fact, the participants also asked for information on how to access their data and how to use them: "we need to get information on how to complain and how to solicit information, to whom and how can citizens use their own information, for instance in a trial or in a civil litigation" (Group Discussion 18).



	CCTV	DPI
I am prepared to use any means I can to prevent its use	5	18
I am prepared to campaign actively against its use	12	15
I would support others who were protesting against its use	13	12
I would like to find out more how to protect my privacy	53	51
I do not oppose it at all	12	2
Don't know/don't want to answer	5	2

Figure 24: Challenging the use of the technology for security purposes (Percentages)

As a result, we may expect an active mobilization to avoid the use of these technologies or to avoid being exposed to them. In fact, the majority of the respondents would not change their behavior in order to avoid the surveillance that the implementation of these technologies implies. As shown in fig. 25, it is important to consider that the amount of participants who may be willing to change their behavior in

order to avoid the surveilling gaze of the technology is significantly higher in the case of DPI than in the case of CCTVs (29,4 percent vs. 13.3 percent)

smart CCTV		DPI	
Percentages			
I would never go into areas where smart CCTV is used	5.1%	I would not go online because of DPI	2.5%
I would avoid going into areas where smart CCTV is used	12.0%	I would avoid going online because of DPI	6.1%
I would change my behavior in areas where smart CCTV is used	13.3%	I would change how I behave online because of DPI	29.4%
I do not think I would change my behavior because of it	52.5%	I do not think I would change my behavior online	40.5%
I would definitely not change my behavior because of it	12.0%	I would definitely not change my behavior online	12.9%
NA	5.1%	NA	8.6%
Total	100%	Total	100%

Fig. 25: Active avoidance of the technology

4.4 Perceptions of individual and collective aspects

Participants are aware that the implementation of new security technologies is part of a legitimate strategy of lowering the costs of security: "These technologies are cheaper in relation to human resource to be used to have the same security" (Group Discussion 7), but they still prefer higher investments in traditional human resources, such policemen, judges and security operators: "Years ago security was really dependent on the local policy, or on the serenos, who were people paid by local residents to watch the streets at night, but now the police forces have been reduced, these other figures have disappeared and they have been completely replaced by technologies that have been developed very far away (Group Discussion 22), and an increase in civil solidarity: "It would be very important to educate people to those values that promote solidarity and unity among neighbors, which in turn would reduce the crime rates" (Group Discussion 11).

Yet, if security has to be necessarily improved through security technologies, participants claim that there is urgent need for a new legislation adapted to the new realities of this century and its new threats. This legislation should be designed, approved and respected at European level but without neglecting regional inequalities: "A global comprehensive legislation to provide transparency and information to citizens" (Group Discussion 6). In this new system, control mechanisms must be transparent and citizens should receive clear information about the use and rules of security technologies: "We, the citizens, we need more transparency and legitimate justification about who accesses our information and for what purposes" (Group Discussion 15).

As previously observed, and consistently with the following table, participants' attitudes towards SOSTs are caught in a paradox: whilst SOSTs are generally considered a suitable instrument to improve security, at the individual level they are not perceived as actually doing so. Moreover, SOSTs generate several concerns related to their use, to the actual regulation and to the possible abuses. Even when participants considered that there is nothing about their individual behavior that convert them into a suspect, 60 percent of them believe that SOSTs generate concern and 90 percent affirm that, once in operation, they can easily be abused by the security agencies or the public authorities (fig. 26).

	N	Strongly agree/ Agree	Neither, nor	Disagree/ Strongly disagree	NA	Total
		Percentages				
Positive attitude variables						
"The use of surveillance-oriented security technologies improves national security"	159	58.5%	14.5%	24.5%	2.5%	100%
"If surveillance-oriented security technology is available national governments might as well make use of it"	171	40.9%	18.1%	39.7%	1.2%	100%
"If you have done nothing wrong you do not have to worry about surveillance-oriented security technologies"	173	29%	10.4%	60.2%	0.6%	100%
Negative attitude variables						
"Surveillance-oriented security technologies are only used to show that something is being done to fight crime"	170	26.5%	17.1%	55.9%	0.6%	100%
"Once surveillance-oriented security technologies are in place they are likely to be abused"	163	90.8%	2.5%	5.6%	1.2%	100%

Figure 26: Positive and negative attitudes

4.5 Perceptions on the trustworthiness of security authorities

It is been hypothesized that social trust simultaneously influences both perceived risks and perceived benefits. For most technologies, the associated risks and benefits are not directly visible; therefore, people rely on risk-benefit information provided by the sources they trust[47]. Trust in authorities, companies and scientists involved in regulating or using a technology was found to have a positive influence on perceived benefits and a negative influence on perceived risks[48].

Whilst this general view on social trust was found to be correct, the Spanish Citizen Summit provided interesting insights about it. The participants made clear, for instance, that trust in operating and regulating actors can only be limited and contextualized: participants' trust was presented as dependent on a number of social and institutional factors. For instance, it was framed as dependent on whether the purpose for which the technology is implemented is actually respected and what are the rules and principles governing the operations of those in charge of controlling the controllers, so to speak: "Who watches the watchers in charge of the cameras?" (Group Discussion 7). Trust and confidence cannot, thus, be considered as stable postures: they need to be constantly negotiated: "Responsible authorities must be honorable, this is the best recommendation and the most important security measure. If you put CCTVs, police forces and more and more employees but then the institution is not honorable … you just cannot trust them" (Group Discussion 19). The problem is, as they often remark, that "We have no choice but to trust the experts, as we they were doctors or physicians" (Group Discussion 4). What is needed, they insist, is that "a guarantee that the use of SOSTs is exclusively linked to security purposes is needed at all times, otherwise mistrust is inevitable" (Group Discussion 2).

[47] Siegrist and Cvetkovich, 2000.
[48] Pavone and Degli Esposti, 2012.

