*"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 6.5 - Citizen Summits on Privacy, Security and Surveillance: Country report Italy

Lead Beneficiary: EUI

Author(s): Maria Grazia Porcedda (EUI) and Melissa Zorzi (EUI)

Due Date: June 2014

Submission Date: October 2014

Dissemination Level: Public

Version: 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 ..... i
1 Introduction ..... 1
2 Privacy, security and surveillance in Italy ..... 2
2.1 Political profile of Italy ..... 2
2.2 "Security" " in Italy: concepts, actors, laws and policies ..... 3
2.2.1 Preventive policing and lack of transparency ..... 4
2.2.2 Policy documents and strategies ..... 7
2.3 "Privacy" in Italy: the law and the DPA (Garante) ..... 9
2.4 SOSTs in Italy: usage and public discourse ..... 10
3 The design of the Italian citizen summit ..... 14
3.1 The summit ..... 14
3.2 Recruiting citizens ..... 15
3.3 The 193 participants of the summit ..... 16
3.4 How participants assessed the Italian summit ..... 18
4 Empirical results of the citizen summit ..... 20
4.1 General attitudes on security and privacy ..... 20
4.2 How do participants perceive the use of SOSTs? ..... 23
4.2.1 Familiarity with DPI and SLT ..... 23
4.2.2 Perceived effectiveness ..... 24
4.2.3 Perceived intrusiveness ..... 25
4.2.4 Trading privacy with security (with reference to DPI and SLT) ..... 28
4.3 Is fighting or fleeing surveillance an option? ..... 31
4.4 Italian citizens accept SOSTs (in general), but worry about privacy and future developments ..... 32
4.4.1 Participants worry about future developments … ..... 34
4.4.2 … and about privacy as a right valuable for the collectivity ..... 34
4.5 Trust in security authorities and regulation: an important explanatory factor ..... 36
4.6 Role of alternative security approaches ..... 39
4.7 Citizens' recommendations to policy makers ..... 39
4.7.1 Short commentary on the recommendations ..... 40
4.7.2 Limitations of the summit ..... 41
5 Summary and Conclusions ..... 42
6 Bibliography ..... 44
7 List of Figures ..... 49
8 List of Tables ..... 50
9 List of Abbreviations ..... 51
10 Annex ..... 52
10.1 Table recommendations ..... 52
10.2 Postcards ..... 63

# 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.

This document reports the results of the Italian citizen summit, held in Florence on February 8th, 2014. The summit lay at the heart of SurPRISE and served multiple purposes. First, it aimed to collect empirical evidence on factors influencing citizens' acceptance, and acceptability, of security measures, and citizens' assessment of the role of trade-offs in their judgment concerning security and privacy. Second, it invited citizens to take an active part in the decision-making process. The summits featured the discussion of surveillance-oriented security technologies (SOSTs) to allow citizens to express their attitudes on surveillance technologies, security and privacy in context, making reference to real-life situations.

The one-day Italian summit featured 193 citizens (for the demographic distribution, see Section 3) who sat at 35 well-assorted tables, each facilitated by a moderator. Participants gathered to discuss security, privacy and surveillance issues, to answer a set of questions on Deep Packet Inspection (DPI) and Smartphone Location Tracking (SLT), and to formulate recommendations for European and national policy makers (full text translated into English is reported in the Annex 10.1).

The questionnaire data, and qualitative data gathered during table discussions, which complement each other (as shown in section 4), must be read in the light of the country profile (discussed in section 2) and other statistics available, as mentioned in the text.

*The level of security threats is high* (more details in section 4.1)

- Less than half of the respondents considered Italy a safe place to live and stated they feel secure in their daily life (the lowest rate among the citizen summits conducted in Europe).
- 38% of respondents "neither agreed nor disagreed" with the statement "I generally feel secure in my daily life" (the highest value of undecided respondents compared with all other countries).
- Citizens feel they have a greater degree of control over personal rather than national security.

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

*In Italy citizens worry (and care) about privacy* (more details in section 4.1, 4.3 and 4.6)

- A clear majority of participants perceives that SOSTs have a negative impact on their personal privacy, and that an increasing use of them leads to an erosion of citizens' privacy in general.
- Disclosing personal information is seen as an increasing part of modern life, but the majority of participants stated that they would like to find out more about how to protect their personal data against the uses linked to both DPI (60%) and SLT (62%).
- Two thirds of people who casted their vote would also favour the adoption of alternative approaches that do not require the use of SOSTs.

*SOSTs: useful but dangerous*

(more details in section 4.2 and 4.4)

- Both technologies are considered useful for security rather than useless, and SLT is considered more useful than DPI (76.9% of respondents considered DPI overall useful compared with 91.9% for SLT).
- The majority of participants agreed with the use of DPI (55%) and SLT (70%) as a security measure.
- The vast majority of participants expressed unease and disagreement with the use of data collected from SOSTS for commercial purposes.
- For the majority of respondents, DPI and SLT are harmful for **privacy**, whether they are used for security or commercial purposes, in spite of the benefits that they can bring.

*Trading privacy for security is not an option*

(more details in section 4.2.4)

- Only 37% of respondents appear to accept the fact that the technology comes with a cost to privacy in the case of DPI, and 38% would do the same in case of SLT.

These results may suggest that one third of participants are ready to trade privacy with security. However, it may equally be that participants do not feel they have a real choice in the matter, but must adapt to privacy intrusions decided by others in the name of security and, as a consequence, are not even in a position to decide whether they would accept the trade-off.

*Trust in institutions is low*

(more details in section 4.5)

- Respondents favour the general use of SOSTs by governments if available, as they believe they can improve national security by targeting criminals.
- Acceptance is overshadowed by doubts and scepticism, due to the fear of abuses of power, the uncertainty about the real effectiveness of SOSTs in countering security challenges, and the cautious approach to the "I have nothing to hide" attitude.
- 40.6% of participants agreed or strongly agreed with the statement "**I believe the citizen summit has generated valuable knowledge for the politicians**", 10 percentage points lower than the European average.

*Table recommendations*

Table recommendations clustered around the following themes: regulation, transparency, awareness, legal protection, privacy by design and alternatives. Many participants asked reassurance that recommendations would be delivered (more details in section 4.7).

### *Pros of the summit*

(more details in section 3.4)

- Almost all strongly agreed to have gained new insight by participating in the citizen summit.
- At the end of the summit, the percentage of participants declaring to "know little to nothing" decreased to 9.1%, and the percentage of participants declaring "I have some knowledge of SOSTs but it would be useful to learn more" increased to 59.1%.
- Many citizens expressed the feeling that participatory events such as the citizen summit represent an important step towards increasing awareness and involving citizens
- Ingraining participation in the process of decision-making, for instance in the form of participatory events assessing different legally protected interests, could be a substantive way to conform to the rule of law, the right to good administration and, in the present case, avoid costly political decisions that have no support among the public.

### *Cons of the summit*

(more details in section 4.7.2)

When reading the results of the summit, it is important to keep in mind the following elements. First, while broadly representative of the diversity within modern Italian society, the sample was nonetheless of geographically limited scope. Second, table discussions were not recorded. Third, the summit was a one-off event, and therefore participants' contributions (and perceptions) cannot be assessed over time.

### *Next steps*

The European comparative report, summarizing the results of the twelve citizen summits, will be published in Autumn 2014.

The summit provided important insight into citizens' approach to surveillance, privacy and security in Italy, but left some questions unanswered. These and other questions informed the organization of a focus group to investigate in greater details citizens' thinking and preferences, held in Florence on June 17$^{th}$. The report for this event will also be released in Autum.

# 1 Introduction

This document[2] reports the results of the Italian citizen summit, held in Florence on February 8th, 2014[3]. The citizen summits lie at the heart of SurPRISE, a project consisting of large-scale participatory assessments of criteria determining acceptability and acceptance of security technologies, and of the costs they (might) impose on privacy.

This report begins with background information on the troubled relation between privacy and security issues in Italy, providing context to the empirical data collected from citizens. It approaches it from a historical perspective, taking into account Italy's democratic evolution against the background of the waxing and waning of the Cold War.

Chapter 3 provides detailed information on the design of the Italian large-scale participatory event. It is written to be accessible to experts in participatory methods and others alike. While it is not necessary for understanding the results, it helps framing the scope of the results.

The empirical results of the Italian summit are presented in chapter 4, which constitutes the most important chapter of this document. There, we present the Italian data interpreted through the lenses of the qualitative analysis derived from small-group discussions (taking place at 35 tables). Data are also enriched by comparison with the results from other summits; note, however, that the comparative results will be the subject of a separate report. When relevant, we compared the results of the summit with those of similar existing studies. In each section we have stressed in boldface the most significant statements and outcomes. Chapter 4 ends with the main messages of the table recommendations.

We report all significant information in the conclusions, where we piece them together in a coherent fashion. The summits have provided groundbreaking insights into citizens' approaches to privacy and security, but they have also left some questions unanswered. We highlight such open issues, and clarify how the project is addressing them.

The full table recommendations and individual postcards (translated into English) are reported in the Annexes at the end of this document.

[2] We wish to thank Professor Martin Scheinin (EUI), Stefan Strauss (ITA), Martyn Egan (EUI) and Professor Giampiero Giacomello (Università di Bologna) for their thorough review and comments.

[3] Our sincere thanks to all that contributed to the success of the Italian citizens' summit. Serena Bürgisser, (Vice Director, EUI Communications Service), Giulia Serafini and Michele Massacesi for their media support and constant encouragement; Jonathan Andrew (team SURVEILLE), Claudia De Concini (team SURVEILLE/SurPRISE), Martyn Egan and Matteo Rocchi for logistics, troubleshooting and invaluable moral and practical support; Paolo Martinez (FUTOUR) for his brilliant head facilitation; Florence City Council's member Prof. Cristina Giachi for her warm welcome speech and institutional presence; Regione Toscana, Provincia di Firenze, Comune di Firenze, Forum Italiano per la Sicurezza Urbana, Garante per la protezione dei dati personali e Rappresentanza in Italia della Commissione Europea for their moral sponsorship; Professor Lewanski (Università di Bolgona), dott. Floridia, dott. Marcotulli, dott.ssa Barlacchi and dott. Siliani (Regione Toscana) for precious advice on participatory events; ReteSviluppo s.c. and Baglioni e Poponcini for sampling and the recruitment of participants; great table moderation and note-taking: Ginevra Avalle, Fabio Baglioni, Francesca Bonechi, Sandro Buggiani, Nicolò Caciotti, Francesca Casini, Luca Caterino, Lorenzo Cecchi, Lapo Cecconi, Riccardo Emilio Chesta, Carmelo Chianura, Giulia Ciampi, Paola Cimbolli, Céline Colombo, Federica Coppola, Marco Algimiro Fusaro, Stefania Gatti, Katia Giannone, Dario Miccoli, Valentina Miola, Sofie Christine Møller, Davide Morisi, Eleonora Moscardi, Vanna Mugnaini, Alfredo Panerai, Fausto Petrini, Silvia Poponcini, Francesco Ranghiasci, Laura Remaschi, Francesco Renzetti, Emanuele Rigutto, Filippo Salvucci, Marco Scarselli, Grazia Sciacchitano, Veronica Spada, Annalisa Suman, Teresa Talò, Gloria Vitaioli, Antonio Volino and Alberto Zinanni.

# 2 Privacy, security and surveillance in Italy

Italy's approach to security, privacy and surveillance must be explained in the light of the country's political and institutional evolution, tied to its place in the evolving international landscape and its enduring internal challenges. This chapter provides an overview of the concepts, laws and practices of privacy, security and surveillance in Italy, and serves as background for the presentation of results.

## 2.1 Political profile of Italy

The current Italian State is the result of historical developments beginning with Italian reunification and independence at the end of the XIX$^{th}$ century. Proclaimed in 1861, the Kingdom of Italy was, according to the *Statuto Albertino* (its constitution), a "parliamentary constitutional monarchy". Suffrage was slowly extended from the rich and educated to the whole male population in 1913, but universal suffrage was introduced in 1946 only. The liberal and democratic evolution of the Italian State was brought to a brisk halt by fascism in 1922. In 1943 the fascist dictatorship was brought to an end, but it was only after the complete liberation of Italy from occupation forces in 1944, that the king and anti-fascist parties formed a transitional government.

Following a referendum in 1946, Italy became a Republic. At the same time, the Constituent Assembly started working on the current Constitution, which entered into force in 1948 and gave birth to a parliamentary republic. The main actors of the post-1948 Italian political system are the President of the Republic, the Parliament elected by universal adult suffrage (composed of the Chamber of Deputies and the Senate), and the Government (President of the Council and ministers). Governments are sworn in, and remain in office, after a confidence vote of both houses of Parliament.

From 1948 to 1992, members of the Chamber of Deputies and of the Senate were elected through proportional systems. This period was characterized by short-lived coalition governments. The electoral system was replaced in 1993 with a relatively majoritarian one[4]. In 1992 – 1993 a grand corruption scandal, known as tangentopoli ("bribesville"), broke out, leading to a major change in the composition of the Italian party system. From the elections of 1994 the trend has been an alternation between center-right and center-left governments, but governmental stability has remained weak. In late 2005 the government in charge changed the electoral law re-introducing proportional representation with a majority prize for elections to the Senate and the Chamber of Deputies.

Falling governments and the impossibility to form governments capable of gaining the support of a parliamentary majority have also caused the President of the Republic to promote transitional governments of technocrats, such as in 2011. The latest elections, held in February 2013, gave birth to a coalition government, which was reshuffled in February 2014. Italians have witnessed short-lived governments, non-elected governments, reshuffled governments, and new corruption scandals almost on a daily basis. A recent ruling by the Constitutional Court declared the current electoral law unconstitutional.[5] In spite of governmental instability, the post-1948 era has been for Italy a period of economic growth and development, although the economic crisis has hit Italy severely.[6]

Today's Italy, with its 59.7 million inhabitants, is the fourth most populated country in the European Union. Local government is four-tiered, and comprise 20 regions[7] (15 regular regions and 5 special regions), provinces (to be abolished[8]), municipalities, which are highly heterogeneous, and Metropolitan

---

4 Richard S. Katz, 'Reforming the Italian Electoral Law, 1993', in Matthew Soberg Shugart and Martin P. Wattenberg (eds.), *Mixed-Member Electoral Systems: The Best of Both Worlds?* (Oxford: Oxford University Press, 2003)..

5 Sentenza 1/2014, n. 144/2013, G. U. 15/01/2014, Corte Costituzionale della Repubblica Italiana, 4 December 2013. Available at: http://www.cortecostituzionale.it/actionSchedaPronuncia.do?anno=2014&numero=1

6 Andrew Walker, 'Italy's Economy: The Mountain Matteo Renzi Must Climb', *BBC News,* 25 February 2014 2014. Available at: http://www.bbc.com/news/business-26266118.

7 Forming four macro-regions, which are the North West, the North East, the Centre and the South, also known as Mezzogiorno.

8 Roberto Landucci, 'Italy's Renzi Wins Confidence Vote on Cutting Local Government', *Reuters,* 26 March 2014 2014.

Cities. Statutes, powers and functions of these autonomous bodies are regulated by Section V of the Constitution, which was revised in 2001.

## 2.2 "Security" " in Italy: concepts, actors, laws and policies

Having outlined the main political traits of Italy, we can introduce the concept of security, the laws overseeing its protection, and the actors involved in it.

Internal security is founded on the notions of public order and public security,[9] interpreted by the Constitutional Court in its material sense[10] as "the protection of the fundamental juridical goods and primary public interests underpinning a civil living together".[11] 'Fundamental juridical goods' are "the physical and psychical integrity of people, the safety of possessions and other goods having primary importance for the very existence of the system"[12], whereas 'primary public interests' "do not encompass all public interests overseen by the branches of the public administration, but only those interests that are essential for the safeguard of an orderly living together" of the citizens.[13]

Intrusive actions and encroachments upon civil liberties and the private sphere of individuals for the pursuit of public order are limited by the Constitution, inspired by the need to reject and prevent the repetition of fascism. Yet, the legacy of fascism permeates the approach to public order and security.[14] Vis-à-vis the failure of the Parliament to declare null and void the fascist substantive law code (*Codice Rocco*) and the public security laws (*TULPS*),[15] also in relation to the permanence of employees of the fascist regime within the security forces,[16] the foundations of Italian criminal law lie in the two instruments.

Invalidated and reinterpreted by several judgements of the Constitutional Court that moulded them into the democratic order,[17] the Parliament also amended the two instruments respectively with *Novella* of 1974 (d.l. 11 apr. 1974 n. 9) and "*depenalizzazione*" (l. 24 nov. 1981 n. 689), as well as the Law of April 1st, 1981 n. 121[18]. The latter is commonly regarded as the point of rupture[19] that started the de-militarization of the police forces in Italy[20]. Criminal procedural law, too, was only reformed in 1988 with the introduction of an adversarial system based on the equality of plaintiff and defendant in the

---

9 Art. 159, co. 2, d.lgs. 31.3.1998, n. 112 (available at: http://www.parlamento.it/parlam/leggi/deleghe/98112dl.htm).

10 Under the Kingdom of Italy public order was understood as the precondition for the enjoyment of civil liberties, but also an inherent limit to all civil liberties. Giuseppe Campesi, *Genealogia Della Pubblica Sicurezza. Teoria E Storia Del Moderno Dispositivo Poliziesco*, (2009).

11 Translation of the authors. Sentenza N. 290, n. 290, Corte Costituzionale, 12 July 2001.

12 Translation of the authors. Ibid.

13 Translation of the authors. Ibid.

14 The concept was elaborated during fascism, in particular through the Penal Code (Codice Rocco) and TULPS, pursuant to which the emerging need to impose legal limitations on the encroachment of civil liberties and the private sphere of the 'subject' by the police was interpreted with wide discretion. Campesi (2009). On the subject, see also Ansoino Andreassi, 'Dalla Polizia Politica Alla Polizia Di Sicurezza - Un'evoluzione Complessa', Polizia Moderna, supplement to n. 2:2000). http://www.interno.gov.it/mininterno/export/sites/default/it/sezioni/ministero/dipartimenti/dip_pubblica_sicurezza/direzione_centrale_della_polizia_di_prevenzione/ (last accessed on 26 August 2014).

15 Testo Unico delle Leggi di Pubblica Sicurezza or consolidated text on the rules of public security, adopted with royal decree n. 773 on June 18th, 1931.

16 This was facilitated by the Cold War. Andreassi, (2000).

17 Donatella Della Porta and Herbert Reiter, *Polizia E Protesta. L'ordine Pubblico Dalla Liberazione Ai "No Global"*, (2003).

18 Nuovo Ordinamento Dell'amministrazione Della Pubblica Sicurezza, Legge n. 121 del 1 Aprile 1981 p.

19 The reform was spurred by concerns internal to the police. Della Porta and Reiter (2003).

20 Nicola Labanca, 'Studiare Le Polizie Italiane Dall'unità Ad Oggi, Dopo La Smilitarizzazione Della Polizia (1981-2011)', in Raffaele Camposano (ed.), *Poliziotti D'italia Tra Cronaca E Storia Prima E Dopo L'unità.* (Quaderno I; Rome: Ufficio Storico della Polizia di Stato, 2013).

process[21]. Many new measures in the field of security and criminal law have followed. As a result of the amendment of Section V of the Constitution in 2001, which gave increased powers to local authorities, regions began adopting laws on security, many of which refer to an "integrated system of security": an ambiguous term ranging from urban degradation to social unease; the education to legality; the mediation of social and cultural conflict; as well as the use of technology.

After WWII Italian security forces underwent only cosmetic change,[22] and retained their military character until 1981. Pursuant to Law 121/81, the Ministry of Interior (*Ministero dell'Interno*) became "autorità nazionale di pubblica sicurezza", that is the responsible body for civilian public order and security,[23] which is enforced by various branches of *Polizia di Stato*[24] (controlled by the Ministry) and *Carabinieri* (military police overseen by the Ministry of Defence), with a complex and sometimes opaque division of labour.

Up until law 124/2007 was passed, the Ministries of Interior and Defence headed the intelligence services, too. Law 124/2007 created the information system for the security of the republic (SIS), made up of the foreign-oriented intelligence service (AISE) and the home-oriented intelligence service (AISI), and overseen by the Government, a board of directors and the Parliament (COPASIR).

A recent reform[25] gave city mayors considerable responsibility for the regulation and maintenance of urban security[26], justified by the representativeness of the mayor, as well as the reform of Section V of the Constitution.[27]

### 2.2.1 Preventive policing and lack of transparency

When appraising the approach to security and surveillance issues in Italy, it is imperative to keep in mind the role of preventive policing, intimately tied to surveillance, and the paucity of scholarly research on the functioning and actions of the institutions in charge of public security (a quasi taboo), which seriously hampers transparency.[28]

Preventive policing and information gathering, i.e. in the absence of any criminal activity, has been a long-lasting feature of policing in Italy,[29] first performed by the so-called 'political offices'[30] of the Kingdom of Italy and, under fascism, also by the OVRA (political police),[31] both holding files[32] of the individuals considered a threat for the political order. The difficult legacy of the dictatorship in a world dominated by the Cold War (which was reflected internally[33]) reinforced the tradition of intelligence-led

---

21 D.p.r. 22 sett. 1988 n. 447. The previous system was inquisitorial, based on secretive preparations by the judge and public prosecutor. For an overview of the Italian criminal law system, see Astolfo Di Amato, *Criminal Law in Italy*, (2011).

22 Della Porta and Reiter (2003).

23 Vv.Aa., 'L'evoluzione Della Normativa in Materia Di Pubblica Sicurezza Fra Stato, Regioni Ed Enti Locali', Rome, Servizio Studi del Senato (2010). See also at: http://www.interno.gov.it/mininterno/export/sites/default/it/sezioni/sala_stampa/dossier/ (last accessed on 26 August 2006).

24 The Italian police forces developed according to the 'continental model' (as opposed to the British 'community model'), whereby the police depended upon the monarch, thus being an expression of the state's powers and conception of security (Della Porta and Reiter (2003).).

25 Decreto Legge 92/2008 "Decreto Sicurezza (Converted into Law 125/2008 "Misure Urgenti in Materia Di Sicurezza Pubblica"), D.L. of 23 May 2008, p.

26 As for a pan-European effort to provide a democratic response to urban security challenges, see Vv.Aa. European Forum for Urban Security, 'Security, Democracy and Cities: The Manifesto of Aubervilliers and Saint-Denis', Paris, European Forum for Urban Security (2012).

27 Vv.Aa. (2010).

28 Labanca (2013).

29 The Carabinieri's most important role was and is the collection of information, prompted by the government or the judiciary. Della Porta and Reiter (2003).

30 Ibid. See also Andreassi, (2000).

31 The Ovra (an acronym whose exact meaning was never unveiled) kept the lists of the individuals connected to activities contrary to the regime. Andreassi, (2000).

32 The Casellario Politico Centrale was created in 1894.

33 Della Porta and Reiter (2003).

policing through the persistent 'political offices'[34] and the Ufficio Affari Riservati[35] well before the terrorist attacks of 9/11, the appearance of homegrown Islamic terrorism and the trend, within the EU, to legally normalize the criminalization of inchoate offences[36] in the context of terrorism.[37] Many factors account for such permanence, not least the fact that, in the 1970s and early 1980s, Italy was ravaged by 'black' and 'red'[38] terrorist attacks.[39] The resurgence of organized crime in the 1990s (in particular, the political killings organized by Mafia, and hooliganism)[40] paved the way to a continuous *de facto* "state of emergency", which substantially supported the approach to preventive policing.

Preventive policing[41] is currently tackled by the Department of Public Security of the Ministry of Interior. The operational arms are the Central Directorate for Preventive Police[42] and the Central Directorate for Criminal Police and the recently created Central Directorate for the Fight against Crime. The former controls the DIGOS (Dipartimento Investigazioni Generali e Operazioni Speciali),[43] which is operational over all national territory.[44] DIGOS has competence on terrorism and the collection of information for the prevention of violence connected to extremism, also in relation to public cultural events and protests, and the protection of democracy. It conducts investigations based on the evidence collected. The Central Directorate for Criminal Police[45] coordinates the investigations of the judicial police and, among others, collects and processes information connected to the "most relevant" forms of crime. In 2005, the Direzione Centrale Anticrimine[46] (Central Directorate for the fight against Crime) was created to tackle organized crime and serious crimes in its international dimension. Under the Directorate operate the Reparti prevenzione del crimine – scattered across the national territory to supplement the specific needs in supporting the control of the territory.

---

34 Ibid.

35 Andreassi, (2000).

36 Incohate offences are the preparatory phases of a crime; after 9/11, counter-terrorism legislation focussed on criminalizing inchoate crimes and directing investigative efforts to their pre-emption. See Katija Sugman Stubbs and Francesca Galli, 'Inchoate Offences.The Sanctioning of an Act Prior to and Irrespective of the Commission of Any Harm', in Francesca Galli and Anne Weyembergh (eds.), *Eu Counter-Terrorism Offences. What Impact on National Legislation and Case Law?* (Brussels: Editions de l'Université de Bruxelles, 2012).

37 Francesca Galli, 'Italian Counter-Terrorism Legislation. The Development of a Parallel Track. ("Doppio Binario")', in Francesca Galli and Anne Weyembergh (eds.), *Eu Counter-Terrorism Offences. What Impact on National Legsilation and Case Law?* (Brussels: Editions de l'Université de Bruxelles, 2012).

38 The right-wing secret society Gladio organized, with the alleged support of the government, numerous terrorist attacks. Likewise, the left-wing terrorist groups, such as the Red Brigades, organized kidnappings and murders (also to protest against the actions of the then Italian Communist Party). Ibid.

39 For a comprehensive discussion, see Della Porta and Reiter (2003).

40 Céline Cocq and Francesca Galli, 'Surveille Deliverable 4.1: The Use of Surveillance Technologies for the Prevention and Investigation of Serious Crimes', (2012).

41 The preventive police tackle threats and risks, and work by coercive and preventive strategies (Della Porta and Reiter 2003), using tools such as confinement (government of peoples) and filing (collection and classification of information). A second type of police is the judiciary police, which support the prosecution and investigation of crimes, which have already occurred. Administrative policing in public spaces and in the regional territory is tackled by the municipal police (controlled at the regional level). Campesi (2009).

42 See description at : http://www.interno.gov.it/mininterno/export/sites/default/it/sezioni/ministero/dipartimenti/dip_pubblica_sicurezza/direzione_centrale_della_polizia_di_prevenzione/scheda_15820.html (last accessed on 26 August 2014).

43 Literally Department of General Investigations and Special Operations See http://www.poliziadistato.it/articolo/23277/. Della Porta and Reiter (2003).

44 See at: http://www.poliziadistato.it/articolo/23277/ (last accessed on 26 August 2014).

45 See at: http://www.interno.gov.it/mininterno/export/sites/default/it/sezioni/ministero/dipartimenti/dip_pubblica_sicurezza/direzione_centrale_della_polizia_criminale/ (last accessed on 26 August 2014).

46 See at: http://www.interno.gov.it/mininterno/export/sites/default/it/sezioni/ministero/dipartimenti/dip_pubblica_sicurezza/direzione_centrale_anticrimine_della_polizia_di_stato/scheda_21205.html (last accessed on 26 August 2014).The international dimension of crime is tackled by a cooperation between investigative bodies. The Directorate hosts an office of the F.B.I. and a laison office with the French Police. See at: http://www.interno.gov.it/mininterno/export/sites/default/it/sezioni/ministero/dipartimenti/dip_pubblica_sicurezza/direzione_centrale_anticrimine_della_polizia_di_stato/ (last accessed on 26 August 2014).

Prevention is also an objective of the security services (AISE and AISI), which engage in extensive collection of information for this purpose, relying on open source, imagery, human, signal, technical, measurement and signature intelligence.

Some decades ago, Italy was termed "the country of the 5 polices";[47] as of a recent Eurostat study, Italy has more policemen per capita than France, Germany and the UK (with the exclusion of Northern Ireland).[48] Despite the crucial roles played by the police – given the peculiar historical conjuncture experienced by the early Republican Italy – there seem to be a persistent scarcity of studies of the recent history of the bodies overseeing security, making the subject-matter appear taboo.

One consequence is the polarized public debate on security. A recent example is the dispute as to whether police officers should wear an identification number (they currently do not),[49] an intervention encouraged by the European Parliament in its resolution of 12 December 2012 on the situation of fundamental rights in the European Union,[50] and the earlier Council of Europe Recommendation on the European Code of Police Ethics.[51]

A second, fundamental, consequence concerns transparency. The multiple branches of security bodies, the duplication of efforts and overlapping roles of the Police and Carabinieri have not helped in clarifying the conduct of the security forces, and thus the relationship between security and civil liberties.[52]

A statute, the Legislative Decree n. 33 of March 14th 2013[53], recently increased the obligations of publicity, transparency, and information sharing of public administration, which concerns equally the Ministry of Interior. The coming years will show the extent to which transparency will be pursued as a democratic principle, rather than a bureaucratic obligation (and how it will be balanced with the protection of privacy).

Change might come, perhaps unexpectedly, from the intelligence services (SIS). Not only is the SIS now overseen by the COPASIR[54] (the parliamentary committee composed by five senators and five members of the lower chamber), but pursuant to the reform, it issues an annual report to Parliament about its activities, and cannot preserve secret documents for longer than 30 years.

The 2013 *Relazione sulla Politica dell'informazione per la Sicurezza* (*infra* section 2.2.2) records the changes undergone by intelligence agencies towards transparency in recent years, and the involvement of citizens in developing a healthy culture of security. Stemming from legal initiatives, such changes gear towards increasing efficiency while anchoring activities in the respect of constitutional democratic principles, in the attempt to reverse the opaque and murky reputation earned by intelligence activities over the years. Revisiting the (implied) trade-off between maintaining security, seen as a necessary precondition for the existence of a polity, and preserving liberties such as privacy, seen as a hinge of modern democracy, are indeed imperative in the wake of the so-called 'datagate', the 2013 revelations by Edward Snowden concerning mass surveillance by the US National Security Agency (NSA) and other authorities. Following Snowden's revelations, the SIS and the Garante signed a Memorandum of

---

47 Referring to Bellavita's "il paese delle cinque polizie, Labanca (2013). These are Polizia di Stato, Guardia di Finanza, Arma dei Carabinieri, Corpo di Polizia Penitenziaria, Corpo Forestale dello Stato.

48 Ibid. See tables at: http://epp.eurostat.ec.europa.eu/statistics_explained/index.php?title=File:Police_officers,_1998-2008.png&filetimestamp=20111124170519 (last accessed on 26 August 2014).

49 Arianna Giunti and Michele Sasso, 'Identificare I Poliziotti? In Italia Non Si Può', *L'Espresso,* 21 Novembre 2013 2013.

50 European Parliament, 'Resolution of 12 December 2012 on the Situation of Fundamental Rights in the European Union (2010 - 2011) ', (2012).

51 Committee of Ministers of the Council of Europe, 'Rec(2001)10 of the Committee of Ministers to Member States', (Strasbourg, 2001).

52 Della Porta and Reiter (2003).

53 Decreto Legislativo 14 Marzo 2013, N. 33. Riordino Della Disciplina Riguardante Gli Obblighi Di Pubblicita', Trasparenza E Diffusione Di Informazioni Da Parte Delle Pubbliche Amministrazioni. (13g00076), p.

54 The comitato parlamentare per la Sicurezza della Repubblica ensures that both intelligence services act in respect of the Constitution and in the interest of the Republic.

Understanding[55] clarifying and strengthening the Italian Data Protection Authority's powers of control over SIS' processing of information.

The media has also played an important role throughout the decades, either demanding accountability of the State and its security forces[56] (often being the only instrument public opinion possessed to gain awareness of the facts), or calling for police action (as in the case of terrorism, and hooliganism). A notable example is represented by the NSA revelations.

### 2.2.2 Policy documents and strategies

An overview of contemporary security issues, policies and strategies is provided by the Ministry of Interior's yearly plan ('Direttiva Generale per l'attività amministrativa e per la gestione relativa all'anno 2014'[57]), the Secret Service's 'Relazione sulla Politica dell'Informazione per la Sicurezza 2013'[58] and the related 'Documento di Sicurezza Nazionale'. These documents provide an important counterpart to citizens' perceptions and impression of security threats. When approaching such documents, it must be taken into account that the Italian word 'sicurezza' encompasses both 'safety' and 'security'.

The *Direttiva Generale* identifies the main internal security issues, namely: thriving domestic and international crime; lasting homegrown (anarchist) and international (fundamentalist) terrorism; the persistence of crime, the deterioration of orderly communities, and the degradation of urban centres; constant migration from North Africa, which is intimately connected to human trafficking (clandestine), and trafficking of women and minors; and the economic crisis. The broad scope of identified dangers seem to support the idea of an "integrated system of security" highlighted above (see *supra,* section 1.2). Each threat paves the way for a number of political priorities and related strategies, some of which concern the relation between privacy, surveillance and security.

First, the *Direttiva* calls for wider data processing. Territorial offices (Questure and the DIGOS) should monitor political extremism in public protests and religious extremism (fundamentalist preaching) to fight the anarchist and terrorist threat. Likewise, international information sharing is seen as an important tool to fight against the mafia.

Second, the *Direttiva* devotes extensive time to databases. On the one hand, it calls for increased interoperability of existing databases, such as fine-tuning the Sistema Informativo Interforze for the sake of the creation of the DNA database pursuant to the Treaty of Prüm. Also, an intranet should be set up to make relevant (unspecified) information accessible to all personnel for efficiency reasons and cost savings. On the other, it establishes the creation of new databases. One is the "Seahorse Mediterranean network"[59] database, based on information shared between European and African members of the network; another is a new database for the department of human resources; the ANPR (national registry of resident population) should be created in compliance with data protection requirements and interoperability of local offices. Moreover, the *Direttiva* identifies the need to better manage existing databases, such as the information system of the Polizia Stradale, and of the unified digital document and electronic identity card where implemented.

---

55 See at: http://www.governo.it/Presidenza/Comunicati/dettaglio.asp?d=73621 (last accessed on August 26 2014).

56 For instance, against the conduct of police forces for the violence committed against peaceful protesters in the Diaz school, and the killing of a protester, during the G8 summit in Genoa in 2001.

57 Ministero Dell'interno, 'Direttiva Generale Per L'attività Amministrativa E Per La Gestione Relativa All'anno 2014', Roma, (2014).

58 Sistema Di Informazione Per La Sicurezza Della Repubblica, 'Relazione Al Parlamentosulla Politica Dell'informazione Per La Sicurezza 2013', (2014).

59 See at http://www.statewatch.org/news/2013/apr/eu-council-cosi-29-measures-4-illegal-migration-es15906-rev1-12.pdf (last accessed on 26 August 2014).

Third, technology investment features in the *Direttiva*. The CCTV systems installed in public areas as identified in the "special security agreements" between the Ministry of Interior and the territory should be appraised from the point of view of sustainability and technological innovation;[60] the EUROSUR EU project should be strengthened, also by using available technology; (unspecified) new technologies should be used to improve the control of migratory fluxes.

Finally, the *Direttiva* identifies other objectives connected to digitalization: training school pupils, teachers and parents to use the Internet safely; ensuring the uniformity and timeliness of published data, and access to information, to foster a culture of legality, transparency and integrity; strenghtening online services, such as for payments and to apply for citizenship; and substituting paper documents with electronic documents.

The Secret Services Annual Report '*Relazione sulla Politica dell'Informazione per la Sicurezza 2013*' focuses on two security priorities: 'cyber threats' and challenges to the economic and financial sectors.

The prominence of cyber threats marks the most important change in comparison with previous years,[61] and was certainly accelerated by the adoption of a Europe-wide cyber security policy. 2013 was dominated by cyber-related activities and the publication of the 'Documento di Sicurezza Nazionale' focussed on cyber security and critical information infrastructure protection. The report acknowledges the importance of protecting the cyber domain due to the fundamental role played by information and communication technologies connected to the Internet for social and economic wellbeing. The report, however, does not focus on threats such as those acknowledged in the Convention on Cybercrime. Rather, it addresses threats to the economy and to political order caused by cyber espionage, the use of the Internet by organized crime to steal financial information, and activism supporting extremist activities online.

Threats to the economic and financial sectors featured in previously published reports, and the challenges identified are of a similar nature. One lies in the potential acquisition of Italian industries in strategic sectors by foreign investors; another comes from energy supply needs (which explains the continuing attention to middle Eastern crises). The proliferation of criminal organizations in different sectors of the economy, and the daunting levels of fiscal evasion and fiscal security complete the picture.

The report covers other challenges that overlap with the priorities of the Ministry of Interior, namely homegrown (subversion) and global (terrorism). Subversion derives from right and left wing extremists (including anarchist-insurrectionist) who exploit the economic crisis to advance anti-systemic views. Terrorism is analysed under the lenses of foreign returning fighters.

Neither of the two reports contains a serious review of the systems and tools put in place to tackle the threats outlined. As a result, the absence of an impact assessment of the use of certain tools (notably on the rights to privacy) is unsurprising. Such assessments are in any case alien to the Italian political culture.

[60] See at (in Italian): http://www.interno.gov.it/mininterno/export/sites/default/it/temi/sicurezza/0999_patti_per_la_sicurezza.html (last accessed on 26 August 2014).

[61] Sistema Di Informazione Per La Sicurezza Della Repubblica (2014).

## 2.3 "Privacy" in Italy: the law and the DPA (Garante)

Privacy, like security, relates to a cluster of closely interrelated rights, namely the right to respect for private and family life, and the right to protection of personal data.

The right to private and family life, in its many facets, is embedded in the Italian Constitution, as interpreted in the judgment of the Cassation of 25 May 1975, n. 2129. Italy ratified both the European Convention on Human Rights (ECHR)[62] (1955) and the International Covenant on Civil and Political Rights (1978)[63], which contain binding rules on the right to private and family life and privacy in articles 8 and 17 respectively.

The protection of personal data acquired increasing relevance in the late 1960s, in parallel with the evolution of computing. Italian scholars began addressing the matter in the 1970s[64]. Italy supported the OECD Privacy Guidelines and signed the Council of Europe Convention 108,[65] the text that inspired the adoption of Directive 95/46/EC[66]. The process proved difficult, as in most countries[67]: several legislative proposals ensued with no result. Consequently, Finocchiaro notes that Italy could not ratify Convention 108[68], and could not be part of the Schengen Information System when it was created in 1995: both required the existence of national rules on data protection.[69]

More importantly, the central database of the police came into being during the impasse on the adoption of a legal framework on privacy and data protection.[70] Article 8 of Law n. 121/1981 created the Centro elaborazione dati (CED) del Dipartimento di Pubblica Sicurezza, a 'fusion centre' hosted by the Servizio per il Sistema Operativo Interforze within the Central Direction for the Criminal Police.[71] The Servizio Analisi Criminale (Criminal Analysis Service) works on the basis of the CED.[72] The CED is regulated by Presidential Decree n. 378 of 3 May 1982, and is in charge of the classification, analysis and evaluation of information and data provided by police forces. The law addressed the relation between the prevention and prosecution of crime on the one hand, and the constitutional guarantees of the individual on the other. Article 7 of Law 121/1981, for instance, forbids the collection of data on individuals solely relating to their ethnicity, political opinions, religious views, membership in trade unions, or in cultural associations, organization of care or cooperatives. However, there was no oversight on matters of data protection.

The situation changed when Italy adopted its first code (after a number of failed attempts), Law of 31 December 1996, n. 675 implementing the Data Protection Directive and creating the Italian Data Protection Authority, the Garante per la Protezione dei Dati Personali (hereafter the Garante). Italy could thus ratify and implement Convention 108.[73]

---

62 Convention for the Protection of Human Rights and Fundamental Freedoms, as Amended by Protocols No 11 and 14, CETS n° 005, p. 4 November 1950.

63 International Covenant on Civil and Political Rights, p. 16 December 1966.

64 See, notably Stefano Rodotà, *Elaboratori Elettronici E Controllo Sociale*, (1973). The book addressed the state of the art of the debate vis-à-vis the Italian case

65 Giusella Finocchiaro, *Privacy E Protezione Dei Dati Personali. Disciplina E Strumenti Operativi*, (2012).

66 Directive 95/46/Ec of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Data Protection Directive), OJ L 281, p. 31-50, 23 November 1995.

67 Lee A. Bygrave, *Data Privacy Law. An International Perspective*, (2014).

68 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, CETS No. 108, p. 28 January 1981.

69 Finocchiaro (2012).

70 Italy ratified Convention 108 in 1997 (see at: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG ).

71 More information (in Italian) at http://www.interno.gov.it/mininterno/export/sites/default/it/sezioni/ministero/dipartimenti/dip_pubblica_sicurezza/direzione_centrale_della_polizia_criminale/scheda_16059.html) and http://www.interno.gov.it/mininterno/export/sites/default/it/sezioni/servizi/come_fare/banca_dati_delle_forze_di_polizia/come_fare_per_saperne_di_pix.html (both last accessed on 26 August 2014).

72 See at http://www.interno.gov.it/mininterno/export/sites/default/it/sezioni/ministero/dipartimenti/dip_pubblica_sicurezza/direzione_centrale_della_polizia_criminale/scheda_15774.html (last accessed on 26 August 2014).

73 Finocchiaro (2012).

The Garante is composed of four members elected by the Parliament; their mandate lasts seven years and cannot be extended. In 2013, the Garante had 104 employees and a budget of € 23 million, which is slightly lower compared with 2012. Each spring the Garante publishes an Annual Report that details its activities in the various field of competence and provides statistical data. Among its many duties, it oversees the correct processing of personal data and prescribes corrective measures; it examines claims and warnings and decides on complaints; it can prohibit part or the whole of a processing; it can inflict sanctions; it advises the Government on the need to adopt certain measures; it educates, informs and consults citizens; it takes part in international gatherings; and it controls, together with a technical commission, the CED (but pursuant to law 125/2008, input and access into the CED has been widened to local security authorities, thus challenging tight controls).

Data protection law was substantially revised in 2003 to incorporate the many adjustements required by technological evolution, as well as the innovations brought about by the e-privacy Directive 2002/58. The result was legislative decree of 30 June 2003, n. 196, called "Code on the matter of protection of personal data"[74] and referred to as the "Privacy Code". The Code protects personal data understood both as the physical data and the information contained therein (in line with national and European jurisprudence). Until three years ago, personal data also included data referring to legal persons, but the provision was amended by decree n. 201 of 6 December 2011.

The scope of application of the Code as far as police activities and intelligence services are concerned is circumscribed. Scholarhip judges this state of affairs either positively,[75] given the importance of the interests at stake, or negatively, in the light of the threats to civil liberties.[76] Title II of the Codice addresses processing of data by police forces; article 53, subparagraph 1 provides for the limited application of most articles of the code.[77] However, the Ministry of Interior has not adopted yet the implementing measures concerning article 53 of the Privacy Code.[78]

The scope of application is particularly reduced in the case of defence and security of the state (title III of the Code), for which there are considerable exceptions, as justified by the role of "high direction, general political responsibility and coordination of security and information policies, in the interest and for the defence of the democratic state which underlie it"[79]; the only possible oversight is exercised by the COPASIR.[80] A positive development consisted in the abovementioned conclusion of a Memorandum of Understanding between the Italian Garante and the Secret Services, which reinforced and clarified the cooperation between the two bodies.

## 2.4 SOSTs in Italy: usage and public discourse

Article 55 of the Privacy Code relates to special technologies used for processing by police forces. The use of special technologies potentially impacting on civil liberties (as clarified by article 17) is allowed, provided the Garante authorizes the processing, which is supposed to take place with additional safeguards. However, as mentioned in section 2.2 above, technologies and practices proposed to tackle security threats are not only unquestioned, but presented as the most appropriate tools for the task. Consequently, alternative instruments and practices are rarely considered. The discussion may simply be deemed inappropriate in the framework of documents addressing security priorities, and be carried out elsewhere. The problem may also lie in the fact that the problematic relation between the use of certain technologies by law enforcement agencies and privacy/civil liberties should not be exposed to public opinion.

---

74 The English version is available at: http://194.242.234.211/documents/10160/2012405/DataProtectionCode-2003.pdf (last accessed on 26 August 2014).

75 Ivano Iai, 'Il Trattamento Dei Dati Personali Da Parte Delle Forze Di Polizia', in Vincezo Cuffaro, Roberto D'orazio, and Vincenzo Ricciuto (eds.), *Il Codice Del Trattamento Dei Dati Personali,* (Torino: Giappichelli editore, 2007).

76 Stefano Rodotà, *Intervista Su Privacy E Libertà. A Cura Di Paolo Conti*, (2005).

77 with exceptions concerning sensitive data, as in article 55.