Another interesting finding in the group debates – which supports the socio-cultural approaches to the analysis of risk – relates to the need of involving the public in order to manage new risks and new threats of the twenty-first century. SOSTs should be regulated at European level to ensure fairness of treatment to all Europeans whilst national and regional peculiarities and demands should contribute to shape overarching policies. For instance, in order to combine effectiveness and legitimacy, participants asked for an institutional mediator or tutor, able to create a permanent and effective communication between security agencies and public authorities and civil society. The technology mediator should ensure that citizens have access to all the information they require in relation to their own data. It should inform citizens about their rights and duties and make politicians and regulators aware of citizens' opinions, concerns and suggestions. Moreover, citizens seemed to be willing not only to contribute to bear the responsibility of the protection and preservation of their data, but they wanted also to collaborate in the design of public policies and new technologies. Citizens wanted to participate actively in controlling infractions and abuses in the use of surveillance technologies.

Social trust in the authorities responsible for the use of SOSTs, therefore, is not a universal but a contextual value, which needs to be renegotiated over and over again, especially at local level. Trust is negotiated all the time, in relation to each technology and changes along with the institutional, organizational and cultural context; it is ignited and maintained only through the existence and correct function of clear rules, transparent information and effective participatory practices.

In this respect, participants expressed clear interest in knowing not only how technologies are used and regulated today, but also how they will be used and regulated in the future to prevent abuse. That is why citizens demand that clear limits on what are the frameworks for action of this kind of surveillance orientated security technologies, what are the parameters under which surveillance acts. Participants' trust in operating and regulating actors is limited and contextualized: their confidence depends on whether the purpose for which the technology is implemented is actually respected and so are the rules and principles governing the operations of those in charge of controlling the controllers.

"There is nothing new to be invented. If usually police needs a court order to act, on the Internet the same legal requirements should be applied to safeguard our privacy. Technology is used against citizens. They must comply with what's written in the Convention on Human Rights!" (Group Discussion 5, facilitator's reflections)

Within this framework, it is easy to imagine how strongly the participants mistrust public authorities and security agencies using CCTVs and DPI. Sure, as figure 27 shows, such mistrust is higher in the case of DPI (54.2 percent) then in the case of CCTVs (44.4 percent) but it is equally distributed when it comes to assess the competence of public authorities and security agencies in operating these technologies: in both cases nearly half of the participants believe that these institutions are not sufficiently competent. Most importantly, around eighty percent of the participants believe that security agencies do abuse their power when operating CCTVs (77.3%) and DPI (82%) (fig. 28).

		Totally agree	Agree	Neither agree nor disagree	Rather disagree	Totally disagree	NA
	N	Percentages					
Security agencies which use Smart CCTV are trustworthy	171	7%	17.5%	30.4%	29.8%	14.6%	0.6%
Security agencies which use Smart CCTV are competent at what they do	164	4.9%	10.4%	37.4%	28.7%	13.4%	3%
Security agencies which use Smart CCTV are concerned about the welfare of citizens as well as national security	165	9.1%	13.3%	26.7%	29.1%	21.2%	0.6%
Security agencies which use Smart CCTV do not abuse their power	172	3.5%	5.8%	12.2%	32.0%	45.3%	1.2%

Figure 27: Level of Institutional Trustworthiness – smart CCTV.

		Totally agree	Agree	Neither agree nor disagree	Rather disagree	Totally disagree	NA
	N	Percentages					
Security agencies which use DPI are trustworthy	166	7.2%	15.1%	21.1%	32.5%	21.7%	2.4%
Security agencies which use DPI are competent at what they do	161	4.3%	12.4%	30.4%	30.4%	14.9%	7.5%
Security agencies which use DPI are concerned about the welfare of citizens as well as national security.	167	9%	15%	25.7%	24%	24%	2.4%
Security agencies which use DPI do not abuse their power	173	1.7%	2.9%	10.4%	30.6%	51.4%	2.9%

Figure 28: Level of Institutional Trustworthiness – DPI.

4.6 Role of alternative security approaches

Participants are aware that the implementation of new security technologies is part of a legitimate strategy of lowering the costs of security, but they still prefer higher investments in traditional human resources, such as policemen, judges and security operators. Needless to say, participants insists that it will be a better alternative strategy to invest in the real causes of the insecurity, the lack of education and employment that are the most important causes of social exclusion.

"Our suggestion? Eradicate insecurity causes: invest in education and generate new jobs: unemployment is a main source of insecurity." (Group Discussion 5,)

Yet, if security has to be necessarily improved through security technologies, participants claim that there is urgent need for a new legislation adapted to the new realities of this century and its new threats. This

legislation should be designed, approved and respected at European level but without neglecting regional inequalities.

"Our suggestion? A global comprehensive legislation able to increase transparency and public awareness." (Group Discussion 6)

In this new system, control mechanisms must be transparent and citizens should receive clear information about the use and rules of security technologies.

"…[We need] The creation of a system, a network, a set of powerful communication campaigns with the aim to provide clear and easy to understand information to the public to let people know where they need to go if they want to complain, who people should contact to make a request and finally to let people know how they could claim back their personal information if at some point they need it (in a judicial trial or to face an accusation)." (Group Discussion 9)

Participants also suggest the creation of a new figure, a mediator, that allows citizens to connect with the authorities responsible for the use and regulation of these technologies, in order to have access at all times to their personal information, to where, when and why their privacy has been legally infringed and to what are their rights in case of abuse.

"Our suggestion? The creation at regional or national level of a technological public advocate, a figure similar to the Ombudsman" (Group Discussion 9)

Needless to say, participants insisted that it will be a better alternative strategy to invest in the real causes of the insecurity, the lack of education and employment that are the most important causes of social exclusion. "The best way to prevent crime is to invest in education, work and empowerment" (Group Discussion 22).