78 See at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1557209 (last accessed on 26 August 2014).

79 Article 1 subparagraph 1 of law n. 801 of October 24th, 1977.

80 Iai (2007).

Keeping in mind such lack of transparency, this section appraises the use of surveillance-oriented security technologies (SOSTs) and, when available, related public discourse in the media (which suffers from the polarized approach to security matters). By means of example we consider five SOSTs appraised by the SurPRISE project[81]: drones, biometrics, deep-packet inspection, smart CCTV and smartphone location tracking.

**CCTV cameras** are a common SOST in Italy, the introduction of which was prompted by several circumstances.

One is the "special security agreements"[82] signed by the Ministry of Interior and local authorities for the provision of measures to tackle exceptional urban security threats. Indeed, one of the operational objectives of the Ministry of Interior is to "monitor the efficacy of the projects of video surveillance, in public places or places open to the public, in terms of sustainability and correspondence to the technological features described in the guidelines to a 'special security agreement' to better control the territory".[83]

Another factor is the local authorities' response to the feeling of insecurity reported by inhabitants of a number of cities,[84] despite the decreasing number of crimes, as discussed later in this report. Indeed, Law n. 48 from 23 April 2009 allows municipalities to employ video surveillance in order to guarantee "urban security," in public places.[85]

Hooliganism in stadiums, which led to considerable violence and public debates, resulted in the introduction of CCTV cameras in stadiums.[86] Video surveillance is also used for prosecuting offences relating to access to areas of limited traffic.[87]

The iniquitousness of CCTV cameras led to their prompt regulation from the perspective of privacy. The Garante issued guidelines to clarify how the Privacy Code applies to matters of video surveillance.[88] The Guidelines call for the lawfulness, necessity and proportionality of the measure, as well as the obligation or desirability to inform citizens affected. Authorizations requested to install smart CCTV have increased in the past few years. CCTV cameras are rarely the focus of public debate, apart from when CCTV footage could help to solve crime.

**Drones** have been spreading quietly in Italy, and the growing numbers of drone-enthusiasts[89] has attracted the attention of the media only recently. Public scrutiny may have grown in connection with ENAC's ("Ente Nazionale Aviazione Civile"[90]) recent adoption of the regulation disciplining the use of civil drones[91] in populated areas. While the regulation refers to issues of data protection (art. 22), its adoption

---

81 Maria Grazia Porcedda, Mathias Vermeulen, and Martin Scheinin, *Report on Regulatory Frameworks Concerning Privacy and the Evolution of the Norm of the Right to Privacy. Deliverable 3.2, Surprise Project.*, (2013); Unabhaengiges Landeszentrum Fuer Datenschutz (Uld), 'Report on Surveillance Technology and Privacy Enhancing Design, Deliverable 3.1, Surprise Project', (2013). ADD D2.3

82 See at http://www.interno.gov.it/mininterno/export/sites/default/en/themes/security/other_security-relatedactivities.html (last accessed on 26 August 2014).

83 Ministero Dell'interno (2014) at 68.

84 For examples of how video surveillance is applied in some Italian cities, see Vv.Aa. European Forum for Urban Security, 'Citizens, Cities and Video Surveillance. Towards a Democratic and Responsible Use of Cctv', Montreuil, European Forum for Urban Security (2010).

85 Marco Calamari et al., 'Country Report Italy', Privacy International (2011).

86 Iai (2007). See also article 1 *quater* of law of 24 April 2003 n. 88.

87 Article 17, § 133-bis, Decreto Legislativo 15 maggio 1997, n.127.

88 Italian Data Protection Authority, 'Video Surveillance Guidelines', Rome, Garante per la protezione dei dati personali (2010).Available at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1767009 (last accessed 26 August 2014).

89 See, for instance, a magazine dedicated to the use of drones (http://www.dronezine.it/) and the organization of fairs dedicated to drones Carlo Lavalle, 'A Roma Il Primo Salone Aeronautico Sui Droni in Italia ', *La Stampa,* 25 maggio 2014 2014.

90 ENAC is the institution overseeing civil aviation.

91 The decision is available at: http://www.enac.gov.it/la_regolazione_per_la_sicurezza/navigabilit-13-/omologazione_e_organizzazioni_di_progettazioni/prodotti/aeromobili_esclusi_dalle_competenze_easa/ (last accessed on August 26 2014).

did not spark much public debate on privacy issues,[92] as opposed to safety.[93] A recent protest was spurred by the use of drones by paparazzi (with some coining the term "dronalists", from drones and journalists) in a glamorous Italian summer holiday destination. The mayor of the town threatened to confiscate the drones to protect the privacy of the famous vacationists.[94] Yet, a debate about the wider social implications concerning the public at large of the use of drones in public spaces has yet to take place.

The ENAC regulation does not apply to the use of drones for law enforcement or military purposes. In fact, surveillance drones seem to be already in use, as in the case of "Guardian 2000".[95] The Polizia di Stato is in the process of selecting the model that will be deployed for enforcement purposes.[96] Drones are also utilized to patrol the coastline of Sicily under the aegis of NATO,[97] but their employment was reported as a *fait accompli* and triggered limited debate.[98]

The use of **biometrics** for security purposes in Italy has been discussed for over ten years, and is linked to a number of initiatives. First, the Ministry of Foreign Affairs proposed to introduce electronic passports endowed with a RFID chip storing biometrics in 2005. However, the plan was never implemented and "the Italian passports were modified only by inserting ordinary enhancements like printing computer-readable text and photo, because the negative privacy consequences of RFID features became an international affair"[99] (rather than a national one). Further attempts to use biometric authentication technologies have been made since 2009, for check-in[100] and boarding operations within a number of airports under the so-called borders information system.[101]

Second, a pilot program of fully electronic national ID cards containing biometric data was launched in 2005, but it was interrupted without explanation, although a new proposal was tabled. "Starting from 1 January 2010 all Italian ID, electronic or traditional, should have carried a printed fingerprint that would have been also centrally recorded in digital format. The Financial Law 2010 (*Legge Finanziaria* 2010) postponed the date to 1 January 2011."[102] The reforms proposed in the "Digitalia" package contain provisions for the mandatory introduction of an electronic ID card integrating the fiscal code with the health insurance documents[103] (currently being implemented).

Third, following the ratification of the Treaty of Prum, the Garante authorized the creation of a DNA database,[104] subject to the adoption of national laws addressing certain legal vacua. Parliament passed Law No. 85 of 30 June 2009, which created two databases, one for genetic samples and the other for DNA profiles; however, the law provides for a disproportionate period of data retention, which may be in breach of article 8 of the ECHR.[105] The database should be operational in 2015.[106]

---

92 On the point, see the presentation delivered by Giovanni Battista Gallus within the conference "La privacy che verrà", available at http://e-privacy.winstonsmith.org/atti/ep2014se_19_gallus_droni_parte_2.pdf (last accessed on August 26 2014).

93 Pino Bruno, 'L Drone Più Sicuro Al Mondo È Italiano, Lo Ha Ispirato Olivetti', *La Repubblica,* 2 giugno 2014 2014.

94 N/A La Repubblica, 'Il Sindaco Di Forte Dei Marmi: "Sequestro I Droni in Volo"', *La Repubblica - Edizione di Firenze,* 14 maggio 2014 2014.

95 N/A Wired, 'Guardian 2000, Un Drone Poliziotto Nei Cieli Italiani', *Wired.it,* 28 marzo 2014 2014.

96 See at: http://www.poliziadistato.it/articolo/view/33560/ (last accessed on 26 August 2014).

97 Alessandro Puglia and Lorenzo Tondo, 'Sigonella Diventa Base Strategica Ecco Le Slides Riservate Della Nato', *La Repubblica - Edizione di Palermo,* 3 agosto 2014 2013.

98 Alberto Bonanno and Alessandro Puglia, 'L'hangar Segreto Di Sigonella Con I Droni Spia Americani', *LA Repubblica,* 29 giugno 2014 2014.

99 Calamari et al. (2011).

100 See the recent http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2059468 (last accessed on 26 August 2014).

101 Commissione Europea, 'Decisione Della Commissione Del 17.7.2012 Che Approva, Per L'italia, Il Programma Annuale 2012 Per Il Fondo Per Le Frontiere Esterne, E Il Cofinanziamento a Titolo Di Tale Fondo Per L'esercizio 2012 ', (2012). Available at: http://autorita-audit.interno.it/download/allegati1/ap_2012.pdf (last accessed on 26 August 2014).

102 Calamari et al. (2011).

103 Valentina Conte, 'Ridotto Il Decreto Sviluppo Bis. Il Colle Taglia Norma Pro-Berlusconi', *La Repubblica,* 4 ottobre 2012.

104 See at: http://www.garanteprivacy.it/garante/doc.jsp?ID=1548579 (last accessed on 26 August 2014).

105 Calamari et al. (2011).

Finally, the use of biometrics by the private sector (in particular banking) has also been the object of discussion, attention and regulation by the Garante, which released guidelines for the use of biometrics in May 2014.[107]

The use of **electronic surveillance** for security purposes has not been brought to public attention for a long time, as opposed to traditional phone tapping (which is widely debated in Italy, but is beyond the scope of this report). A hint was given in 2005, when the Italian ISP Autistici/Inventati discovered that the Postal Police had placed a backdoor in their servers relating to an investigation of the anarchist collective Crocenera. The backdoor led to the monitoring of the communications of more than 30,000 subscribers, which include many NGOs, associations and grassroot activists.[108] Yet, the topic seized public attention only with Edward Snowden's revelation of the mass electronic surveillance scheme,[109] referred to as "datagate". However, there has been a relative silence of the institutions on the matter;[110] In fact, a parliamentary inquiry has not been issued yet, even if Italian citizens have been subject to surveillance, too.[111] Reportedly, the Italian secret services knew about the eavesdropping operations, without taking part in them.[112] Following the scandals, the Garante and the Intelligence Services have agreed on a protocol of intent (i.e., not binding) on closer cooperation.[113]

The Italian Parliament ratified the Convention of Budapest on Cybercrimes with law 48/2008 modifying articles 244 and 247 of the Code of Criminal Procedure.[114] Both search and seizure and wiretapping of ISPs for criminal investigation require an Attorney General's decision, and request to the judicial authorities for "pre-emptive investigation" respectively.[115]

Finally, (**smart)phone location tracking** relates to different techniques of tracking. One concerns the provisions of the recently invalidated Data Retention Directive (24/2006/EC), which was enforced by Legislative Decree No. 109/08.[116] The destiny of data retention provisos will depend on political and further judicial decisions. Meanwhile, the judgment and datagate sparked the publication of articles relating to the collection of metadata, including location data. The British newspaper 'The Guardian' revealed that Italy ranks first among the states requesting metadata of communications, with a total 606,000[117] demands. There seems to be less debate relating to GPS-based localization and localization based on apps.

---

106 Walter D'amario, 'Banca Dati Del Dna, C'è La Sede E Lo Spot Tv. Ma L'istituto Funzionerà Dal 2015', *La Repubblica,* 4 February 2014 2014.

107 N/A, 'Privacy, Dal Garante Nuove Regole Per Le Tecnologie Biometriche', ibid.21 May 2014.

108 Calamari et al. (2011).

109 Bruno Manfellotto, 'Quattro Mesi Per Capire Il Datagate', *L'Espresso,* 5 November 2013 2013.

110 'Datagate - Bonino in Parlamento - Chiarimenti Necessari Ma Andare Avanti Con Trattato Usa-Ue ', (updated 4 July 2013) <http://www.esteri.it/MAE/IT/Sala_Stampa/ArchivioNotizie/Approfondimenti/2013/07/20130704_datagate_bonino_parlamento.htm>.

111 Redazione Del Fatto Quotidiano, 'Datagate, Italia Intercettata. Copasir E Garante Della Privacy: "Chiarire"', *Il Fatto Quotidiano,* 22 Octobr 2013 2013b.

112 Redazione Del Fatto Quotidiano, 'Datagate, Letta Al Copasir: "La Privacy Degli Italiani Non È Mai Stata Violata', *Il Fatto Quotidiano,* 2013a.

113 Martina Pennisi, 'L'accordo Fra Garante E Servizi Segreti Ci Difende Dalla Nsa?', *Wired,* 12 November 2013 2013.

114 Calamari et al. (2011).

115 Ibid.

116 Ibid.

117 Alessandro Longo, 'Vodafone: "Alcuni Governi Hanno Accesso Diretto Alle Comunicazioni Dei Nostri Utenti". Il Garante: "Inaccettabile"', *La Repubblica,* 6 June 2014 2014.

# 3 The design of the Italian citizen summit

## 3.1 The summit

The Italian citizens' summit took place in Florence on Saturday February 8th 2014. The summit, which lasted from 10:00 am to 16:30 pm, featured the participation of 193[118] citizens, gathered to discuss and answer a set of questions on Deep Packet Inspection and smartphone location tracking, and formulate recommendations for European and national politicians.

The venue for the Italian citizens' summit was 'Palazzo degli Affari', a congress room of Firenze Fiera (the city's main Congress and Exhibition Centre), located directly in front of the Florence central railway station.

Professor Martin Scheinin, the scientific director of SurPRISE at the European University Institute (EUI), opened the day, followed by a guest speech by Professor Cristina Giachi, vice Mayor, member of the Florence City Council and at the time representative for education, European funds, universities, research, youth and equal opportunities affairs. As a sign of its importance, the summit received the moral sponsorship of the Region of Tuscany, the Province of Florence, the Municipality of Florence, the Representation of the European Commission in Italy, the Italian Data Protection Authority and the Italian Forum for Urban Security.

A professional in the field of facilitation of participatory events, contracted for the event, guided the summit as head facilitator. The programme of the day followed the pattern of all other citizen summits in SurPRISE. The first SOST discussed was Deep Packet Inspection (DPI), followed by smartphone location tracking. Finally, citizens drafted and presented their recommendations to European and national politicians. The 193 citizens were assigned to groups of 5-7 people sitting at 35 tables. A table moderator led each group. Table moderators were partly professional moderators experienced in group moderation at participatory events, and partly EUI PhD students in social science.

In order to ensure the widest participation possible, all participants received a gift voucher worth 50€ and compensation for travel expenses[119]. Moreover, a babysitting service was made available at the venue, and a bus service was organized for participants coming from rural areas. At the summit participants received a complimentary breakfast, lunch and coffee break. The participants were ordinary citizens, without any professional knowledge in the area of surveillance, privacy and security. They came from the territory of the Province of Florence and were chosen so as to reflect Italian national demographics.

[118] The day before the summit 255 citizens had confirmed their participation, which accounts for a 24% no-show rate.

[119] Compensation was also in the form of vouchers of varying value depending on the places of residence of participants.

## 3.2 Recruiting citizens

Citizens were invited by a recruitment company specialized in participative processes and methods, in cooperation with a spin-off of the University of Florence specialized in computer-assisted telephone surveying. The company identified a sample of 2,500 citizens from a wider sample of individuals extracted from the public registries of 7 representative municipalities of the Province of Florence. Citizens' data, formally requested and obtained from the public registries, included:

- Name and surname; number of family members; name and surname of the head of household (to connect the individual to a house phone number);
- Age; gender;
- Educational level; employment status;
- Address; place of birth (and ISTAT code of the municipality); place of residence; and nationality.

The sample was identified according to the following criteria: age (representative spread across age groups from 18 to over 90); gender (50/50 spread); geographical area (representative spread of urban, suburban and rural areas and a share of citizens living in the Province of Florence but born in other Italian regions); education (a good spread of categories ranging from primary, lower and upper secondary school, to university education); and occupation (a good spread of the categories used in the questionnaire). An example (random extraction requested to the City of Florence) of the sampling of citizens is shown below:

| Gender | Educational level 2 categories | Age | Number of individuals |
|---|---|---|---|
| **F** | Upper secondary and university | 18-35 | 1000 |
| **F** | Upper secondary and university | 36-59 | 1000 |
| **F** | Upper secondary and university | Over 60 | 1000 |
| **F** | Primary and lower secondary | 18-35 | 1000 |
| **F** | Primary and lower secondary | 36-59 | 1000 |
| **F** | Primary and lower secondary | Over 60 | 1000 |
| **M** | Upper secondary and university | 18-35 | 1000 |
| **M** | Upper secondary and university | 36-59 | 1000 |
| **M** | Upper secondary and university | Over 60 | 1000 |
| **M** | Primary and lower secondary | 18-35 | 1000 |
| **M** | Primary and lower secondary | 36-59 | 1000 |
| **M** | Primary and lower secondary | Over 60 | 1000 |
| **Total** | | | 12000 |

Table 1: Random extraction requested to the City of Florence for the sampling of citizens.

In order to ensure the inclusiveness and diversity of the sample, citizens or residents with foreign origins and people with disabilities were invited through direct contact with local civil society organizations.

The target for the recruitment company was set at 250 confirmed participants before the summit, to account for no-shows on the day of the event.

The company performed three rounds of calls to recruit citizens: the first to identify a group of interested citizens and invite them to the summit, the second to confirm participation of the selected group of citizens, and the third as a reminder and to receive additional confirmation of participation from citizens (including substitution of citizens who decided to withdraw). Citizens also received a final call two days before the summit and a text message the day before the summit.

In addition to the phone calls, the EUI SurPRISE team sent emails and letters of invitation to those people who agreed to be contacted and expressed interest in the event, and letters of confirmation[120] to the citizens who confirmed their participation during the second round of phone calls. A dedicated telephone line and an email account were also created to address queries during the weeks before the summit. Information on the summit could also be found on a dedicated page on the EUI website (www.eui.eu/surprise).

During the month of January, posters advertising the citizen summit were placed in several neighbourhoods of the city of Florence, which offered citizens the chance to enrol in the summit by writing to the SurPRISE EUI email account.

The final citizen panel resulted from the combination of the different recruitment methods used: 3% of the respondents were voluntarily enrolled, 24% were invited through local associations, 9% were recruited through snowball sampling and 64% were recruited through demographic sampling.

## 3.3 The 193 participants of the summit

Of the 193 participants, 47% were women and 53% were men[121]. The age groups 18-30 and 50-59 were slightly overrepresented, but in general all age groups were equally represented (18-29: 21%, 30-39: 13%, 40-49: 16%, 50-59: 25%, 60-69: 10%, over 70: 15%)[122]; the panel featured the same share of participants below and above 50 years old (50% each).

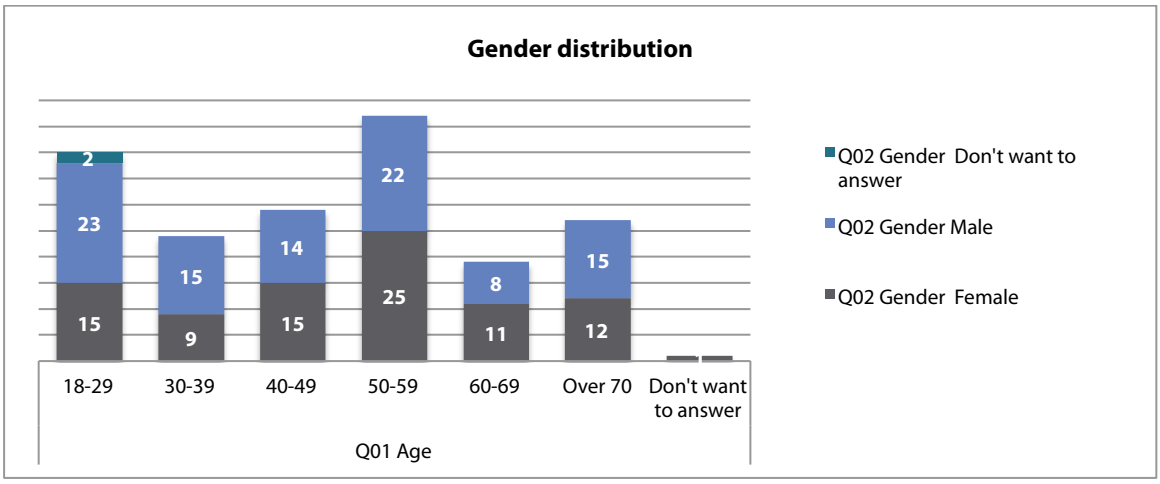



Figure 1: Gender distribution

The municipalities of the Province of Florence identified for recruiting the participants included a city (Florence, 366,039 inhabitants), 4 towns (12,000 – 50,000 inhabitants) and 2 small towns/ villages (5,000 inhabitants). The selected municipalities were also representative in terms of population density, since three of the municipalities have a density below 150 inhabitants per square kilometre, which can be considered rural following the OECD criteria[123]. Taking into consideration both the number of inhabitants and population density, urban participants accounted for 66% of the panel, suburban participants for 28% and rural for 6%.[124]

[120] The package included the information material, the consent form, programme of the day, practical information about the venue and about the incentives for participation.

[121] Percentages relating to the entire panel of 193 participants. Demographic information has been provided by participants during the organization of the citizen summit. On the day of the summit 102 males and 91 females were present.

[122] Percentages relating to the entire panel of 193 participants.

[123] Organization for the Economic Cooperation and Development, 'Defining and Describing Regions', *Oecd Regions at a Glance 2011* (Paris: OECD Publishing, 2011). Available at: http://www.oecd-ilibrary.org/urban-rural-and-regional-development/oecd-regions-at-a-glance-2011/defining-and-describing-regions_reg_glance-2011-4-en.

[124] Percentages relate to the entire panel of 193 participants.

By including in the selection citizens who currently reside in the territory of the province of Florence but were born and/or previously resided in other Italian regions, the geographical diversity of the panel was increased. These participants accounted for 12%[125] of the panel. In addition, the panel included foreign-born residents and citizens, both from EU and non-EU countries, accounting for 20% of the panel[126]. Indeed, the respondents declared to be: Italian citizens (76.9%); citizens of a non-European country (9.3%); citizens of both a European and a non-European country (4.9%); citizens of another European country (3.8%); dual citizens of two non-European countries (1.1%); and dual citizens of two European countries (0.5%)[127]. As for minorities, 23.33% of respondents declared to consider themselves as belonging to a minority group, only slightly higher than the European average.[128]

The educational level of participants was also diverse as the panel included respondents having completed primary or lower secondary school (16%), higher secondary school (39%) and university studies (42%)[129], either undergraduate, graduate or postgraduate. The level of education is lower than the average of all SurPRISE summits (Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland and United Kingdom), but in line with national statistics given the distribution of age of the Italian sample.