As a matter of fact, the support for the adoption of alternative measures to security is very strong, both at the beginning (64.4 percent) and at the end of the event (74.1 percent). The increase of support is not so much due to a change of mind among skeptics but rather to the reduction of undecided participants, who were 22.9 percent at the beginning of the event and only 13.8 percent at the end (fig. 29).

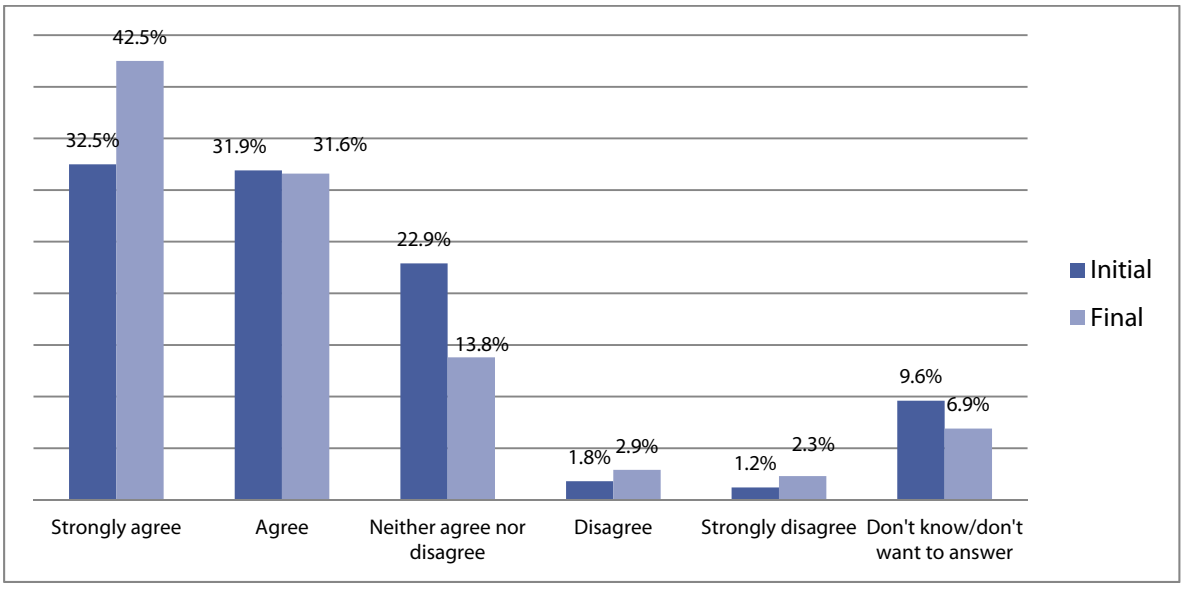


Figure 29: Alternative approaches to security which do not involve surveillance-oriented security technologies should be given higher priority (Percentages)

4.7 Citizens' recommendations to policy makers

Participants agreed that new technologies improve security to some extent, but they stated that their usage should be restricted in order to make them less intrusive. Regarding DPI (or "Deep Package Inspection"), participants believed that it should only be used to monitor specific individuals who have previously committed a crime and after having obtained a court warrant. CCTV should be restricted to public spaces. The use of these technologies should be limited and restricted by virtue of transparent, global and strict laws that allow their use only in specific cases. It should be controlled to avoid abuse of authority ("watching the watchmen").

In general, the debates in the tables showed a great awareness of the participants who, consistently across the groups called for broader and stricter laws related to the implementation of SOSTs. Whilst, many participants asked for severe punishment for the security agencies and the commercial actors who break the law, they also asked for a more thorough control over who, why and for what purposes, accesses their information. At the same time, they also asked for better and more extensive access to their own data, wherever they may be stored in order to increase control of their data and their own information. It was suggested to establish of a system, a net or a collection of campaigns aimed at providing this kind of information in a clear and simple way, so that we are able to identify whom to complain to, whom to address in the case of requests and, basically, being able to know how citizens could use this information, which belongs to them, at any given time (in a trial, facing a claim or an accusation, etc.). An equally interesting suggestion, again widely shared across the tables, was the adoption of a more focused, targeted and fine-grained surveillance. More than one discussion group suggested that surveillance should be adopted only towards those individuals that are reasonably considered dangerous and have criminal records or are likely to join cardinal groups and criminal activities. This is why the massive use of DPI against millions of citizens was thoroughly rejected and considered unacceptable under any circumstance.

One of the most pressing problems highlighted, however, was the wide variety of regulatory regimes vis-à-vis the extremely globalized fluxes of data across all the countries of the world. It was clearly understood that as long as each country adopt its own rules, it would be impossible to discipline security and data practices across the world. As a result, several participants suggested that, even though the goals of one country differ from those of another, some kind of arbitration should be implemented (similar to the United Nations system, that is, including representatives of every country) to avoid abuse of power by a country, for example the United States.

The attention of the participants, though, was not only directed at the regulatory framework. Another very interesting element of these debates was the emphasis given by several groups to a re-orientation of surveillance devices and practices. It was suggested to shift the focus of surveillance and observation from terrorism and petty criminality to fiscal frauds, tax havens and the multimillionaire flows of money and resources hidden behind the bank secret codes and the fiscal tricks and boxes used to avoid tax enforcement.

Additionally, the participants not only underlined the need for more educational and training campaigns aiming at informing and advising population on this kind of surveillance methods. They also argued that citizens, once informed, should have an option to avoid being under surveillance. For instance, one of the proposed solutions was to use computers and cell phones less frequently, as they constitute an excellent entry point for surveillance, that is, the source from which the information can be obtained. These information campaigns were expected to be set up and push forward by different institutions, such as politicians, companies and civil society associations. In some groups, it was even proposed to create a Monitoring Board, made up by members of a variety of political parties (from all across the political spectrum), companies and associations. The idea behind this specific composition was to have a body of independent members who did not owe their participation to their affiliation with the parties in power at any given time. The proposed members of this body were to include Judges, Lawyers, Scientists/IT specialists, Sociologists/philosophers and members of the lay public, too. In effect, there was a shared call for a greater protection against the political power. Generally speaking, private actors were not considered as acceptable institutions to be entrusted the responsibility of enacting security measures and/or operate security technologies, let alone monitor and control the "controllers". In contrast, it was

explicitly suggested by all the groups that only a public body, independent from political control, should enact these tasks and operation. In sum, while some participants advocated a stricter (public) control over the controllers, some others called for a stricter implementation of the existing Data Protection Act in order to prevent the feeling of insecurity and avoid a false sense of over control.