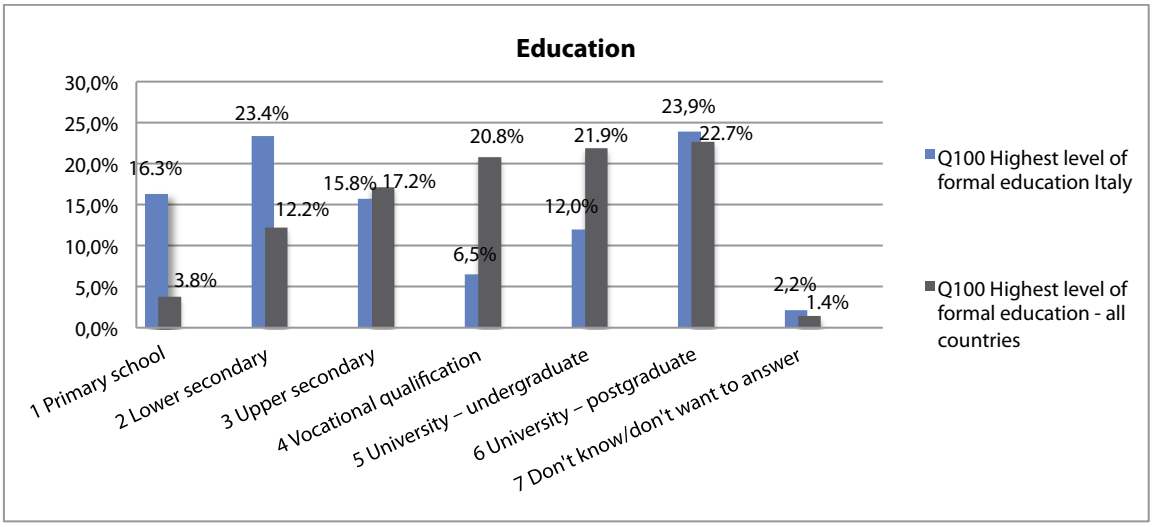



Figure 2: Education

In terms of employment status, 33% of the participants declared to be employed, 17% self-employed, 13% unemployed, 3% stay-at-home parents or carers, 10% students and 21% retired[130].

Regarding categories of employment, the most common were 'clerical support' (29.8%), 'technician and associated professional role' (17%), 'professional' (13.5%), while 6.4% of the respondents declared to be 'services and sales worker', and the same share chose 'crafts and related-trades'. The item 'manager, legislator or senior official' was selected by 5.3% of respondents, the entry 'elementary worker' was

[125] Percentages relate to the entire panel of 193 participants. 131 participants residents and born in the Province of Florence, 24 participants born/who spent part of their life in other regions (South, 6 participants, Centre, 3, Islands, 2, North West, 7, North East, 6) and 38 foreign born (EU and non EU countries) residents.

[126] Percentages relate to the entire panel of 193 participants.

[127] 182 respondents out of 193 voted on this questionnaire item and among them 3.3% used the option "I don't know I don't want to answer".

[128] The definition "minority ethnic group" was considered inappropriate for the Italian context and the word ethnic was removed from the question. 180 respondents out of 193 voted on this questionnaire item and 9.44% used the option "I don't know / I don't want to answer".

[129] 3% chose the option "I don't know / I don't want to answer".

[130] 3% chose the option "I don't know / I don't want to answer".

chosen by 5.2% of the panel, while 'skilled agricultural, fisheries or forestry worker' was clicked by 4.7% of the respondents. The least selected category was 'plant and machine operator or assembler', 0.6%[131].

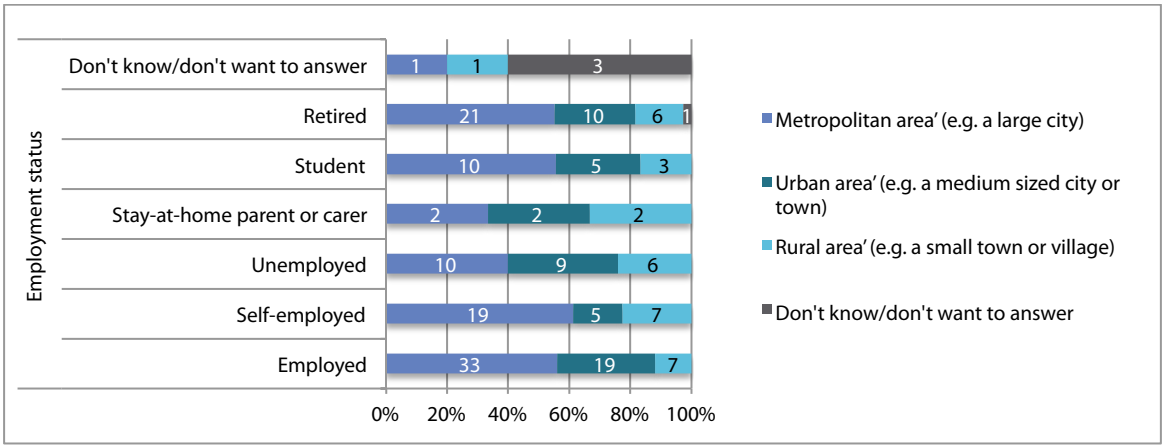



Figure 3: Employment status in different areas

In terms of income, 29.07% of the participants declared to earn more than € 19,655[132] (with 8.72% declaring to earn considerably more than the average annual income), 12.21% said to earn about the same as the average national income, and 40.12% claimed to earn less than the average (with 23.26% declaring to earn a considerably less than the average)[133].

An additional demographic question inquired into the share of participants having children at home aged 16 or under. As a result, 19.67% of the respondents declared to have children at home aged 16 or under[134].

In addition to the previous criteria, inviting people with disabilities, who accounted for 4% of the panel, has increased the inclusiveness and diversity of the sample[135].

## 3.4 How participants assessed the Italian summit

Participants' assessment of the summit was captured through direct observation, feedback solicited from citizens during the summit, and evaluation reported by the table facilitators who filled in a dedicated form. According to the accounts provided by table moderators and direct observation, participants' general response to the summit was very positive. Citizens felt welcome and deeply enjoyed the event. They appreciated the methodology and were enthusiastic about how the summit was organized. In particular, participants liked the rotation between voting sessions, discussion sessions and breaks. Many valued the importance of elaborating recommendations and requested reassurances that they would be delivered, although they manifested pessimism as to the possibility that politicians would listen to them. This attitude was reflected in the vote to the second evaluation question (question #107, N=180): **40.6% of participants agreed or strongly agreed with the statement "I believe the citizen summit has generated valuable knowledge for the politicians",** 10 percentage points lower than the average of all SurPRISE summits as shown below. While 25.6% were undecided, in line with the other summits, a third disagreed or strongly disagreed, as opposed to 17% at the European level.

[131] Only 171 respondents out of 193 voted on this questionnaire item and among them 11% used the option "I don't know / I don't want to answer".

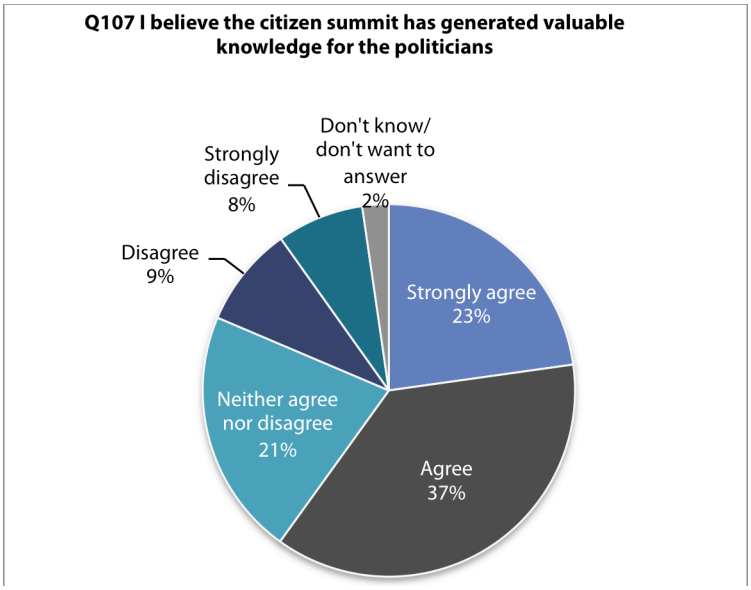
[132] Average annual earnings of Italian tax payers based on income tax declarations presented for the year 2011, Ministero Dell' Economia E Delle Finanze, 'Analisi Dei Dati Irpef. Anno D'imposta 2011', (2011).Available at: http://www1.finanze.gov.it/analisi_stat/contenuti/analisi_dati_2011_irpef.pdf

[133] 172 respondents out of 193 voted on this questionnaire item and among them 18.6% used the option "I don't know / I don't want to answer".

[134] 183 respondents out of 193 voted on this questionnaire item and among them 5.46% used the option "I don't know / I don't want to answer".

[135] Percentage relate to the entire panel of 193 participants.

**The data might reflect Italians' high rate of disaffection with politics recorded shortly after elections,[136] but might also reflect the lack of involvement of public opinion on matters of national security**.




Some citizens had never taken part in a participatory event and enjoyed, in particular, the possibility to confront themselves with strangers and people of completely different backgrounds. **Many citizens recommended repeating similar events and expressed the desire to be informed of the results of the event in other countries and the project as a whole.** The discussions on surveillance-oriented security technologies (SOSTs) were mostly positive and constructive, and participants respected the rules of good dialogue, whether they shared similar views or not. Table recommendations were prepared with enthusiasm and a lot of tables volunteered to have their recommendation read aloud; those shared were very structured and detailed. Many moderators underlined they had a very pleasant experience due to the interest and engagement of participants.

The information material (magazine and films) was positively rated by participants and table facilitators. The combination of the magazine, complete and detailed but accessible, with the films,[137] captivating but accurate, ensured that all participants, irrespective of their level of education and age, or varying degrees of thoroughness in reading the magazine, were able to contribute to the discussions and vote. According to both participants and table facilitators the magazine has been a good tool to conduct informed table discussions. The films were very well received, as they were considered accessible and explanatory. They also worked well as a good kick-off for the discussions.

The result of the vote on the first evaluation question (question #106, N=180) is in line with the accounts of the table moderators. **93.3% of the participants strongly agreed or agreed with the statement "I have gained new insight by participating in the citizen summit**", higher than the average of all SurPRISE summits, but which must be read in the context of the lower knowledge of the subject and the answer to the third evaluation question (question nr. 108, N=182) was very balanced: 44.5% of the participants stated that their participation in the summit had changed their attitudes regarding security technologies (18.7% of citizens had become more positive and 25.8% had become more critical), and **51.6% of the participants stated that the summit had not changed their attitudes.**

The comparison between the results of the vote on question #6 (N=184) "Before reading the SurPRISE information booklet how would you rate your knowledge of SOSTs" and question #93 (N=186) "After watching the SurPRISE films, discussing with fellow participants and reading the information booklet how would you rate your knowledge of SOSTs" indicates that **the citizens' summit was successful in raising awareness on SOSTs.** The percentage of participants declaring to "know little to nothing" about SOSTs decreased form 35.9% at the beginning of the summit to 9.1% at the end of the summit, and the percentage of participants declaring "I have some knowledge of SOSTs but it would be useful to learn more" increased from 19.6% at the beginning of the summit to 59.1% at the end of the summit.

[136] Carlo Renda, 'Rapporto Eurispes 2014; Metà Degli Italiani Senza Orientamento Politico, Senza Fiducia Nelle Istituzioni', *L'Huffington Post,* 31 January 2014 2014.

[137] The movies can be downloaded at http://www.eui.eu/DepartmentsAndCentres/Law/SurPRISE/Index.aspx (with Italian subtitles) and http://surprise-project.eu/events/citizen-summits/ (English only).

# 4 Empirical results of the citizen summit

The citizens' summit served multiple purposes. First, it aimed to collect empirical evidence on factors influencing citizens' acceptance and acceptability of security measures, and on citizens' approach to security and privacy matters. Second, it invited citizens to play an active part in the decision-making process, by elaborating recommendations for national and European policy-makers.

To this end, citizens answered 95 questions[138] based on a theoretical model that identified variables potentially influencing citizens' choices: acceptability of surveillance oriented security technologies (SOSTs); perceived level of threat; familiarity with SOSTs; perceived effectiveness and perceived intrusiveness of SOSTs; social, temporal and spatial proximity of SOSTs; substantive privacy concerns; resistance to SOSTs; institutional trustworthiness; regulation; risk-benefit balance; and general attitudes towards technology to foster security. The theoretical model will be tested at the European level and will be the object of the comparative report of the citizens' summits.[139] While referring to the variables, this report provides first and foremost an account of Italian participants' views on privacy, security and surveillance, as results from the combination of quantitative data and qualitative information derived from the methodology used.

What made the citizens' summit distinct was that individual voting was integrated into a broader deliberative process. Voting results were collected through wireless hand-held voting equipment, which registered the votes of each participant anonymously, and allowed to project on a screen the collective voting results for each question in real-time. After a first series of general questions related to security, a short documentary film introduced the session on Deep Packet Inspection (hereafter DPI), during which citizens had the opportunity to exchange opinions by engaging in a table discussion (lasting ca. 45 minutes), before answering the following set of DPI-specific questions. The session on smartphone location tracking (hereafter SLT) followed the same pattern. During table discussions, table moderators wrote down notes in a standardized template to capture the central points made. In addition, at four randomly chosen tables minute takers took detailed notes of the discussions. After the two SOST-specific sessions, participants were allowed 50 minutes to formulate one recommendation for policy makers on the topics discussed (*infra* Annex: 10.1 Table recommendations). Finally, citizens were given the chance to write individual messages to policy makers on anonymous postcards (*infra* Annex: 10.2 Postcards)

Hence, this section summarizes the empirical results of the citizens' summit based on the replies to the 95 questions, the notes taken by the 35 table moderators, the accounts sketched by the minute takers, the 35 table recommendations and 15 postcards.

## 4.1 General attitudes on security and privacy

One of the hypotheses of the SurPRISE project is that public acceptability of SOSTs could be influenced by, on the one hand, the extent to which individuals feel in danger because they believe their personal safety or the security of the context in which they live is threatened, and, on the other hand, the extent to which people are concerned about the impact of SOSTs on their physical and information privacy. The perceived level of threat and citizens' privacy concerns were the object of a round of questions asked at the very beginning of the summit, before table discussions and the informational movies.

[138] The citizens have answered a total of 108 questions: 95 investigating the factors identified as likely to affect SOSTs acceptability, 10 demographic questions and 3 evaluation questions.

[139] The report will be available in the Fall 2014 at the page: http://surprise-project.eu/dissemination/research-results/.

Three questions, on public security (perception of security in Italy), personal security and Internet security, intended to capture general attitudes on security.

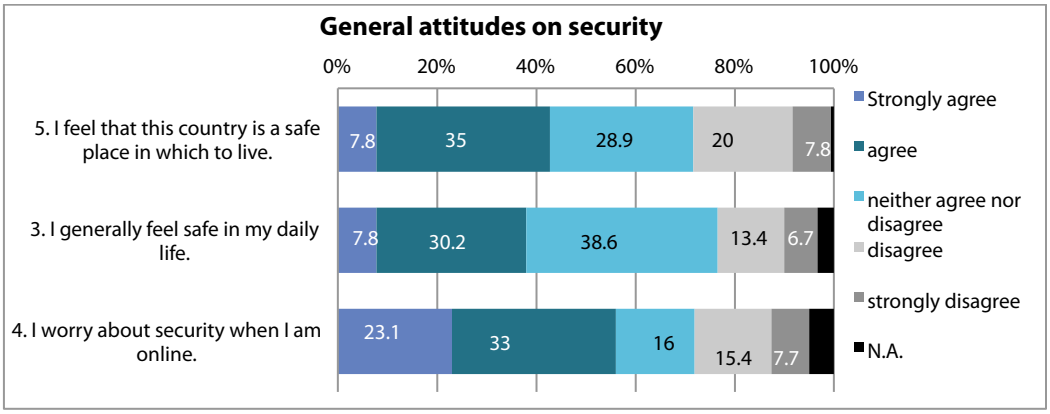



Figure 4: General attitudes on security.
Questionnaire item nr. 3 (N=179), 4 (N=182) and 5 (N=180).

Participants' perception of the level of public and personal security seems to converge/align. Less than half (ca. 40%) of the respondents considered Italy a safe place to live and stated to feel secure in their daily life. As for the statement "I feel that this country is a safe place in which to live" the share of respondents agreeing with the statement, i.e. 42.8%, is the second lowest after Hungary. The share of respondents agreeing with the statement "I generally feel safe in my daily life", i.e. 38%, is the lowest among the nine citizen summits conducted in Europe. It is remarkable that 38% of respondents chose to "neither agree nor disagree" with the same question, generating the highest value of undecided respondents compared with all other summits. As for the Internet, the majority (56.05%) of respondents declared to be concerned about security. This might relate to the level of computer literacy of the respondents.

The relevance of the subjective perception of insecurity has been confirmed by the analysis of the table discussions. Actually, security was the most widely discussed topic during table discussions. Citizens expressed a high perceived level of threat, fear, insecurity and general exposure to risks. Participants often expressed concern for the security of minors. At tables citizens expressed the desire of increased public security and community protection both at the local and national levels, a desire in line with existing studies. Italy is a country where, while the number of crimes committed (homicide, theft, pickpocketing and robbery) has been constantly decreasing since the 1990s, the perception of insecurity of the population has not decreased accordingly.[140] On the contrary, the percentage of Italians declaring to feel safe when going out alone at night in their neighbourhood has decreased from 64.6% in 2002 to 59.6% in 2009. In 2013, 31% of Italian families declared to perceive a risk connected to criminality in the area where they live, with an increase of 5 percentage points compared to 2012. The subjective perception of insecurity can thus be seen as a relevant factor in Italy, with 15 million Italians feeling unsafe in going out alone at night[141], in spite of the fact that Italy is below the European average for the number of homicides and the number of robberies perpetrated every 100 thousand inhabitants and only slightly above the European average for the number of thefts in private houses every 100 thousand residents[142].

However, the security challenge changed depending on whether participants were focussing on the national, personal, or Internet level. The most frequently mentioned challenges to public security

[140] Istituto Nazionale Di Statistica (Istat), ' Chapter 7. Security', Rapporto Bes 2013: Il Benessere Equo E Sostenibile in Italia (2013), pp. 149 – 70.

[141] Ibid. at 156.

[142] Istituto Nazionale Di Statistica (Istat), 'Noi Italia - 100 Statistics to Understand the Country We Live in, Crime and Safety', (2014). Available at: http://noi-italia.istat.it/index.php?id=6&L=1&user_100ind_pi1%5Buid_categoria%5D=09&cHash=9514867dfdb0c21d95cd527451aa89bf.

included criminality, terrorism, organized crime, trafficking, abductions and natural catastrophes. In terms of personal security, citizens mentioned emergencies, mainly of a medical nature, that could happen to themselves or to their family members. As for Internet security, citizens referred to cybercrime, identity thefts, child pornography, racist statements, viruses and attacks by hackers. The existence of differences between threats to national and individual security is in line with outcomes of previous studies. Prof. Isernia, for instance, found that people are more worried about internal security threats (rather than external ones), and that objects vary at the individual and collective level.[143]

The different connotations attached to security might explain the number of people who feel undecided about their level of personal security. The Special Eurobarometer 371[144], which investigated the public perception of internal security, can offer some insights. Italian citizens provided 15 different answers to the open question of what they considered to be the most important challenges to European citizens' security. Respondents could identify up to three challenges. The most frequently mentioned were economic and financial crises, followed by organised crime, terrorism, illegal immigration, corruption, poverty, natural disasters, environmental issues/climate change, nuclear disasters, civil wars and wars, cybercrime, insecurity of EU borders, petty crime, religious extremism and other[145]. Remarkably, at the time of the Italian citizens' summit, the unemployment rate was 12.9%, rising to 42.4% for young people.[146]

Overall, it seems that participants at the Italian summit perceived an appreciable level of security threat, in particular when browsing on the Internet, then at the personal level, and finally for public security. It must be noted, however, that table discussions reveal awareness of the possible misapplication of the concept of "national security". The opinion that the notion could be used as an excuse to develop mechanisms of social control, to advance economic interests, and the idea that abuses could be committed in the name of national security was recorded at some tables. In addition, citizens admitted that lay people might not be able to objectively evaluate the level of threat presented to them by politicians and the media. While security has to be guaranteed, the promise of an increased security should not be used to influence public opinion. Citizens also raised the question as to whether increased public security would translate into higher personal security.

General attitudes on privacy were investigated through questions on the relation between SOSTs and privacy. Citizens were asked to reflect on privacy in general, and their personal privacy, both at the beginning and at the end of the citizens' summit.

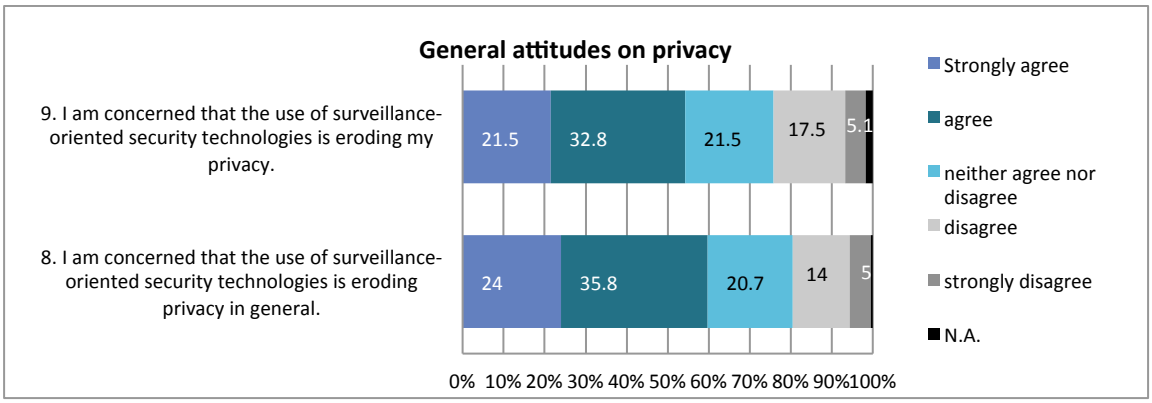



Figure 5: General attitudes on privacy *at the beginning* of the citizens' summit.

[143] Pierangelo Isernia, *Dove Gli Angeli Non Mettono Piede. Opinion Pubblica E Politiche Di Sicurezza in Italia*, (1996).

[144] European Commission, 'Special Eurobarometer 371 - Internal -Security. Italian Factsheet', (2011a).http://ec.europa.eu/public_opinion/archives/ebs/ebs_371_fact_it_it.pdf.

[145] Ibid.

[146] N/A, 'Istat, Nuovo Record Per La Disoccupazione: A Gennaio Il Tasso Balza Al 12,9 Per Cento', *La Repubblica,* 28 February 2014 2014a.

At the beginning of the citizens' summit, public and personal privacy attitudes converged. Nearly 60% (59.77%) of participants feared that the use of SOSTs is eroding privacy in general and 54.24% feared that the use of SOSTs is eroding their personal privacy. **The data show that the majority of participants perceive that SOSTs have an impact on their personal privacy, and that an increasing use of ICTs leads to an erosion of citizens' privacy in general**.

This result is consistent with the outcome of special Eurobarometer survey 359 on Data Protection and Electronic Identity[147]. While 80% of the surveyed Italian population agreed that disclosing personal information is an increasing part of modern life, and 76% agreed that the government of their country asks them for more and more personal information, 58% claimed that disclosing personal information is a big problem for them.

Privacy was the second mostly debated topic after security. Participants attached to privacy many meanings (in line with the comprehensive scope of the rights to respect for private and family life and the protection of personal data). Concepts mentioned included: banking information, medical data, reserved documents and commercial secrets; personal devices, passwords and communications; pictures; consent; data storage; private life, personal movements, control over one's personality and reputation; political beliefs and party affiliation, religion and sexual orientation.

**Statements about SOSTs causing a restriction, violation or erosion of privacy were recurrent at tables**. The erosion was qualified both as an intrusive and non-regulated access to personal data and as an intrusion into citizens' private life, in accordance with the meaning denoted by the concept of privacy.

Citizens mentioned external threats (such as intrusion, abuses, use of data for secondary purposes, commercial gains), risks tied to an inadequate legal framework (legal grey areas, lack of judicial control), threats related to a lack of transparency on the part of public and private agencies (profiling, disrespect of consent, a false feeling of choice), and dangers caused by individuals' lack of responsibility (when using devices and social networks, in disclosing data, especially for underestimating the value of one's information or being unaware of the risks). Participants reported the risk of limiting one's action and feeling uneasy. **Some raised the question as to whether convenience should be paid by eroding privacy (with both positive and negative replies).** One table reported the importance of cultural sensitivities, another the fact that higher trust in institutions translated into an increased availability to disclose one's data.

## 4.2 How do participants perceive the use of SOSTs?

The Italian summit featured Deep Packet Inspection (DPI)[148] and Smartphone Location Tracking (SLT) as practical examples of SOSTs. **The focus on SOSTs did not intend to capture citizens' evaluation of DPI and SLT, but rather allowed citizens to express their attitudes on surveillance technologies, security and privacy in context, by making reference to real-life situations.**

### 4.2.1 Familiarity with DPI and SLT

To begin with, two questions investigated familiarity of respondents with the two SOSTs. The first concerned awareness of the SOSTs: 50% of participants declared to know what DPI is, while a remarkable 79% declared to know what SLT is. The second concerned exposure to SOSTs in participants' daily life, with 78% of the citizens declaring to use the Internet often/all the time, and 80% declaring to use mobile phones or smartphones often/all the time. **Thus, participants showed more familiarity with smartphone location tracking than with deep packet inspection**.

Table discussions prove useful in explaining why this is the case. Unlike DPI, SLT is a technology that citizens can make active use of, and which proves useful in many situations of daily life, from keeping in touch and localizing children, through moving around traffic and travelling, to finding services. Many participants described it as useful in wider contexts (e.g. tracking goods, controlling the use of the many

[147] European Commission, 'Special Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union', (2011b).

[148] DPI was debated in the morning session, to allow more time for discussion if needed, given that the Italian public might have been less familiar with DPI as opposed to SLT.

state cars made available to politicians, supporting tourism), and crucial in situations of emergency (natural disasters, accidents, kidnappings). On the other hand, most participants could not identify advantages of DPI beyond security, besides online ads and the reduction of spamming (with dubious results). Some acknowledged it is useful to fight viruses, raising the question as to what "online security" means to different citizens.

### 4.2.2 Perceived effectiveness

After having shown the information film, each SOST-specific session featured a round of questions on SOSTs' perceived effectiveness and intrusiveness (asked before and after table discussions). Perceived effectiveness was measured in terms of SOST's efficacy in achieving a security goal, increasing personal safety, addressing a real threat.

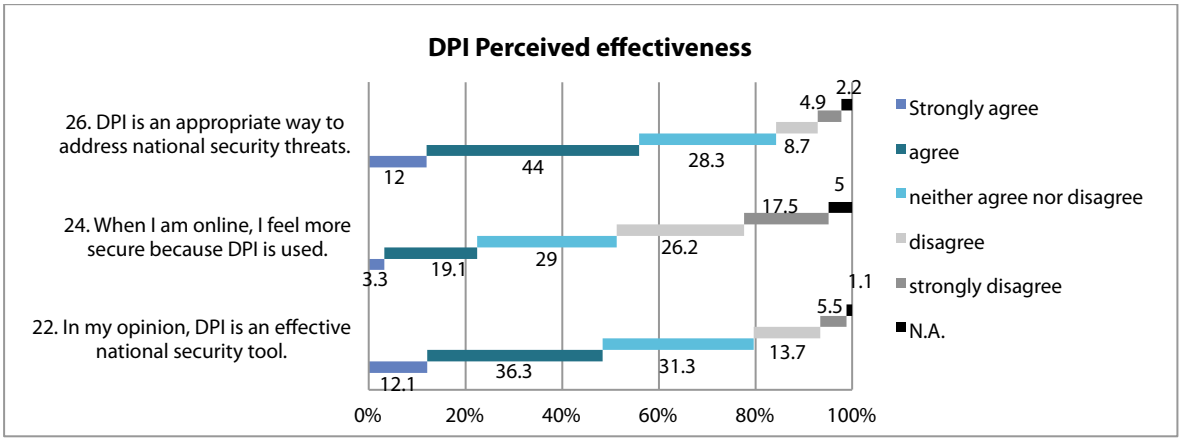



Figure 6: Perceived effectiveness of DPI

**DPI was an effective national security tool for 48% of respondents, while SLT was considered effective by 62% of respondents**. Casting the vote seemed easier in the case of SLT, resulting in 22% of undecided, than in the case of DPI, with 31% of undecided.

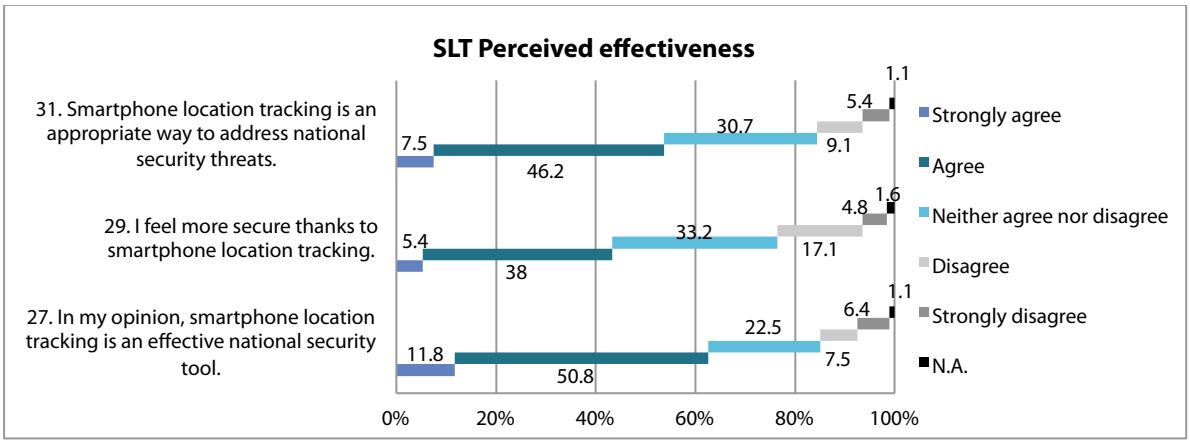



Figure 7: Smartphone Location Tracking perceived effectiveness

Table discussions provide insight into such uncertainty. One table explicitly raised the question of SOST's real efficacy, and a few whether the instrument is adequate (but no specific threat was used to measure adequacy). Some participants lamented the lack of data to buttress SOSTs' promise of increased security. Another issue discussed was the possibility of circumventing SOSTs, in line with the adage whereby "crime is always a step ahead", especially with reference to SLT. Some participants noted

that more control does not equal increased security. Some doubted DPI because the phenomena it is supposed to fight are widespread, and it might be too broad a filter to sieve relevant information.

Participants drew a clear difference in terms of the extent to which SOSTs can lead to an increase in personal safety: 43.32% of respondents argued they felt more secure thanks to SLT, while only 22.41% agreed with the same statement for DPI. Nonetheless, both SOSTs were considered similarly appropriate tools to address national security, with 55.98% supporting the use of DPI, and 53.77% approving the use of SLT.

The fact that SLT is clearly associated with increased personal safety may be determining the more favourable approach than DPI. The perceived increase in personal safety, however, does not seem to influence the suitability of a SOST in addressing national security threats, as the vote on this questionnaire item for DPI and SLT converges**. Keeping in mind the ambiguous nature of security, there might be a gap between personal and national security** (see *supra*, section 4.1). **Citizens have a greater degree of control over personal rather than national security, identified by some as a vague concept, which is in line with Italy's historical lack of transparency regarding its public security policies.**

### 4.2.3 Perceived intrusiveness

Perceived intrusiveness was measured through the extent to which SOSTs encroach on peoples' personal sphere in terms of risk of privacy intrusiveness, human rights infringement and embarrassment.

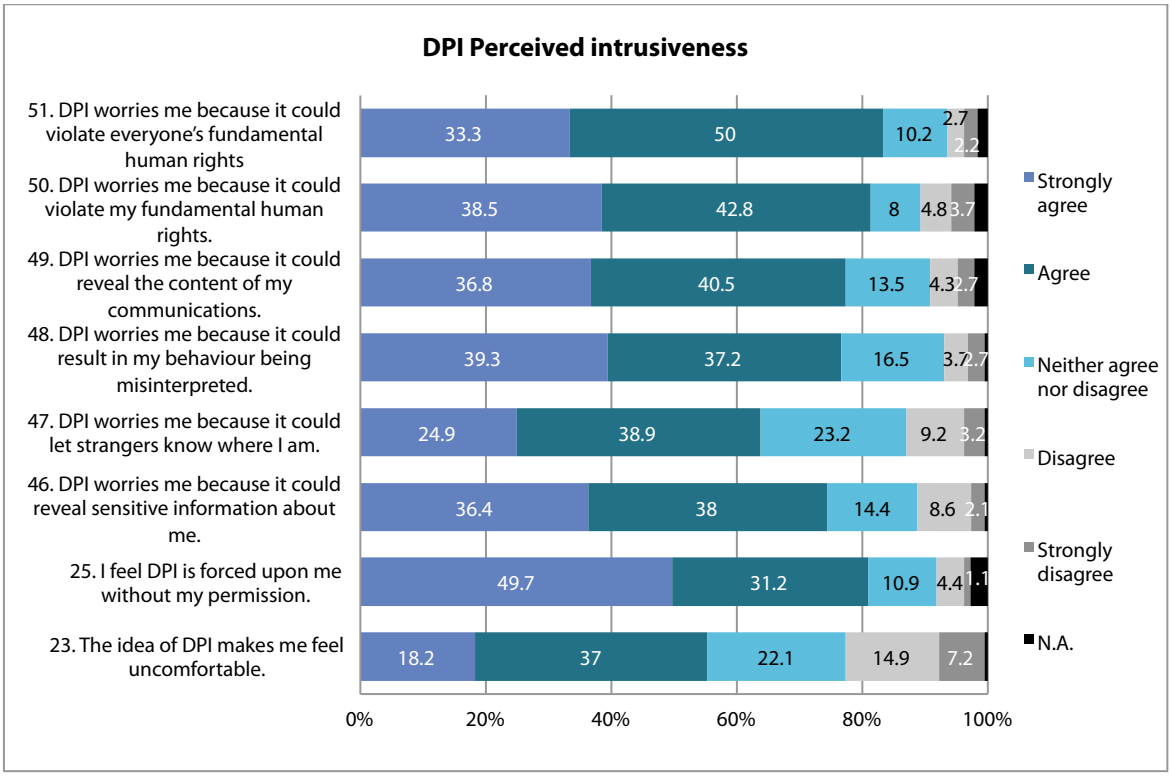



Figure 8: DPI perceived intrusiveness

**Citizens clearly perceive DPI as intrusive**. They were first and foremost concerned about human rights infringement, for everyone's (83.3%) and for themselves (81.28%). Subsequently participants worried about the stealthy nature of DPI (80.88% agreed), which deprives them of control and empties consent. People worried substantially about DPI's ability to encroach upon several dimensions of privacy, namely the fact that DPI could:

- Reveal the content of personal communications (77.3% were concerned, compared to 80% in Europe and 92 % in Spain);
- Result in the misinterpretation of an individual's behaviour (76.59%);
- Reveal personal sensitive information (74.33%); and
- Let strangers know where a person is (63.78%).

Finally, a slight majority of participants agreed DPI provokes embarrassment and unease (55.25%).

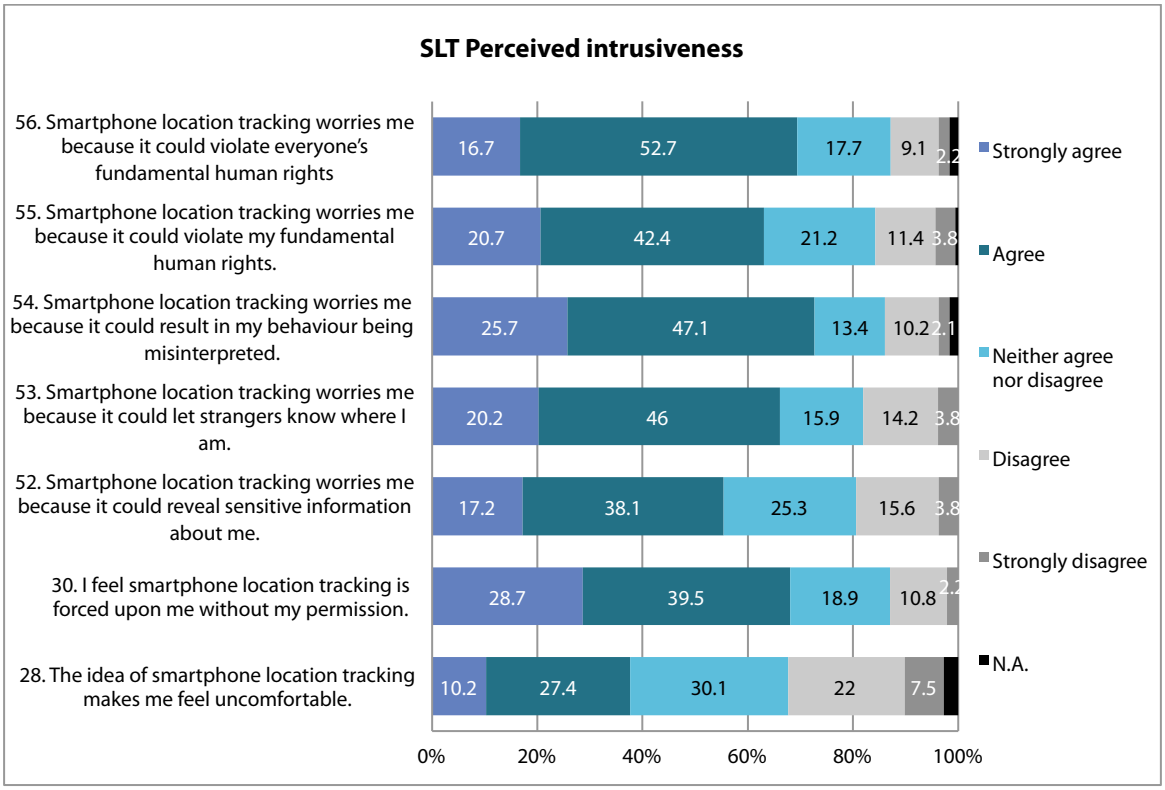



Figure 9: Smartphone Location Tracking perceived intrusiveness

**Although SLT is not considered to be as problematic as DPI, the majority of respondents still consider it intrusive**. The most worrying feature identified by voters is that SLT could result in the misinterpretation of an individual's behaviour. The rate of participants showing concern (72.73%) is similar to that of Germany and Denmark's citizen summits, six percentage points above the European average. As for SLT's impact on other facets of privacy, citizens expressed concern for:

The fact that SLT could let strangers know a person's position (66.12%, in line with the European average);

The fact that DPI could reveal personal sensitive information (55.3%).

SLT's potential capability to infringe human rights ranked second among participant's worries (69.36%); the fear for participants' personal rights is 6 percent point lower. Third, participants expressed fear because of the imposition of SLT upon people (68.11%). Only 37.64% of respondents felt to be embarrassed and uneasy because of SLT, but a third claimed to be undecided.

**Overall, the majority of citizens considered SOSTs as intrusive, almost irrespectively of the technology taken into consideration**. This result is consistent with the concern over personal and public privacy clearly expressed by respondents when asked about their general attitudes on privacy by means of questionnaire items n. 8 and n. 9. **In the case of both DPI and SLT, worry is first and foremost tied to concerns for human rights infringement and privacy intrusiveness.** During table discussions, many participants noted how SOSTs affect human rights and freedoms, such as to manifest, of association, of religion. A few tables featured discussions on the impact of SOSTs on democracy, too. While many noted that the biggest challenge relates to the use of SOSTs by dictatorships (some participants brought up the case of north Africa), many admitted that SOSTs give great powers to governments, and that this could pave the way to future restrictions of democratic life. **Some raised the question as to what would have happened if SOSTs had been available during fascism.**

**However, there seem to be SOST-specific concerns, too. The second most important reason to fear DPI is its covert nature.** At the moment, the average Internet users are unable to "switch-off" DPI. The covert nature of SLT might not have been as worrying, possibly because of the existence, in Europe, of such a switch (enabling to turn off the GPS and the Wi-Fi), as noted during table discussions (with very few contrary opinions, due to phone masts' capability to track phones regardless of GPS). Due to its practical use, its greater transparency, and the fact that data are not immediately available to security forces, SLT is seen as friendlier. This may also explain the reason why SLT was seen as being less worrying for individual human rights than DPI (whose practical uses are questioned). Also, some participants expressed that content is more private than location (in few but interesting cases, participants said SOSTs do not worry them as much as interception, thus not associating DPI with interception). **At the same time, however, SLT's second most feared feature is the fact that it could lead to misinterpret peoples' behaviour, leading to adverse decisions.** Some participants, for instance, gave the example of finding themselves near a violent street protest, and being wrongly accused of other people's misdeeds.

### 4.2.4 Trading privacy with security (with reference to DPI and SLT)

Towards the end of each SOST-specific session, a questionnaire item tried to understand how participants' views about the intrusiveness of a technology (DPI or SLT) relate to their views about the usefulness of the same technology for security.

Both technologies are considered useful rather than useless, and SLT is considered more useful than DPI (76.9% of respondents considered DPI overall useful compared with 91.9% for SLT). However, both SOSTs were labelled as "useful but highly intrusive" by the majority of participants, 64% for DPI and 59% for SLT (considered as "useful and not very intrusive" only by a third of respondents). 79.04% of respondents chose the options that qualified DPI as highly intrusive and 64.32% of respondents chose the options that qualified smartphone location tracking as highly intrusive.

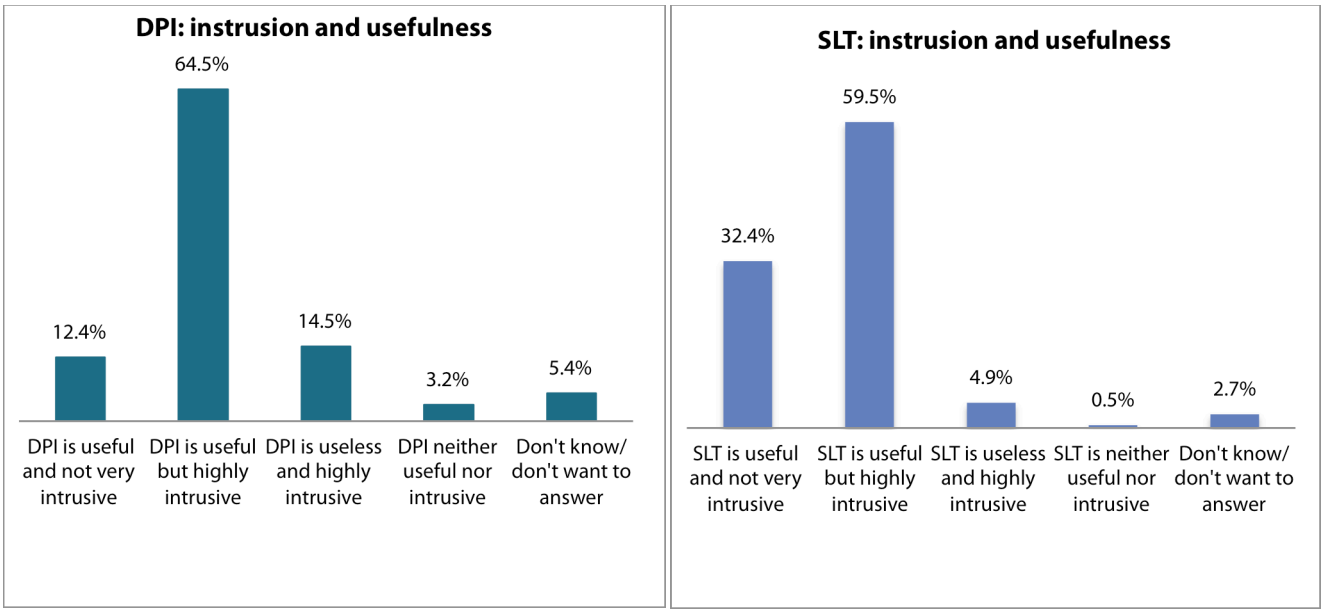



Figure 10: DPI and Smartphone Location Tracking are useful but highly intrusive

**Table discussions provide further insight into the reason why SOSTs were considered intrusive.** Citizens fear that data collected through SOSTs could be used by criminals (e.g. to control one's position, to stalk, or for identity theft, hackers). Pharmaceutical companies, and employers, may want to access personal information. Others worried that the content of their communications could be changed, and information forged. Some argued that the use of SOSTs reduces humans' mental capability. Others worry for children and the "memory" of the Internet.