Finally, the causes and origins of crime, terrorism and insecurity were not neglected. Though effective they may be security technologies do not eradicate the ultimate causes of crime and violence. In order to eradicate crimes, for instance, social differences should be reduced. They did not accept, to give an example, that poorer and richer neighborhoods were monitored differently in terms of extension and depth of the surveillance, as they considered this a form of discrimination. Current security measures, for example, are only concerned about the security of European and American population, not about African people. Some participants found appalling that, under the current security regimes, the problems of people living in other countries, which often force them to try to enter our European borders undocumented, do not seem to matter at all.

These proposals have been summarized in the following list:

1. Worldwide common law: minimum limits for private data access (this is difficult to attain due to the different notions of privacy that exist and to the fact that some countries might not sign or comply with this legislation: the USA and countries in conflict or under dictatorship).
2. Training and information campaigns about every consequence derived from using the Web.
3. Access to our own stored data as well as the right to remove them or to revoke consent (right to rectify), e.g., being able to delete a picture we uploaded a long time ago.
4. Forbidding the sale of data by one company to another and imposing fines aimed at enforcing the law.
5. Tackling the causes of insecurity: investing in education and creating employment, which may become the main source of security.
6. Shifting the focus to the people in power: monitoring tax havens.
7. Not installing CCTV in parks or private areas.
8. Adapting legislation to the development of the SOST and their usage.
9. Ensure that security is organized and managed by the public sector (under no circumstances should it come from the private sector). It must be managed by the State and its public servants, who are highly qualified for this task, unlike the private sector workers, who act according to different criteria.
10. Generate opinion and participation channels that are later effectively taken into account.

5 Summary and Conclusions

The Spanish views on surveillance, security and privacy are generally similar to other countries in Southern and Central Europe. They are characterized by a generally benevolent attitude towards the implementation of new technologies but are also deeply influenced by a significant mistrust towards political authorities, which is partially due to the inheritance of their totalitarian and undemocratic past and partially to the high level of public corruption. The economic crisis has only worsened these general feelings and has extended them, like in a spill over effect, towards European institutions, too. The peculiarities of the Spanish context are, thus, more related first to its the security strategy, which has expanded security to a number of domains, such as energy, immigration and the economy, previously considered part of the traditional welfare policies. Second, they are also related to its privacy framework, which is articulated around the correct interaction and preservation of three specific rights: the right to intimacy, the right to data protection and the right to anonymity. Privacy in Spain is not so much an issue of protecting our private life, but rather an issue of having, at all times, the right to decide what to share and what to keep private.

The outcomes of the citizen summits reveal a number of interesting insights. First, the participants to the summit feel pretty secure in their daily life and consider that Spain is a safe place to live. While they support the introduction of SOSTs as a general measure to improve national security, they did not consider that these technologies actually improved their own individual security. Second, only about half of the participants actually adopted a trade-off approach and believed that security and privacy stood in a zero-sum game, however only a very small percentage of them was prepared to exchange privacy for security. Third, as expected, almost the totality of participants mistrust public authorities and security agencies and believe that security agencies do abuse their power when operating CCTVs and DPI. Fourth, smart CCTV systems are perceived in Spain differently depending on its private or public use. Citizens are more critical towards the private use of CCTV cameras, which are considered intrusive, while quite supportive of the use of cameras in public locations. The fundamental lack of transparency and information around DPI raises serious concerns among citizens, who consider this technology fundamentally unacceptable because it operates in spaces, virtual spaces, which are considered intimate. The 'algorithmic' components of both smart CCTV and DPI also worry participants. Fifth, participants consistently asked SOSTs to be regulated at European level to ensure fairness of treatment to all Europeans.

Finally, the participants did not neglect the social and economic causes of crime and violence and insisted that security technologies only address a specific aspect of security leaving these causes unattended. SOSTs, as they say, only make sense as part of a broader strategy that involve alternative security measures and also addresses the real causes of violence and crime. While they ask policy-makers to re-orient their efforts towards fiscal fraud, white-collar crimes, tax havens and multi-millionaire flows of money, they also ask for the implementation for a new regulatory regime based on a participatory framework. Citizens seem to be willing not only to contribute to bear the responsibility of the protection and preservation of their data, but they also want to collaborate in the design of public policies and new technologies and to participate actively in controlling infractions and abuses in the use of surveillance technologies. In other words, their view is that trust in public institutions and authorities cannot be taken fro granted at any point in time: it rather needs to be negotiated all the time, in relation to each technology, and maintained through the existence, and correct function, of clear rules, transparent information and effective participatory practices

6 Bibliography

Amitai Etzioni, 2012 “Los limites de la privacidad”, Edisofer, Madrid

Blanco Navarro, José Maria (2011): “Security and intelligence: 10 years after 11-S”. Working Paper, 7 September 2011, Strategy Investigation Spanish Institute

El Mundo (2012): Newspaper article from June 27, 2012.

EL Mundo (2012): Newspaper article from May 7, 2012.

El Mundo (2012): Newspaper article from March 12, 2012.

El Mundo (2010): Newspaper article from March 5, 2010.

El Mundo (2010): Newspaper article from January 17, 2010.

El Pais (2010): Newspaper article from June 3, 2010.

El Pais (2012): Newspaper article from July 26, 2012.