**In synthesis, the majority of Italian respondents highlighted that DPI and SLT are harmful technologies, in spite of the benefits they can bring.** This result does not, however, mean that citizens are prepared to trade privacy for security, which depends on the acceptance and acceptability of the specific SOSTs, and the consent of citizens to give in privacy. The trade-off was discussed at many tables, and participants seemed to split equally between those thinking that intrusion into privacy is inevitable, and those thinking that, in order to enjoy security or the convenience of SOSTs, we cannot pay by giving up privacy. Moderators reported that some vouched explicitly against the trade-off, saying that privacy is as important as security.

Those results, in fact, must be crossed with the citizens' willingness to support SOSTs as a tool for national security, as asked of citizens at the end of every SOST-specific session. **The majority of participants agreed with the use of DPI (55%) and SLT (70%) as a national security measure. Support increased when compared with the perceived level of effectiveness and the utility to implement national security.** This is consistent with the general increase in the approval of SOSTs registered at the end of the summit (see *infra*, section 4.4).

**The result might suggest that the more citizens approve of technology in general, the more likely they are to perceive a particular SOST to be effective.**

**Only slightly more than a third are prepared to support the adoption of a technology they consider intrusive**. When crossing the responses of peoples' opinion on the usefulness/intrusiveness nexus of SOSTs, and acceptance of the SOST for national security, 37% of respondents appear to accept the fact that the technology comes with a cost to privacy in the case of DPI, and 38% would do the same in case of SLT.

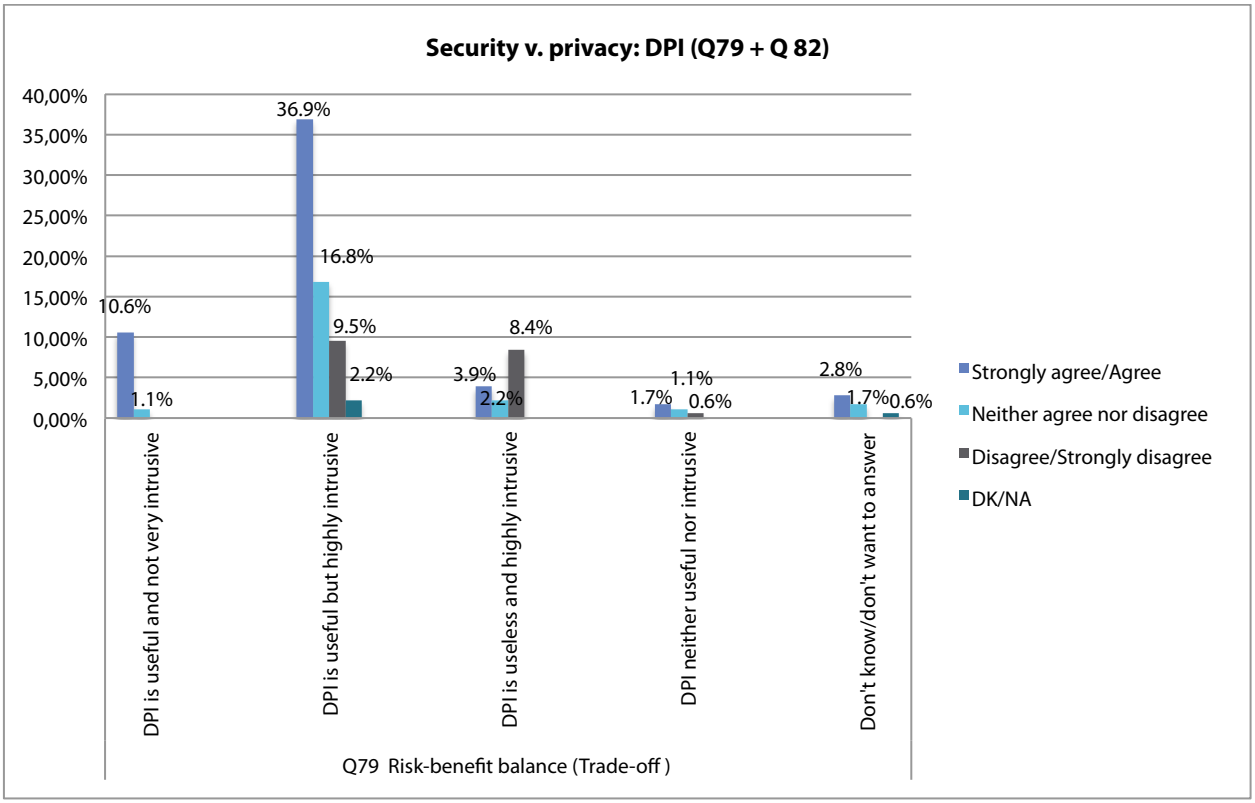



Figure 11: Q79 Risk-benefit balance (Trade-off)

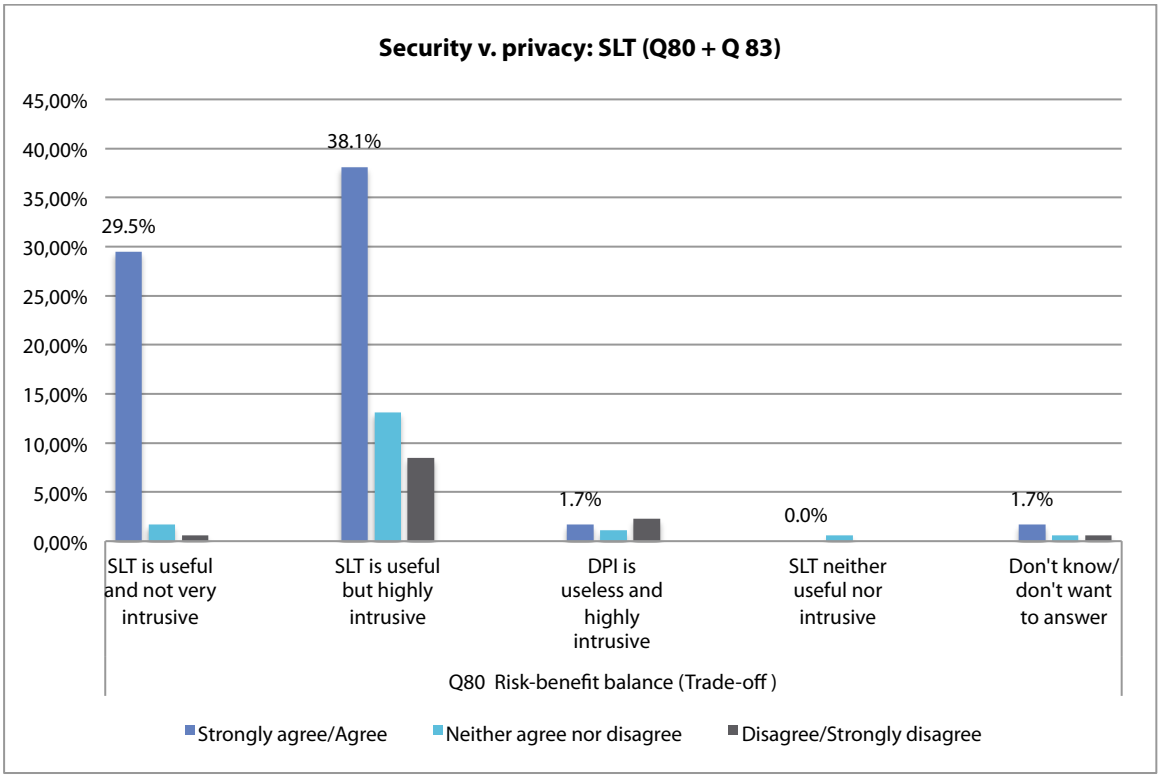



Figure 12: Security v. privacy: SLT (Q80 + Q 83)

These findings suggest two possible interpretations requiring further investigation. On the one hand, we might conclude that one third of participants are ready to trade privacy with security. On the other hand, the conclusion may also be that participants do not feel they have a real choice in the matter, but must adapt to privacy intrusions decided by others in the name of security, and therefore are not in a position to decide whether they would accept the trade-off.

## 4.3 Is fighting or fleeing surveillance an option?

Participants were further asked the extent to which they would oppose or avoid SOSTs. The majority of participants stated that they would like to find out more about how to protect themselves when using both DPI (60%) and SLT (62%), but expressed little support to other forms of opposition to surveillance technologies (questions n. 58 and 59). The majority of respondents (59%) indicated that they would not change their behaviour because of DPI, but a third stated that they would. In the case of SLT, only 15% of voters were prepared to change behaviour, whereas 73% would not act differently.

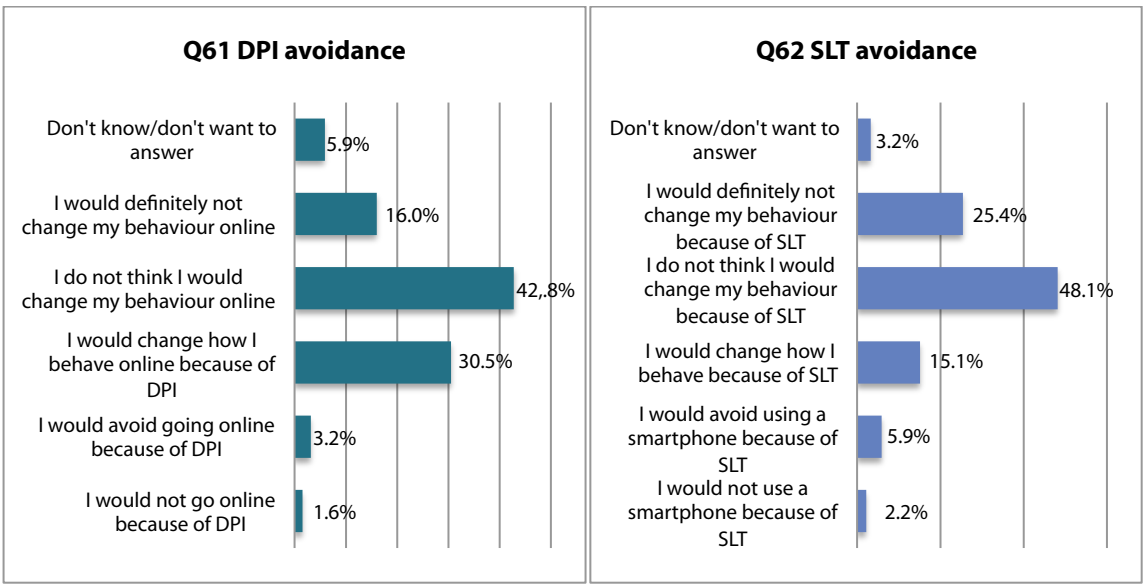



Figure 13: Change of behaviour because of DPI and smartphone location tracking

Such results, taken together, are consistent with the opinion expressed by 80% of the Italians involved in the Eurobarometer survey on Data Protection and Electronic Identity[149]: **disclosing personal information is seen as an increasing part of modern life.** This is reflected in table discussions. Most participants agreed on the importance of technology, and noted that avoiding SOSTs is not an option, as it would cut them off from their social life; however, they recognized the risks and the ensuing feeling of powerlessness. **Reactions to this state of affairs, however, varied. On the one hand, some participants showed defeatism**, saying that risks must be accepted; others challenged the idea of blocking technological development. Some claimed that surveillance always existed, but simply that control increased (although admitting it is now more invasive). Many avowed they found it difficult to understand when SOSTs intrude on privacy. **On the other hand, participants reacted by demanding adequate information on SOSTs**, so that citizens can take conscious decisions, and express valuable consent (or rather protect themselves). Some called for a suitable legal framework, or a technologically rooted solution that would address the problem of law becoming quickly obsolete (regulate by code). It was also proposed to conduct more research.

[149] European Commission (2011b).

## 4.4 Italian citizens accept SOSTs (in general), but worry about privacy and future developments

At the beginning of the citizen summit 52% of participants agreed with the regular use of SOSTs to improve national security (in line with the European average), while 24% disagreed and 22% expressed uncertainty. The same question was asked again at the end of the summit, and the figure had increased to 68%, almost ten percentage points higher that the average in Europe (but it must be kept in mind that participants at the Italian summits declared to have learnt a great deal, and acceptance might be linked to a better understanding of the technology).

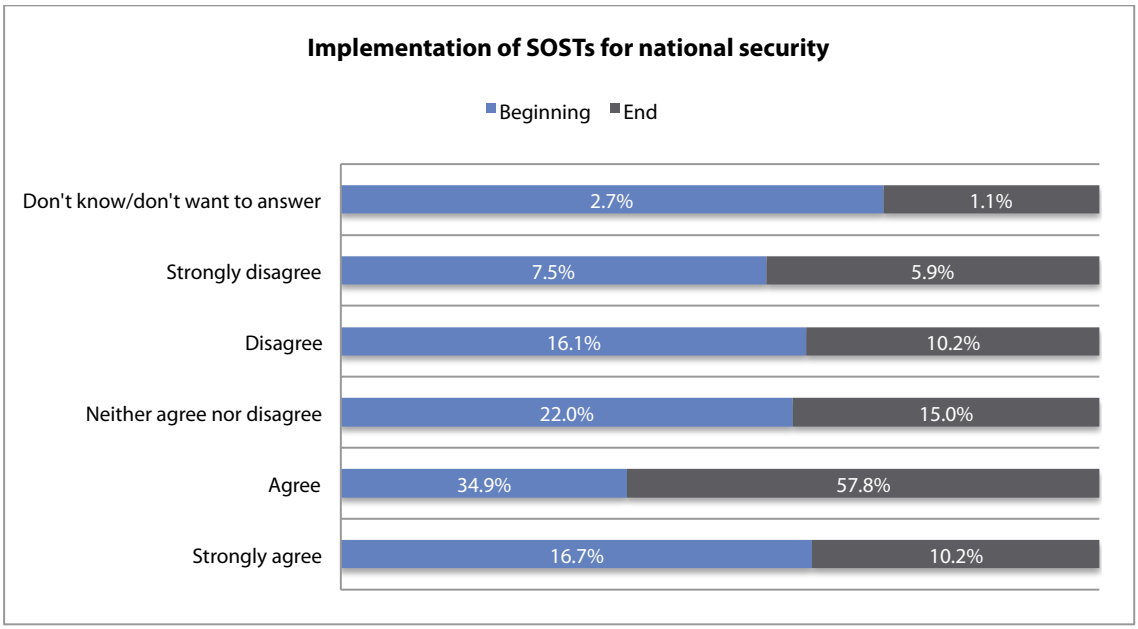



Figure 14: Overall I believe surveillance-oriented security technologies should be routinely implemented to improve national security (Percentages)

The result shows that, in Italy, people clearly support the use of SOSTs to foster public security, even if this means being exposed to surveillance, but their support is surrounded by a degree of diffidence higher than in other European countries. Two more questions confirmed such positive belief regarding the ability of technology to enhance security, while another three channelled diffidence. While 79% of respondents agreed that the use of SOSTs improves national security (compared to 64% on average in Europe), and 63% of respondents agree that if a SOST is available national governments might as well make use of it (in line with the European average), opinions on the item "SOSTs are only used to show that something is being done to fight crime" are divided, with 32% agreeing and 37% disagreeing with the statement (50% on average in Europe).

Likewise, opinions on the item "If you have done nothing wrong you do not have to worry about surveillance-oriented security technologies" are divided, with 43% agreeing (compared to 37% in Europe) and 43% disagreeing with the sentence, as reflected by table discussions. When asked about the possibility of abuse connected with the use of SOSTs, a great majority of participants (82%) could envisage abuses (10 percentage points higher than the European average).

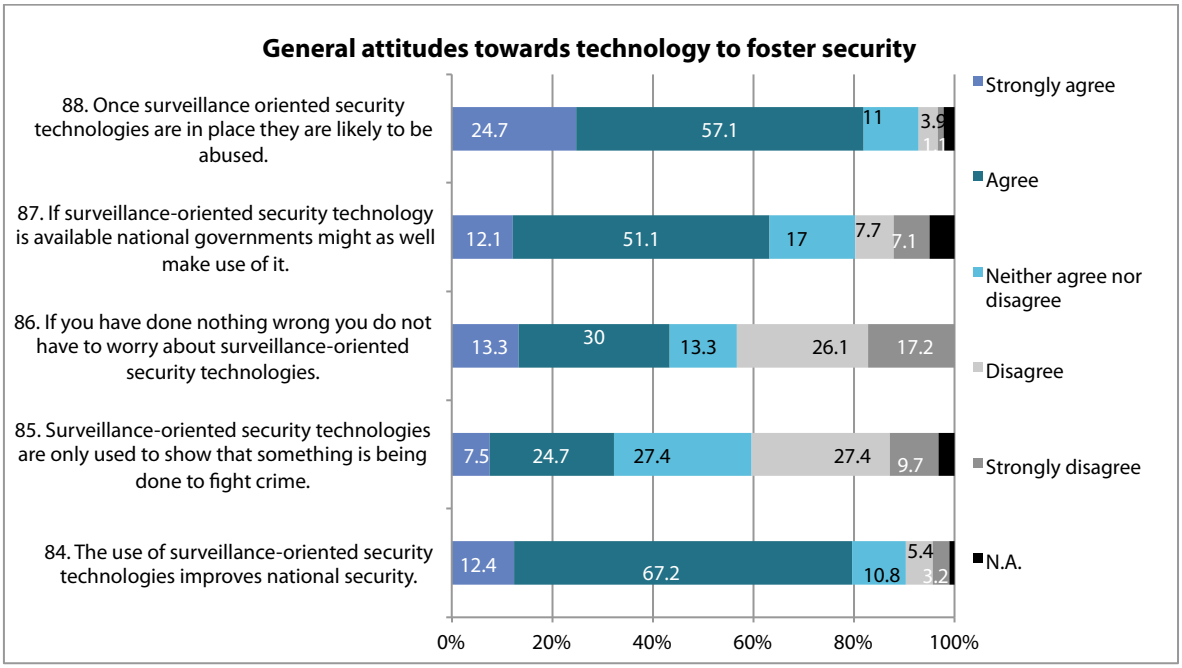



Figure 15: General attitudes toward technology to foster security

The results are challenging. Respondents favour the general use of SOSTs by governments if available, as they believe they can improve national security. However, acceptance is overshadowed by doubts and skepticism, due to the fear of abuses of power, the uncertainty about the real effectiveness of SOSTs in countering security challenges, and the rejection of the "nothing to hide" attitude (as well as the trade-off).

Earlier we discussed the uncertainty as to the effectiveness of SOSTs. The fear of abuse seems to be strongly connected with the opacity reported in most tables. Citizens could not exclude abuses, because of the general lack of transparency concerning who produces SOSTs, who collects the data, how data are used and what legislation applies. Requests of increased transparency, leading to more knowledge, abounded. Some participants insisted on the need to have appropriate regulation. Others insisted on the need for vendors to inform citizens at the time they buy devices, or mass media to inform citizens. Another suggestion concerned publishing reports on the use of data. **A moderator noted that participants believed that the summit they were taking part in was already a step forward, as many reported during breaks directly to us**. Some raised the question of how to hold institutions accountable in case of false positives and false negatives. Informed consent featured strongly here, too.

One third of the tables reported some citizens discussed the common phrase "if you have nothing to hide, you have nothing to fear". It seemed a third of the tables accepted the reasoning and thus surveillance, in line with the vote on trade-off (but more analysis on data must be performed in order to confirm this interpretation). Part of the citizens seemed to accept control more easily, as they do not believe themselves to be under surveillance, "because of their humble lives". A few noted that innocents should not be controlled (even by mistake, e.g. if a felon uses on purpose their device to commit a crime). Some said that SOSTs are a double-edge sword, in that they might be harmful, but they could also be used for self-defence.

### 4.4.1 Participants worry about future developments …

Another challenge to generalized acceptance of the use of SOSTs to foster security comes from the fear of future developments expressed by citizens. 72% of respondents declared to be worried about how the use of DPI could develop in the future and 53% expressed the same concern for SLT. The difference comes mainly from a higher percentage of undecided in the case of SLT. The item appeared in table discussions, too. Future developments were either not qualified, or couched in terms of employers using such powers to control workers.

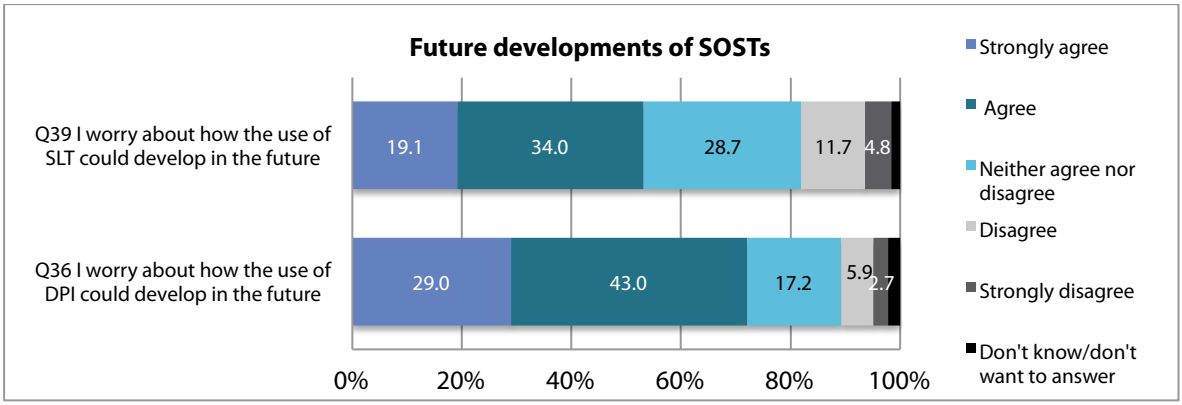



Figure 16: Future developments of SOSTs

### 4.4.2 … and about privacy as a right valuable for the collectivity

In addition, citizens expressed strong concerns about their informational privacy. The dimension of informational privacy that mostly concerns citizens (90%) was the possibility of disclosing their data (Q 91) without permission, in line with the average from all other summits. Two-thirds (78%) were concerned that information held about them might be inaccurate, and that their personal information might be used against them, showing a widely shared concern about errors in the processing of information and use of personal data for secondary purposes, to a stronger extent than in other countries (69%). Finally, 63% of respondents expressed concern for the excessive information collected about them.

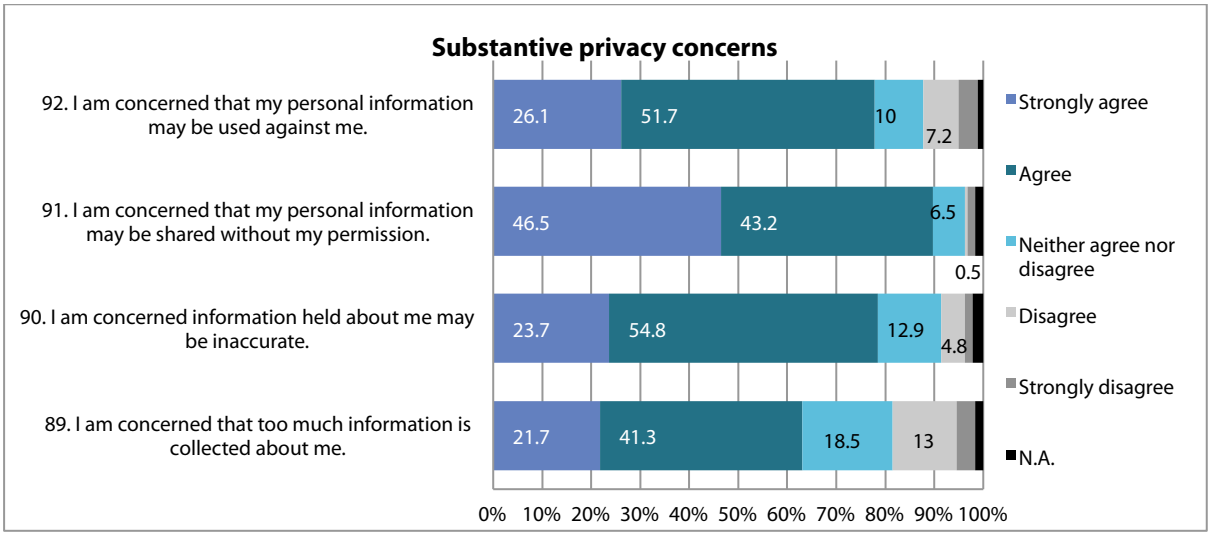



Figure 17: Substantive privacy concerns

Citizens were asked twice whether they were differently worried about the intrusion of SOSTs into privacy as a human right, and into their own individual privacy, once at the beginning of the summit (see *supra*, section 3.1), and once at the end. The concern grew; respondents were more worried about privacy in general (72% compared to the initial 59.77%) than about their individual privacy (65% compared to the initial 54.24%,). Both final outcomes are aligned with the European average. **The more citizens perceive SOSTs to be intrusive, the more they are concerned about their privacy**. **The outcome is interesting, as citizens became more supportive of SOSTs in general, too. A factor could be the increased knowledge of participants, who appreciated better both pros and cons of SOSTs.**

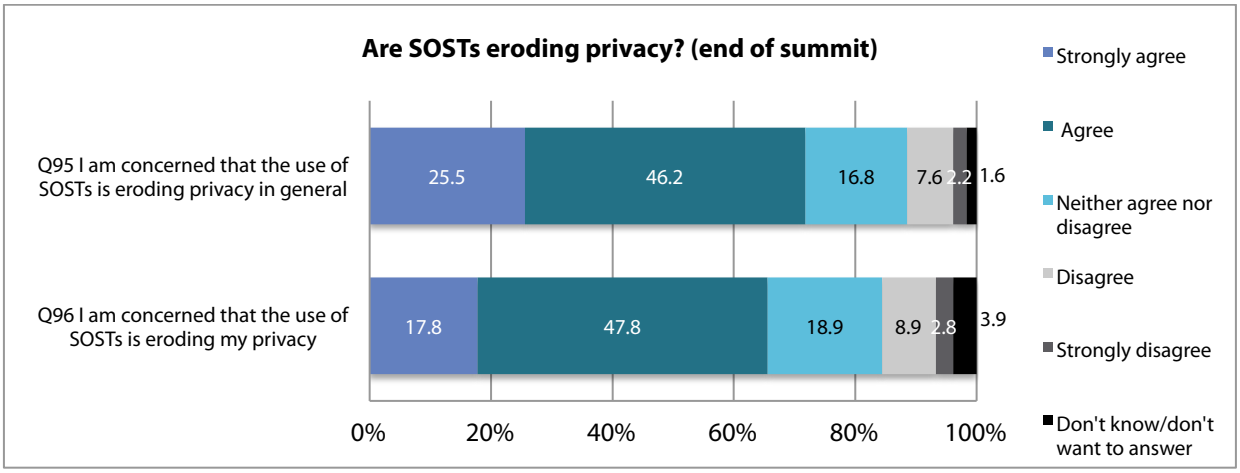



Figure 18: General attitudes on privacy at the end of the summit

By combining this result with the one on the item "If you have done nothing wrong you do not have to worry about surveillance-oriented security technologies" (43% agreeing and 43% disagreeing), the impression is that the idea that citizens do not think of privacy from a purely individual perspective can be extended from privacy concerns to matters of security and surveillance.

It is interesting to note that the idea that DPI and SLT are disturbing only when they have a direct effect on the privacy of their own communications and personal data, as expressed at some tables, does not find wide consensus. When asked whether a SOST "only bothers me if it is used to track my online activities", the case of DPI resulted in 43% agreeing with the statement, and 31.5% disagreeing (21% undecided), while in the case of SLT, the respondents disagreeing with the statement, i.e. 44%, outnumbered the respondents agreeing with the statement, i.e. 36% (19% remained undecided).

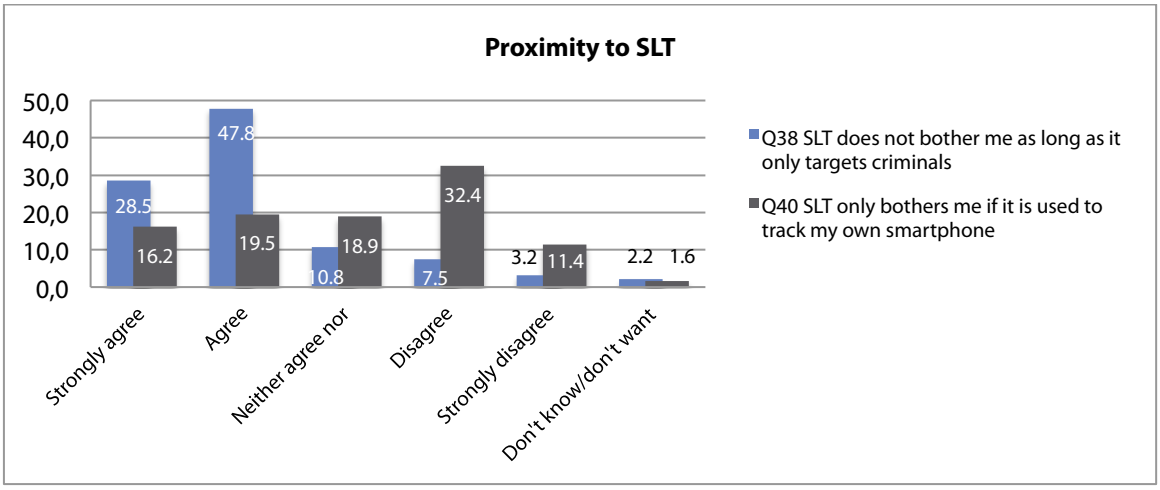



Figure 19: Social proximity compared in the case of SLT

Responses change for the item "DPI/smartphone location tracking does not bother me as long as it only targets criminals". It resulted in 80.6% of respondents agreeing with the statement for DPI and 76.3% of respondents agreeing for smartphone location tracking. The result might stand in contradiction with the previous one, but it could also be read as **an acceptance of SOSTs as long as they are accurate in targeting criminals and not screening the entire population**. Table discussions provide additional insight, as some underlined that SOSTs should be used to fight criminals, rather than control citizens. However, a minority raised the issue of how to define a criminal. Some raised the fear that it might be necessary to check everyone before the criminal is found, or that innocent people might be checked by mistake.

## 4.5 Trust in security authorities and regulation: an important explanatory factor

The extent to which institutions using SOSTs are considered trustworthy was analysed by looking into three dimensions: ability (whether the institution is perceived to be able to do what it sets out to do), benevolence (whether the institution is perceived to be concerned about welfare and integrity) and integrity (whether the institution is perceived to act in good faith). A first question asked about trustworthiness of security agencies responsible for the use of SOSTs in general. Had there been only this question, the impression would have been of a fairly high level of trust in security agencies, as the clear majority of respondents (61% in the case of DPI and 59% in the case of SLT) indicated that security agencies look trustworthy to them. However, the results of the votes on the different dimensions of institutional trustworthiness painted a different picture. Looking into DPI first, 40% of participants agreed that security agencies are competent at what they do (and within this result, only 3% strongly agreed), but 33% were undecided and 16% disagreed. For SLT, over a third of participants (34%) agreed that security agencies are competent at what they do (and within this result, only 2.15% strongly agreed), but 39% were undecided and 14% disagreed.

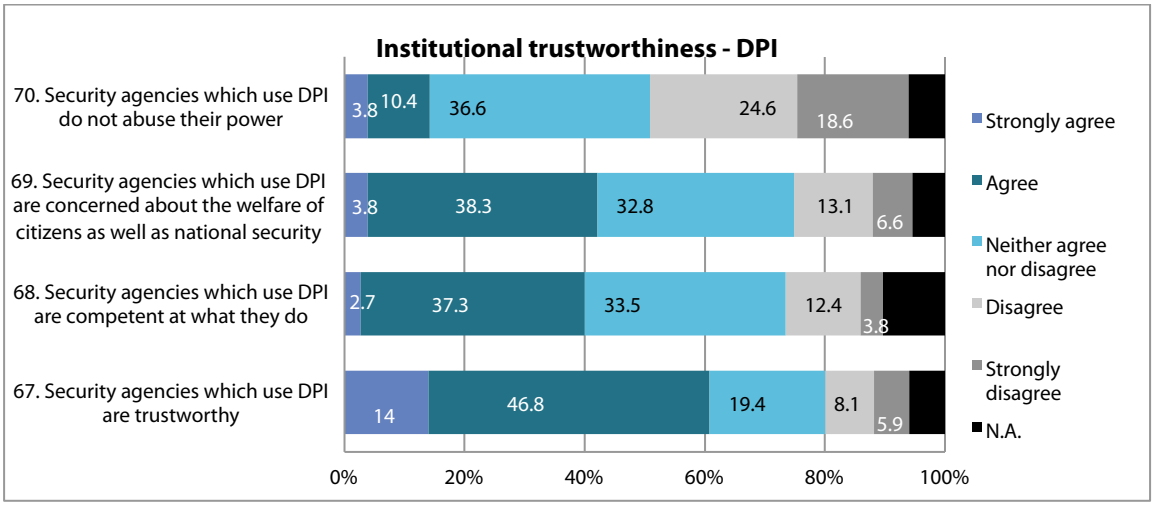



Figure 20: Institutional trustworthiness – DPI

As to whether institutions are concerned about the welfare of the citizens, 42.08% of respondents agreed that this is the case for DPI, and 51.72% agreed that this is the case for SLT. About a third of the sample remained undecided in both cases. Confirming citizens' attitude on possible abuses of power, only 14.21% of respondents agreed that security agencies using DPI do not abuse their power, and only 20.43% of respondents agreed that security agencies that use SLT do not abuse their power. The rate of undecided reached ca. 40%. **There seem to be a great degree of uncertainty when it comes to trusting institutions using SOSTs, and for some specific questions the balance is tilted towards lack of trust.**

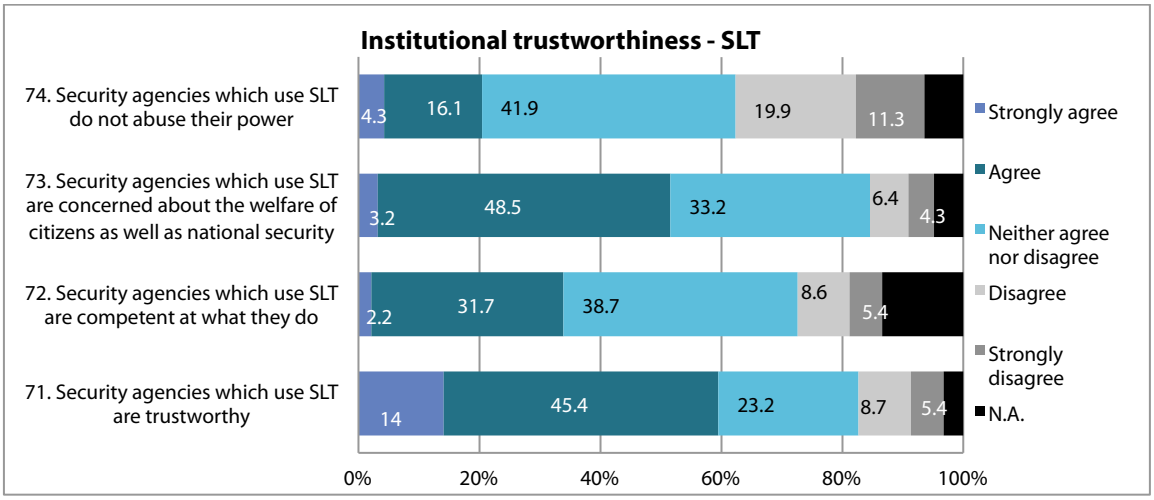



Figure 21: Institutional trustworthiness - SLT

The lack of transparency we referred to many times seems to be particularly relevant here. Table discussions provide additional insight. Citizens, in fact, drew a clear line between security institutions and commercial actors. While some expressed support for the use of SOSTs by public institutions overseeing security, a few expressing explicit trust (and noting that mistakes can happen with all forensics), all comments converged towards criticizing the use of data by commercial actors. The citizens' summit did not contain questions on the processing of data by private companies, yet the subject was constantly raised. **The vast majority of participants expressed unease and disagreement with the use of the data collected from SOSTs for commercial purposes**. Reasons related to the risks inherent in SOSTs and the context (lack of control, possibility of abuses). In any case, the general feeling was one of uncertainty and perplexity. Many wondered about the uses of data given the lack of transparency (as participants expressed loudly even when they were voting!). Some questioned whether there is a definition of "suspect", others whether security forces are properly trained for the job.

Another aspect taken into account was the perception on the effectiveness of laws and regulations in ensuring that SOSTs are used in a lawful way and not abused or misused. Citizens' opinions were captured through a questionnaire item that included options on the effectiveness of laws and regulations, the role of DPI or SLT in improving national security, a final opinion on the intrusiveness of the two SOSTs and, again, the possibility of framing acceptability of a SOST through a trade-off framework.

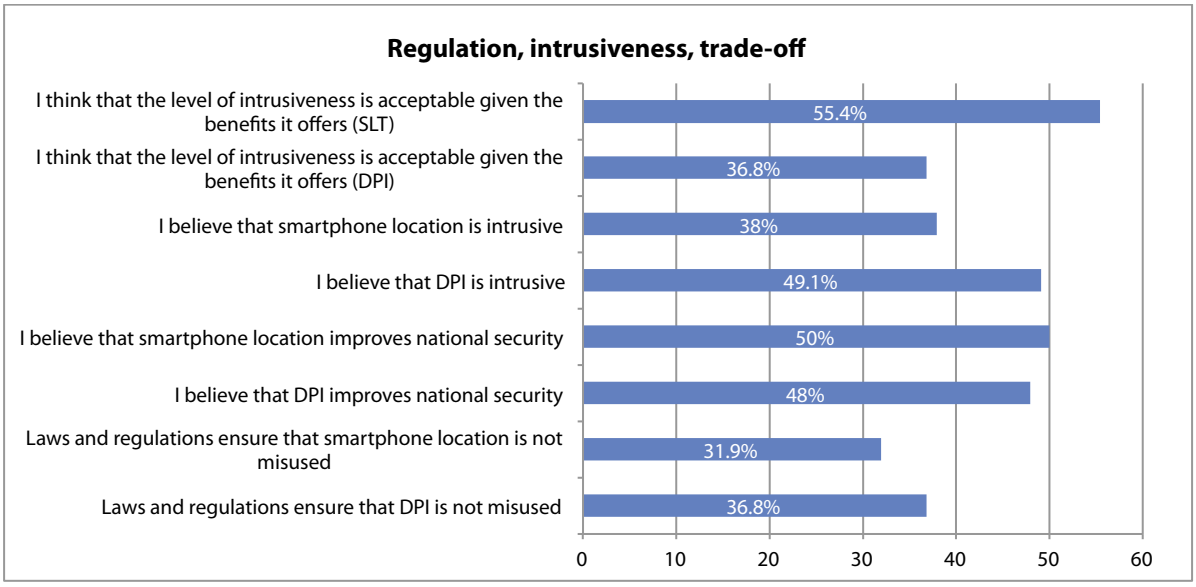



Figure 22: Regulation, intrusiveness, trade-off

This time citizens could select up to four options. Respondents showed uncertainty as to the fact that laws and regulations ensure that DPI and SLT are not misused (36.84% of respondents selected this option for DPI and 31.93% for SLT). During table discussions, many participants noted the lack of suitable norms, and demanded the adoption of wide-ranging regulation clarifying the conditions under which data may be used, the institutions that could access the data, a clear framework for consent, and sanctions for errors and abuses. Most participants claimed the need for rules at the European and even international level. Some said that the EU and the US ought to find an agreement on DPI, which should then be extended to other countries. Some participants mentioned the need to have supranational bodies overseeing the application of rules and controlling the actions of those using SOSTs. Only a minority did contest the validity of rules, and suggested instead that technology should be the answer (applied by the vendor, too).

Almost half agreed with the statement "DPI/SLT improves national security", thus confirming previous results. The opinions on intrusiveness differed according to the technology considered: almost 50% of respondents selected the option "I believe that DPI is intrusive", while 37.95% of participants selected the same option for SLT. 55.42% of respondents thought that the degree of intrusiveness of SLT is acceptable considering its benefits, and 36.84% of respondents did the same for DPI. *The combination of the last two options should provide an additional nuance to the trade-off model*.

## 4.6 Role of alternative security approaches

At the beginning of the citizen summit, 72% of participants agreed that alternative approaches to security (which do not involve SOSTs) should be given higher priority, while at the end of the summit the figure had slightly decreased to 66%, in line with the average resulting from all summits.

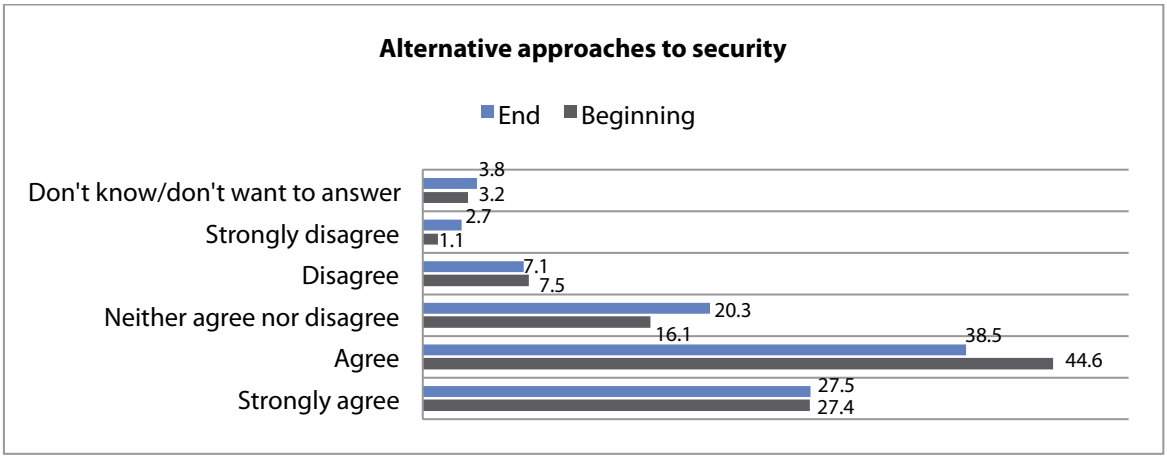



Figure 23: Alternative approaches to security which do not involve surveillance-oriented security technologies should be given higher priority

Discussions on alternative measures were reported by about a third of the table moderators (11 out of 35). Citizens claimed that alternative security approaches were desirable, especially for crime prevention. Alternative measures were described in very general terms as measures aimed at reducing social inequalities or other root causes of insecurity, and as mechanisms that do not target citizens and their personal data. Suggestions included: i) addressing societal injustice and unease, taking care of the environment, investing in harmonious cohabitation, rather than targeting criminals; ii) protecting critical infrastructure at the source, addressing culturally-sensitive issues, such as tax evasion; iii) investing in neighbourhood patrols, or CCTV cameras (one suggestion); and adopting global regulation. Some suggested that research should be conducted to find out less impacting alternatives and, once found, lobbying for their application.

## 4.7 Citizens' recommendations to policy makers

After the two SOST-specific sessions, citizens had to agree on a table recommendation to send to national or European policy-makers. What follows is a synthesis of the main themes that emerged from the 35 recommendations (which are reported in full and translated into English in Annex 10.1)**: regulation, transparency, awareness, legal protection, privacy by design and alternatives**. We believe recommendations should be read in the light of the empirical results, as well as the context of the country.

As for **regulation**, citizens asked for effective laws to regulate access, collection and use of the personal data for both commercial and public security purposes. They recommended harmonizing national laws in the European Union and adopting laws to protect personal data of European citizens, also when they are transferred outside of the European Union, e.g. by US-based companies. Some citizens proposed to negotiate a multilateral treaty on privacy.

Greater information was a recurrent theme in the recommendations, which could be divided into two main branches: institutional transparency, and education.

Citizens demanded increased **transparency** and accountability of the institutions that process personal data collected through the use of SOSTs. First, citizens suggested that the names of the offices processing information for public and national security purposes, and the data controllers working

therein, be made available. Then, they proposed that such offices be accountable for their activity, for instance by releasing regularly reports on their processings.

As for **education**, participants proposed to train and raise citizens' awareness regarding the use of SOSTs for the processing of personal data for public security purposes. Among other things, citizens suggested public awareness campaigns, information campaigns on the Internet, courses and seminars in schools for students, but also courses for adults, e.g. organized by municipalities in their structures.