El Pais (2012): Newspaper article from July 11, 2012.

El Pais (2012): Newspaper article from 24 March 2012.

El Pais (2011): Newspaper article from Feb.16, 2011.

El Pais (2010) Newspaper article from July 30, 2010.

El Pais (2010): Newspaper article from June 19, 2010.

El Pais (2010): Newspaper article from January 9, 2010.

El País (2009): Newspaper article from 23 December 2009.

El Pais (2008): Newspaper article from September 18, 2008.

Encarnación, O.G. 2001. "Civil society and the consolidation of democracy in Spain." Political Science Quarterly 116(1):53-79.

Hempel, L., & Töpfer, E. (2004). Cctv in Europe: final report. Centre for Technology and Society, Technical University Berlin, Germany (August 2004).

López Roman y J. Mora, 2009, Un análisis de la estructura institucional de protección de datos en España, Indret, No. 2/2009, pp. 1-34. See also Cristina Gomez Piqueras, Spanish Data Protection Agency, presentación en power point accessible at: http://www.faisscv.es/4jornadasxativa/1conferenciacristina/confidencialidad.pdf .

Luján, J. L. y Todt O. (2000): "Perceptions, attitudes and ethical valuations: the ambivalence of the public image of biotechnology in Spain, Public Understanding of Science 9: pp. 383-392.

Luján López, J. L. (2007): "El principio de precaución y la imagen social de la ciencia", en Fundación Española para la Ciencia y la Tecnología (FECYT), Percepción Social de la Ciencia y la Tecnología en España 2006, pp. 65-80.

Menéndez, I. V. (2013). LA INTIMIDAD, ESE "TERRIBLE DERECHO" EN LA ERA DE LA CONFUSA PUBLICIDAD VIRTUAL. Espaço Jurídico: Journal of Law [EJJL], 14(3), 57-72.

Montero, J., Gunther, R., & Torcal, M. (1999). Legitimidad, descontento y desafección. Estudios Públicos, 74.Torres-Albero C. (2005): "Representaciones sociales de la ciencia y la tecnología", Reis, 111 (5):pp 9-43

Pavone, 2010. "Genetic testing, geneticization and social change: Insights from genetic experts in Spain" chapter 4 Assessing life: on the organization of genetic pp104-132.

Pavone, V., Osuna, C., & Degli Esposti, S. (2010). Invertir en ciencia y tecnología en tiempos de austeridad económica:¿ Qué opinan los ciudadanos?. FECYT (2011) Percepción Social de la Ciencia y la Tecnología, 115-136

Pavone, V. and S. Degli Esposti (2012) "Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security " Public Understanding of Science 21(July): 556-572.

PRISE Spanish National Report, 2008.

Publico (2008): Newspaper article from 21 October 2008.

Sanquist, T. F., Mahy, H., & Morris, F. (2008). An exploratory risk perception study of attitudes toward homeland security systems. Risk analysis, 28(4), 1125-1133.

Sanz-Menéndez, L., Muñoz, E., & García, C. E. (1993). The vicissitudes of Spanish science and technology policy: coordination and leadership. Science and Public Policy, 20(6), 370-380.

Sanz Menéndez, L., & Cruz Castro, L. (2010). Análisis sobre ciencia e innovación en España.Siegrist, M y Cvetkovich G. (2000): "Perception of Hazards:The Role of Social Trust and Knowledge", Risk Analysis 20: pp. 713-720.

Slovic P., Fischhoff B. and Liechtenstein S. (1986) "The psychometric study of risk perceptions" en Covello V.T., Menkes J and Mumpower J. (eds.) Risk evaluation and management. New York, London, Plenum Press, pp. 3-24.

Tálos, E. and Kittel, B., 2002, Austria in the 1990s: The Routine of Social Partnership in Question?, in: Berger, S. and Compston, H. (Eds): Policy Concertation and Social Partnership in Western Europe. Lessons for the 21st Century, New York, Oxford: Berghahn Books, 35-50.

Tello Diaz, Lucía. 2013. "Intimacy and «Extimacy» in Social Net-works. Ethical Boundaries of Facebook." Comunicar, Vol. 21, 205-213.

The Spanish Constitution. Lamoncloa.gob.es.

Torcal, Mariano and José Ramón Montero. 1999. "Facets of Social Capital in New Democracies: the Formation and Consequences of Social Capital in Spain," in Paul Whiteley and Kenneth Newton, eds., Social Capital in European Democracy. London: Routledge.

7 List of Figures

8 List of Tables

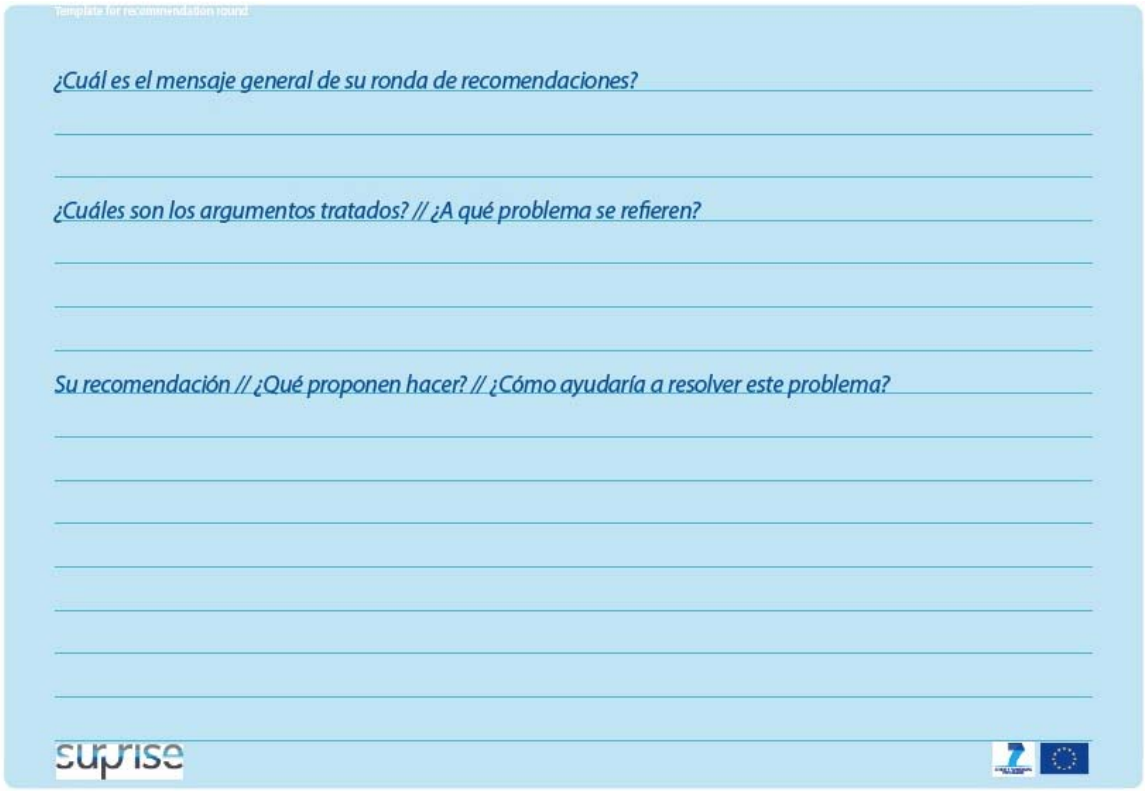
9 List of Abbreviations

Abbreviation	Definition
AEPD	Agencia Española de Protección de Datos (“Data Protection Agency”)
BBVA	Banco Bilbao Vizcaya Argentaria
CCTV	Closed circuit television
CICO	Centro de Inteligencia Contra el Crimen Organizado (“Centre for Intelligence against Organised Crime”)
CNCA	Centro Nacional de Coordinación Antiterrorista (“National Anti-terrorist Co-ordination Centre”)
CNI	Centro Nacional de Inteligencia (“National Intelligence Center”)
DPI	Deep Packet Inspection
EC	European Commission
ETA	Euskadi Ta Askatasuna ("Basque Homeland and Freedom")
EU	European Union
FECYT	Fundación Española para la Ciencia y la Tecnología (“The Spanish Foundation for Science and Technology”)
GDP	Gross domestic product
NATO	North Atlantic Treaty Organization
OECD	Organisation for Economic Co-operation and Development
PRISE	EU Project (“Privacy enhancing shaping of security research and technology”)
SOST	Surveillance-oriented security technology
TSJC	Tribunal Superior de Justícia de Catalunya (“High Court of Justice of Catalonia”)
UN	United Nations
WTO	World Trade Organization

10 Annex

10.1 Table recommendations produced at discussion groups

Template[49]



Recommendations – content[50]

What is the core statement of the table's recommendation?	What is the background of the recommendation? What is the problem?	The recommendation in detail/ What should be done/ how to address the problem?
Participants in table 1 agreed that new technologies improve security to some extent, but they stated that their usage should be restricted in order to make them less intrusive.	Regarding DPI (or "Deep Package Inspection"), participants believed that it should only be used to monitor specific individuals who have previously committed a crime and after having obtained a court warrant. CCTV should be restricted to public spaces.	The use of these technologies should be limited and restricted by virtue of transparent, global and strict laws that allow their use only in specific cases. It should be controlled to avoid abuse of authority ("watching the watchmen").
Greater awareness, broader and, particularly, stricter laws on this issue. Severe penalties for those who break the law. Thorough control over access	Education and training campaigns aiming at informing and advising population on this kind of surveillance methods, as well as ways avoiding being	It is proposed to create a Monitoring Board, made up by members of a variety of political parties (from all across the political spectrum),

[49] This recommendation sheet was filled in by each table. The translation of the template's questions, as well as the translations of the submitted recommendations, can be found bellow.

[50] Translated from Spanish

to information. Focusing surveillance.	under surveillance. One of the proposed solutions both at this point and throughout the debate is to use computers and cell phones less, as they are considered to be overused and they are the focal point for surveillance, that is, the source from which the information can be obtained. These campaigns must come from different institutions: at the very least, politicians, companies and associations.	companies and associations. (The participation of companies still casts some doubts, but in general there is consensus.) This idea intends for this commission to not be elected at the convenience of the people who are in power at any given time.
About the CCTV. We agree on their use only and exclusively for public safety purposes. About the DPI. Only for public safety purposes, without personal intrusiveness.	About the CCTV. Need for information about location, goal, subsequent conditions (duration) and owners (bodies) of the recorded images. About the DPI. Need for information about the time when it is conducted, purpose and information processing. Emphasis is placed on rejecting the commercial use of the data.	As for the CCTV. Unambiguous legislation on its usage, informing the citizens concerned of its objective. By means of a court warrant, access to the recorded images by citizens affected by a crime. For the DPI: Worldwide, unified legislation on the processing and possession of these data. An independent body must be in charge of this task. The fundamental idea is that the Internet is free and some contents are not subject to regulation, so that there is no need of implementing these control methods. It is about tackling the root of the problem.
1) They feel comfortable with the SOST (Surveillance-Oriented Security Technologies). They don't think they are intrusive and they feel safer. 2) They think that we do not control when and by whom are we monitored.	In relation to the previously mentioned positions: 1) Arresting someone can justify the massive use of these technologies. 2) The SOST give rise to more insecurity and they affect the presumption of innocence.	1. Worldwide common law: minimum limits for private data access (this is difficult to attain due to the different notions of privacy that exist and to the fact that some countries might not sign or comply with this legislation: the USA and countries in conflict or under dictatorship). 2. Training and information campaigns about every consequence derived from using the Web. 3. Access to our own stored data as well as the right to remove them or to revoke consent (right to rectify), e.g., being able to delete a picture

		we uploaded a long time ago. 4. Forbidding the sale of data by one company to another and imposing fines aimed at enforcing the law. 5. Tackling the causes of insecurity: investing in education and creating employment, which may become the main source of security. 6. Shifting the focus to the people in power: monitoring tax havens. 7. Not installing CCTV in parks or private areas. 8. Adapting legislation to the development of the SOST and their usage.
Freedom of expression, right to privacy... If we lose that, it will be as if they broke down the door and got into one's home.	We know the benefits of both methods. Uncertainty lies in the fact that we are ignorant of which data are collected, who gathers them and how they are managed. The solution is a specific legislation on new technologies and surveillance. The establishment of a body controlling the use of the data and its processing. Mechanisms that enable us to decide whether we want them to go public. Being able to decide for myself if I want advertisements to pop up or not.	Creating a European law.
Use of new technologies with specific purposes (terrorism, paedophilia...), but not to invade and manipulate the average citizen.	Access is granted to all data. In some cases, there are no limits to spy, there is no transparency (it is not revealed what and who it is for), and it can be used for commercial purposes. Reference is made to privacy invasion and manipulation.	Recommendations: Worldwide legislation enabling transparency and information for citizens. How - Even though the goals of one country differ from those of another, some kind of arbitration should be implemented (similar to the United Nations system, that is, including representatives of every country) to avoid abuse of power by a country, for example the United States.
Promote policies on public participation and legislation on this issue.	"Citizens need to feel protected and still be informed in order to safeguard their privacy."	"To create a legislation and a competent body to protect us, informing citizens and

		companies or entities with full transparency and proposing as an alternative the reinforcement of policies on public affairs education."
Legislate at an international level so that complying with the law is mandatory for every state.	To protect citizens against potential abuses and misuses; For the usage of these technologies to be safer; To prevent the private sector from using them with commercial purposes;	Establishment (either at a local or national level) of a technological ombudsman, as a body similar to the current ombudsman.
We want to know with full transparency who the natural people using our data are.	The Data Protection Act is not complied with, since no matter what we do, we always receive advertisements from other companies, which means that our data are being sold.	Worldwide legislation, not only for some countries; improve the data legal framework; transparency and knowledge about who is in control; training in using the Web properly; teaching kids how to use the Internet adequately; control mechanisms applied to controllers; being more aware of how and to what purpose our information is being used; events, debates about this subject; disposal of data that are unimportant for public safety; not justifying the gathering of information for selling it to companies in a future;
Unified legislations, both at a global and EU level.	Furthermore, technology progresses at a fast pace and legislation always lags behind it.	Enforcing actual protection of citizen's data must close enforcement loopholes.
Less intrusive, more regulated, less invasive.	Uselessness for control and security improvement. Unfulfilment of the crime.	Increasing human presence instead of IT presence. -A greater control of technology.
The general message is closely linked to the need for an agreed and common legislation on surfing the Internet. That must imply a greater engagement of the governments and a strict and fast judiciary.	The main issues dealt within the group have to do with security, in relation with both surfing the Internet and with monitoring citizens. A lack of transparency is felt regarding the practices of both security agencies and information gathering companies.	In specific terms, it is advised to enact agreed and common legislation, at a national, European and global scale, on the security of Internet surfing. This legislation must specify who monitors citizens and how it is done. This will allow transparency and accountability. In order to be independent, it must be agreed upon by all parties and left out of any political conflict.

Citizens need greater transparency and explanations about who is going to manipulate their information and why.	There is much uncertainty about who is using our data, in which way and to what purposes. Citizens must express consent regarding the use of their personal data even in the cases when these are apparently uninteresting.	More specific legislation about the usage and limits of technology.
There is a lack of transparency and information about what happens to our data.	Regarding the use of social networks, there is a general fear of being tricked or making mistakes that can have a negative impact on us.	1. Information campaigns in order to inform citizens about what the use of Internet entails. 2. Possibility of extracting, deleting, etc. for good any record of the uploaded pictures, posted comments, etc. in social networks, so that, apart from being removed from the network in question, they are not recorded in any database.
Not to violate privacy for the sake of security.	We are not aware of the way our data are processed, who uses them and to what purpose. Fraudulent use of information. Intrusion into personal privacy.	Tightening of penalties for fraudulent use of the obtained information via CCTV and DPI.
There is not much information about surveillance technologies in general.	The main problem is the lack of awareness about control systems, processing of the data obtained through surveillance technologies, control of people in charge of gathering information, procedures that allow citizens to have access to those data at any given time, etc.	Establishment of a system, a net or a collection of campaigns aimed at providing this kind of information in a clear and simple way, so that we are able to identify whom to complain to, whom to address in the case of requests and, basically, being able to know how citizens could use this information, which belongs to them, at any given time (in a trial, facing a claim or an accusation, etc.).
Surveillance technologies are very intrusive, so their use should be forbidden except for duly justified exceptional cases.	Surveillance technologies take us all as suspects and violate everyone's privacy. In spite of the fact that they are useful to prevent certain crimes, their usage must be restricted and regulated.	Everybody must be able to have free access to the information stored about them on the Internet, as well as the images recorded where they are present. Having some decision-making capacity regarding that information. Forbidding commercial usages of that information. Regulating the periodic deletion of camera recordings and Internet information (such as the search and browsing

		history).

There is a lack of information about the general use of these technologies, as well as a lack of regulation aimed at protecting individuals against fraudulent and commercial uses.	No permission is asked when cameras are installed. It is not stated properly who they are for, how they are registered, how long they are staying or who is going to watch them. We are unaware of the fact that there is a data processor. Furthermore, there are not any warnings on the Internet that we are being monitored, or about what it is happening. It is also said that technologies must not substitute human work. Activities carried out on the spot by natural people have to be prioritized.	Establishing control mechanisms for those in charge of surveillance. Greater transparency, identification of watchers. Equal surveillance. In wealthy and poor neighborhoods. Monitoring people in power. Regulation should be international.
Citizens have to have access to information about legislation, to know if it is complied with, etc. Transparency in methods and results.	We are unaware of what monitoring institutions and companies do, whether the actions they take have any effects, if they fulfil the goals they set and if they justify why they have been created.	Training for personnel using the SOST; maintaining the human factor, that is to say, not replacing humans for robots in processes and their uses. It should be a comprehensive training: not only on technical aspects, but also on ethic values regarding surveillance and security. The State should act under public safety criteria, rather than productivity or profitability criteria oriented to companies and with commercial purposes. Transparency in all processes and legislation. Granting access to information on what is done, to what purposes and who is in control.
It is useful for the safety of citizens as long as it does not interfere with the lives of innocent people. In case there is any interference, we must be informed about it, and if any crime has been committed, they must act in full transparency.	1. Arguments in favour of the use of these means: prevention and condemn of criminal acts. 2. Disadvantages: misuse, economic expenditure, violation of rights and privacy.	1. Non-technological alternatives: a greater use of security personnel and animals. 2. Standing up for our right to privacy.
Need to provide citizens with clear, concise and free of deception data about the actual usage of these tools.	The basis of the issue is the loss of freedom. Problems are not solved by means of these tools. Ignorance heightens the	In order to eradicate crimes, social differences should be reduced. If it is really about security, they are only

Transparency, so that these technologies entail security rather than control.	conflict, as it is unknown what lies behind this surveillance. What difference do cameras make?	concerned about European and American population, not about Africa, for example. The problems of people living in other countries do not seem to matter.
Actually chasing hackers and intrusive companies; limiting legislation.	Establish legal boundaries and citizen protection rules. It is not reasonable to make hasty assumptions on behalf of fear and security and believe that everyone is a criminal until proven not guilty.	A greater protection of the citizens against the power. Actual implementation of the Data Protection Act in order to prevent insecurity and overcontrol.
Need to create a data protection regulatory body (similar to a Ministry) at a national and EU level.	So that control, transparency, knowledge of usages, information and worldwide legislation can exist.	A new power not linked to the political sector or any ideology regulating data protection: - Strict action protocol regarding DPI and smart CCTV or any other surveillance mechanisms. - Direct and up-to-date information for citizens about available data, how they are available and whether they have been used or not. - Entering into agreements with other international bodies. - Adopting legal penalties to ensure law enforcement. - Members of this body: o Judges o Lawyers o Scientists/IT specialists o Sociologists/philosophers o Popular assembly
Security, both surveillance and cyber surveillance must be exercised in a responsible and transparent way, and it must only be active under State and public control. To that purpose, popular opinion and participation must be taken into account, with the adoption of a clear, transparent and fast legislation.	The group is willing to renounce part of their privacy in exchange for security as long as democracy (only the State and relevant Government officers are entitled to undertake security measures) and respect for human rights are kept.	1. Ensure that security is organized and managed by the public sector (under no circumstances should it come from the private sector). It must be managed by the State and its public servants, who are highly qualified for this task, unlike the private sector workers, who act according to different criteria. 2. Generate opinion and participation channels that are taken into account.

10.2 Postcards

Template

Postcards - content[51]

What I would like to add…to the European politicians
Technology changes, but ethics remain the same. Laws must also protect us individually on the Internet. Web control must be subject to international regulation. Technology gives and demands at the same time.
The control system must be transparent, and whoever uses, discloses or modifies the information must be monitored.
At a national level, there is a much greater concern about how public money is managed than about public safety. The security issues that we are exposed to are directly linked with political and welfare matters: surveillance technologies should be focused on those who run our country and manage our money.
3-year-old children are being monitored through their iPads, think about it!
The people responsible for the DPI belong to the elites to whom nothing ever happens. They create the webs, they are safeguarded.
As for DPI, I believe that the developers of such analysis are capable of setting the boundaries. If such thorough analysis is performed inside the so-called "Deep Web", that is fine for me. I think that there

[51] Translated from Spanish

should not be such a deep analysis when it comes to our personal Internet surfing or physical movement: whoever wants to commit a crime will do it in the dark side of the Web. The average user should be protected not only regarding crimes, but also against commercial uses that violate our privacy.
Corrupt politicians must be investigated.
I propose to improve the legal framework that protects us when it comes to the misuse of our data by any institution.
I would kindly request that the Spanish Official State Gazette is removed from the Internet, as it contains sensitive information.
CCTV should always be controlled by people rather than by a software.
There is a global lack of information, clarity and regulation on these practices about surveillance and interference in the individual's privacy. The interest in knowing and providing information about these practices should be encouraged.
The usage of CCTV should be confined to security forces of each country so as to investigate and solve criminal offences. They should never be used in mass media, especially without the consent of the concerned individuals.
Security does not justify interference in people's lives. Laws must protect citizens.
Whoever trades data protected under the Data Protection Act should be pursued and more severely punished.
Until there is not a DPI control, it should be forbidden.
The DPI should only be applied to individuals who have previously committed a crime.
CCTV installation in neighbourhoods should be done with the residents' consent.
If we citizens do not trust those who run our country, we do not trust technological watchers either.
Technology must under no circumstances substitute humans. It has to be a support, but not an end.
Monitoring and protection of personal data must be conducted by public bodies. Outsourcing such services to the private sector should never be an option.
The legislation on SOSTs must be agreed at an international level.
What is important regarding the use of technology is changing education. Technology is part of our lives and we cannot avoid it, but we can actually prevent ignorance. Knowledge is power.
Surveillance technologies should never be used for commercial purposes.
Further information about regulations, laws, control procedures and bodies before which we could lodge a claim.
A greater investment against poverty and inequality must be made. No doubt this would prevent a lot of insecurity problems.