Many citizens proposed to create an independent authority, composed of experts, in charge of overseeing the processing of personal data for public security purposes, and entrusted with the power to sanction violations of citizens' rights. Most recommendations proposed to create a European institution, whereas some suggested locating it at the international level. Some suggested that the processing of personal data should be authorized by a judicial authority.

Citizens often expressed the desire to better **control SOSTs**, in particular they asked for mechanisms embedded in the technologies to manage functions that have an impact on personal data. They demanded producers include and list the "privacy" risks in the instruction guides. Some proposed to use a seal on websites that protect personal data and private life.

Finally, citizens recommended the use of unspecified **non-technological measures** to address security issues, both in the investigation of crimes and when protecting communities.

### 4.7.1 Short commentary on the recommendations

Further analysis of the recommendations elaborated by participants provides important insights.

On the one hand, when read in the negative, they provide a hint of citizens' lack of awareness of regulation and oversight. Citizens mentioned neither the Italian Privacy Code nor the role played by the Italian Garante in protecting personal data processing, especially in the private sector. Moroever, they never alluded to existing European authorities, such as Europol, the European Data Protection Supervisor and Eurojust.

Some of the authorities mentioned have competence in those areas where participants felt there was a need to intervene (e.g. the private sector). There might be a need to scale up information on existing safeguards offered by the law, and the protection provided by the institutions in charge of implementing existing regulations.

Recommendations testify to the complexity of SOSTs and seem to suggest that convenience and the lack of information, rather than indifference toward privacy, determine people's behaviour. Citizens have widely expressed their interest in privacy, but entrust the state (and companies) with the role of educator as to the consequences tied to the processing of their personal data.

On the other hand, participants' recommendations also provide an indirect litmus test for some of the current policy initiatives.

The demand for greater European harmonization seems to support the adoption of the proposed Regulation on the protection of personal data and the free flow thereof. Likewise, the request for protecting one's personal data even when transferred abroad backs the conclusion of an effective transatlantic agreement on the processing of transferred data. Proposals for an international treaty are in line with current initiatives, e.g. at the United Nations level[150], or the Madrid Declaration[151].

[150] See, for instance, General Assembly, 'Resolution 68/167. The Right to Privacy in the Digital Age ', United Nations (2013).

[151] International Conference of Data Protection and Privacy Commissioners, 'Joint Proposal for a Draft of International Standards on the Protection of Privacy with Regard to the Processing of Personal Data (the Madrid Resolution)', (Madrid: 30th International Conference of Data Protection and Privacy Commissioners, 2009).

Also, citizens' request of being in control of the personal data processed by SOSTs seems to support the idea of privacy by design[152] currently proposed in policy circles.

### 4.7.2 Limitations of the summit

While the summit has generated important information and insights into an underexplored area, we deem it important to highlight some limitations.

First of all, while broadly representative of the diversity within modern Italian society, the sample was nonetheless of geographically limited scope. The size of the sample was deemed too small to test the empirical model designed within the SurPRISE project; instead, the model will be tested against the full European sample.

Second, table discussions were not recorded, and therefore we have relied on the notes collected by the 35 table moderators and the 4 note takers during the event. Moreover, it is not possible to assess the extent to which participants influenced each other in the course of table discussions, as well as the impact that showing immediately the result of the collective voting on screens may have had on individual voting behaviour.

Third, the summit was a one-day event, therefore participants' contributions and perceptions cannot be assessed over time. Furthermore, we had to rely on self-assessments about participants' previous knowledge, and the extent to which the material we provided was informative.

The comparative report will provide more robust results, thus complementing this report.

[152] Ann Cavoukian, 'Privacy by Design in Law, Policy and Practice. A White Paper for Regulators, Decision-Makers and Policy-Makers', Toronto, Information and Privacy Commissioner, Ontario (2011).

# 5 Summary and Conclusions

**The citizens' summit** served multiple purposes. First, it aimed at collecting empirical evidence on factors influencing citizens' acceptance, and acceptability, of security measures, and citizens' assessment of the role of trade-offs in their judgement concerning security and privacy. Second, it invited citizens to take an active part in the decision-making process, by elaborating recommendations for national and European policy-makers. The focus on SOSTs did not intend to capture citizens' evaluation of DPI and SLT, but rather allowed citizens to express their attitudes to surveillance technologies, security and privacy in context, making reference to real-life situations.

Overall, it seems that participants at the Italian summit perceive an appreciable level of **security** threat, in particular when browsing the Internet, then at the personal level, and finally for public security. Less than half of the respondents considered Italy a safe place to live or felt secure in their daily life (the lowest rate among the nine citizen summits conducted in Europe). Remarkably, 38% of respondents "neither agreed nor disagreed" with the statement "I generally feel secure in my daily life" (the highest value of undecided respondents compared with all other countries). The outcome is in line with Italy's perceived high level of crime. There seems to be a cleavage between citizens' perceptions of personal and national security. Citizens feel they have a greater degree of control over personal rather than national security, identified by some as an intangible concept, which is in line with Italy's historical lack of transparency concerning its national security policies.

The majority of Italian respondents highlighted that DPI and SLT are harmful for **privacy**, whether they are used for security or commercial purposes, in spite of the benefits that they can bring. A clear majority of participants perceived that SOSTs have a negative impact on their personal privacy, and that an increasing use of ICTs leads to an erosion of citizens' privacy in general. In the case of both DPI and SLT, worry is caused by fear of human rights infringements and privacy intrusiveness. The second most important reason to fear DPI is its covert nature. SLT's second most feared feature, for which participants in Italy worried more than their European counterparts at the other SurPRISE summits, is the fact that it could lead to misinterpret people's behaviour and lead to adverse decisions.

**Disclosing personal information** is seen as an increasing part of modern life. The majority of participants stated that they would like to find out more about how to protect their personal data against the uses linked to both DPI (60%) and SLT (62%). Two thirds of people who cast their vote would also favour the adoption of **alternative approaches** that do not require the use of SOSTs. Two thirds of Europeans taking part in the SurPRISE summits shared this view.

When it came to **SOSTs**, participants were more familiar with SLT than DPI. The majority of participants agreed with the use of DPI (55%) and SLT (70%) as a national security measure. Support increased, compared with the perceived level of effectiveness and the utility to implement national security. The result might suggest that the more citizens approve of technology in general, the more likely they are to perceive a particular SOST to be effective. However, only slightly more than a third are ready to trade privacy with security.

The outcome is interesting, as citizens became more supportive of SOSTs in general, too, during the event, even if this meant being exposed to surveillance. One factor could be the increased knowledge of participants, who came to appreciate better both the pros and cons of SOSTs. While citizens overall **support SOSTs as a tool to foster public security**, the results are challenging, as their support is surrounded by a degree of diffidence higher than in other European summits.

Respondents favour the general use of SOSTs by governments if available, as they believe they can improve national security by targeting criminals. However, acceptance is shadowed by doubts and scepticism, due to the fear of abuses of power, the uncertainty about the real effectiveness of SOSTs in countering security challenges, and the cautious approach to the "I have nothing to hide" attitude.

There seems to be a great degree of uncertainty when it comes to trusting institutions using SOSTs, and for some specific questions the balance is tilted towards lack of trust. The lack of information and transparency strongly contributed to participants' doubts as to the trustworthiness of institutions, and the effectiveness of regulation. The vast majority of participants expressed unease and disagreement with the use of data collected from SOSTS for commercial purposes.

In line with the themes discussed during the day, **table recommendations** clustered around the following themes: regulation, transparency, awareness, legal protection, privacy by design and alternatives. 40.6% of participants agreed or strongly agreed with the statement "**I believe the citizen summit has generated valuable knowledge for the politicians**", 10 percentage points lower than the European average. While 25.6% were undecided, in line with the other summits, a third disagreed or strongly disagreed, as opposed to 17% at the other summits level. The data might reflect Italians' high rate of disaffection with politics recorded shortly after the event, but might also reflect the lack of involvement of public opinion on matters of public security. Yet, many participants asked reassurance that recommendations would be delivered to leaders.

**The summit provided important insight into the approach to surveillance, privacy and security in Italy, but left some questions unanswered.** What does security and privacy mean exactly to participants? Under what precise circumstances would they agree to be surveilled, give up privacy, accept certain SOSTs, but not others? Which specific authorities should be in charge of using SOSTs? What factors can reduce the fear of abuse, and increase trust? What kind of regulation and safeguards do citizens desire in relation to the use of their personal data for public and national security purposes? Would greater control and information change attitudes? These and other questions informed the organization of a second participatory event, designed as a focus group to investigate in greater details citizens' thinking and preferences. The subsequent Italian focus group event took place in Florence on June 17th, and its results will be the object of a dedicated report.

A last important conclusion relates to participants' **general response to the summit.** Almost all strongly agreed to have gained new insight by participating in the citizen summit. The summit was successful in raising awareness on SOSTs: at the end of the summit, the percentage of participants declaring to "know little to nothing" decreased to 9.1%, and the percentage of participants declaring "I have some knowledge of SOSTs but it would be useful to learn more" increased to 59.1%. More importantly, many citizens expressed the feeling that participatory events such as the citizens' summit represent an important step towards increasing awareness and involving citizens. There is more to participation than renovating the façade of democracy. Participation, in fact, is an expression of the rule of law, the ordering and guiding principle of the European polity. As elaborated by Mendes, the rule of law protects dignity and a "positive freedom: active engagement in the administration of public affairs, the freedom to participate actively and argumentatively in the way one is governed".[153] The primary consequence is introducing rules that subject public authority to include the participation of citizens. Such active engagement in the administration of public affairs would concretize material justice, which results from the decision-maker taking into proper account and addressing the legally protected interests of public and private parties,[154] as well as the right to good administration (art. 41 of the Charter of Fundamental Rights of the European Union).

Therefore, ingraining participation in the process of decision-making, for instance in the form of participatory events assessing such different legally protected interests[155], could be a substantive way to conform to the rule of law, the right to good administration and, in the present case, avoid costly political decisions that have no support among the public. Perhaps this might be the single most important lesson of the summit for policy makers.

---

[153] Joana Mendes, 'Rule of Law and Participation: A Normative Analysis of Internationalised Rulemaking as Composite Procedure', New York, New York University School of Law (2013) at 14.

[154] Ibid.

[155] See, for instance, the initiative undertaken by the Italian representation of the European Commission through the project POLITICALLY.EU, which gathers stakeholders to discuss relevant European Union policies on which they have expertise. As of May 2014, the project performed four national debates, on growth and employment, a on the reform of the Common Foreign and Defence Policy, on democratic participation and accountability in the EU, on European migration policies. For updates of their initiatives, consult the website: http://www.politically.eu/.

# 6 Bibliography

Andreassi, Ansoino (2000), 'Dalla Polizia Politica alla Polizia di Sicurezza - Un'evoluzione complessa', *Polizia Moderna,* (supplement to n. 2).

Bonanno, Alberto and Puglia, Alessandro (2014), 'L'hangar segreto di Sigonella con i droni spia americani', *LA Repubblica,* 29 giugno 2014.

Bruno, Pino (2014), 'l drone più sicuro al mondo è italiano, lo ha ispirato Olivetti', *La Repubblica,* 2 giugno 2014.

Bygrave, Lee A. (2014), *Data Privacy Law. An International Perspective* (Oxford: Oxford University Press).

Calamari, Marco, et al. (2011), 'Country Report Italy', *Global Surveillance Monitor* (Privacy International).

Campesi, Giuseppe (2009), *Genealogia della pubblica sicurezza. Teoria e storia del moderno dispositivo poliziesco* (Verona: Ombre Corte).

Cavoukian, Ann (2011), 'Privacy by Design in Law, Policy and Practice. A White Paper for Regulators, Decision-makers and Policy-makers', (Toronto: Information and Privacy Commissioner, Ontario).

Cocq, Céline and Galli, Francesca (2012), 'SURVEILLE Deliverable 4.1: The use of surveillance technologies for the prevention and investigation of serious crimes'.

Commissione Europea (2012), 'Decisione della Commissione del 17.7.2012 che approva, per l'Italia, il programma annuale 2012 per il Fondo per le frontiere esterne, e il cofinanziamento a titolo di tale Fondo per l'esercizio 2012 '.

Committee of Ministers of the Council of Europe (2001), 'Rec(2001)10 of the Committee of Ministers to member states', (Strasbourg).

Conte, Valentina, 'Ridotto il decreto sviluppo bis. il Colle taglia norma pro-Berlusconi', *La Repubblica,* 4 ottobre 2012.

'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', (1981), in Council of Europe (ed.), (CETS No. 108; Strasbourg).

Council of Europe (1950), 'Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No 11 and 14', (Council of Europe,, CETS n° 005; Rome).

D'amario, Walter (2014), 'Banca dati del Dna, c'è la sede e lo spot tv. Ma l'istituto funzionerà dal 2015', *La Repubblica,* 4 February 2014.

'Datagate - Bonino in Parlamento - Chiarimenti necessari ma andare avanti con trattato Usa-Ue ', (updated 4 July 2013) <http://www.esteri.it/MAE/IT/Sala_Stampa/ArchivioNotizie/Approfondimenti/2013/07/20130704_datagate_bonino_parlamento.htm%3E.

'Decreto Legge 92/2008 "decreto sicurezza (converted into Law 125/2008 "misure urgenti in materia di sicurezza pubblica")', (2008), (D.L. of 23 May 2008; Repubblica Italiana).

'Decreto Legislativo 14 marzo 2013, n. 33. Riordino della disciplina riguardante gli obblighi di pubblicita', trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni. (13G00076)', (2013), (Repubblica Italiana).

Della Porta, Donatella and Reiter, Herbert (2003), *Polizia e Protesta. L'ordine Pubblico dalla liberazione ai "no global"* (Bologna: Il Mulino).

di Amato, Astolfo (2011), *Criminal law in Italy* (Kluwer Law International).

European Commission (2011a), 'Special Eurobarometer 371 - Internal -Security. Italian factsheet'.

--- (2011b), 'Special Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union'.

European Forum for Urban Security, VV.AA. (2010), 'Citizens, Cities and Video Surveillance. Towards a democratic and responsible use of CCTV', (Montreuil: European Forum for Urban Security).

--- (2012), 'Security, Democracy and Cities: The Manifesto of Aubervilliers and Saint-Denis', (Paris: European Forum for Urban Security).

European Parliament (2012), 'Resolution of 12 December 2012 on the situation of fundamental rights in the European Union (2010 - 2011) '.

European Parliament and Council (1995), 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive)', (OJ L 281), 31-50.

Finocchiaro, Giusella (2012), *Privacy e protezione dei dati personali. Disciplina e strumenti operativi* (Bologna: Zanichelli).

Galli, Francesca (2012), 'Italian counter-terrorism legislation. The development of a parallel track. ("doppio binario")', in Francesca Galli and Anne Weyembergh (eds.), *EU counter-terrorism offences. What impact on national legsilation and case law?* (Brussels: Editions de l'Université de Bruxelles).

General Assembly (2013), 'Resolution 68/167. The right to privacy in the digital age ', (United Nations).

Giunti, Arianna and Sasso, Michele (2013), 'Identificare i poliziotti? In Italia non si può', *L'Espresso,* 21 Novembre 2013.

Iai, Ivano (2007), 'Il trattamento dei dati personali da parte delle forze di polizia', in Vincezo Cuffaro, Roberto D'Orazio, and Vincenzo Ricciuto (eds.), *Il codice del trattamento dei dati personali,* (Torino: Giappichelli editore).

International Conference of Data Protection and Privacy Commissioners (2009), 'Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data (The Madrid Resolution)', (Madrid: 30th International Conference of Data Protection and Privacy Commissioners).

Isernia, Pierangelo (1996), *Dove gli Angeli non Mettono Piede. Opinion Pubblica e Politiche di Sicurezza in Italia* (Milano: Franco Angeli).

Istituto Nazionale di Statistica (ISTAT) (2013), ' Chapter 7. Security', *Rapporto Bes 2013: il benessere equo e sostenibile in Italia*, pp. 149 – 70.

--- (2014), 'Noi Italia - 100 statistics to understand the country we live in, Crime and Safety', 129 -46.

Italian Data Protection Authority (2010), 'Video surveillance guidelines', (Rome: Garante per la protezione dei dati personali).

Katz, Richard S. (2003), 'Reforming the Italian Electoral Law, 1993', in Matthew Soberg Shugart and Martin P. Wattenberg (eds.), *Mixed-Member Electoral Systems: The Best of Both Worlds?* (Oxford: Oxford University Press).

La Repubblica, N/A (2014), 'Il sindaco di Forte dei Marmi: "Sequestro i droni in volo"', *La Repubblica - Edizione di Firenze,* 14 maggio 2014.

Labanca, Nicola (2013), 'Studiare le polizie italiane dall'Unità ad oggi, dopo la smilitarizzazione della polizia (1981-2011)', in Raffaele Camposano (ed.), *Poliziotti d'Italia tra cronaca e storia prima e dopo l'unità.* (Quaderno I; Rome: Ufficio Storico della Polizia di Stato).

Landucci, Roberto (2014), 'Italy's Renzi wins confidence vote on cutting local government', *Reuters,* 26 March 2014.

Lavalle, Carlo (2014), 'A Roma il primo salone aeronautico sui droni in Italia ', *La Stampa,* 25 maggio 2014.

Longo, Alessandro (2014), 'Vodafone: "Alcuni governi hanno accesso diretto alle comunicazioni dei nostri utenti". Il Garante: "Inaccettabile"', *La Repubblica,* 6 June 2014.

Manfellotto, Bruno (2013), 'Quattro mesi per capire il Datagate', *L'Espresso,* 5 November 2013.

Mendes, Joana (2013), 'Rule of Law and Participation: A Normative Analysis of Internationalised Rulemaking as Composite Procedure', *Jean Monnet Working Paper Series* (New York: New York University School of Law).

Ministero dell' Economia e delle Finanze (2011), 'Analisi dei Dati IRPEF. Anno d'imposta 2011'.

Ministero dell'Interno (2014), 'Direttiva generale per l'attività amministrativa e per la gestione relativa all'anno 2014', (Roma).

N/A (2014a), 'Istat, nuovo record per la disoccupazione: a gennaio il tasso balza al 12,9 per cento', *La Repubblica,* 28 February 2014.

--- (2014b), 'Privacy, dal Garante nuove regole per le tecnologie biometriche', *La Repubblica,* 21 May 2014.

'Nuovo ordinamento dell'Amministrazione della pubblica sicurezza', (1981), (Legge n. 121 del 1 Aprile 1981 Repubblica Italiana).

Organization for the Economic Cooperation and Development (2011), 'Defining and Describing Regions', *OECD Regions at a Glance 2011* (Paris: OECD Publishing).

Pennisi, Martina (2013), 'L'accordo fra Garante e servizi segreti ci difende dalla Nsa?', *Wired,* 12 November 2013.

Porcedda, Maria Grazia, Vermeulen, Mathias, and Scheinin, Martin (2013), *Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy. Deliverable 3.2, SurPRISE Project.* (Florence: European University Institute).

Puglia, Alessandro and Tondo, Lorenzo (2013), 'Sigonella diventa base strategica ecco le slides riservate della Nato', *La Repubblica - Edizione di Palermo,* 3 agosto 2014.

Redazione del Fatto Quotidiano (2013a), 'Datagate, Letta al Copasir: "La privacy degli italiani non è mai stata violata', *Il Fatto Quotidiano*.

--- (2013b), 'Datagate, Italia intercettata. Copasir e Garante della privacy: "Chiarire"', *Il Fatto Quotidiano,* 22 Octobr 2013.

Renda, Carlo (2014), 'Rapporto Eurispes 2014; metà degli italiani senza orientamento politico, senza fiducia nelle Istituzioni', *L'Huffington Post,* 31 January 2014.

Rodotà, Stefano (1973), *Elaboratori Elettronici e Controllo Sociale* (Bologna: Mulino).

--- (2005), *Intervista su Privacy e Libertà. A cura di Paolo Conti*.

'Sentenza 1/2014', 144/2013, G. U. 15/01/2014, Giudizio di legittimità costituzionale in via incidentale: Corte Costituzionale della Repubblica Italiana (4 December 2013).

'Sentenza n. 290', 290, Constitutional legitimacy: Corte Costituzionale (12 July 2001).

Sistema di Informazione per la Sicurezza della Repubblica (2014), 'Relazione al Parlamentosulla Politica dell'Informazione per la Sicurezza 2013'.

Stubbs, Katija Sugman and Galli, Francesca (2012), 'Inchoate offences.The sanctioning of an act prior to and irrespective of the commission of any harm', in Francesca Galli and Anne Weyembergh (eds.), *EU counter-terrorism offences. What impact on national legislation and case law?* (Brussels: Editions de l'Université de Bruxelles).

Unabhaengiges Landeszentrum fuer Datenschutz (ULD) (2013), 'Report on Surveillance Technology and Privacy Enhancing Design, Deliverable 3.1, SurPRISE Project'.

United Nations (1966), 'International Covenant on Civil and Political Rights', (New York).

VV.AA. (2010), 'L'evoluzione della normativa in materia di pubblica sicurezza fra Stato, Regioni ed enti locali', (Rome: Servizio Studi del Senato).

Walker, Andrew (2014), 'Italy's economy: The mountain Matteo Renzi must climb', *BBC News,* 25 February 2014.

Wired, N/A (2014), 'Guardian 2000, un drone poliziotto nei cieli italiani', *Wired.it,* 28 marzo 2014.

# 7 List of Figures

Figure 1: Gender distribution ..... 16
Figure 2: Education ..... 17
Figure 3: Employment status in different areas ..... 18
Figure 4: General attitudes on security. Questionnaire item nr. 3 (N=179), 4 (N=182) and 5 (N=180). ..... 21
Figure 5: General attitudes on privacy *at the beginning* of the citizens' summit (Percentages). ..... 22
Figure 6: Perceived effectiveness of DPI ..... 24
Figure 7: Smartphone Location Tracking perceived effectiveness ..... 24
Figure 8: DPI perceived intrusiveness ..... 25
Figure 9: Smartphone Location Tracking perceived intrusiveness ..... 26
Figure 10: DPI and Smartphone Location Tracking are useful but highly intrusive ..... 28
Figure 11: Q79 Risk-benefit balance (Trade-off) ..... 29
Figure 12: Security v. privacy: SLT (Q80 + Q 83) ..... 30
Figure 13: Change of behaviour because of DPI and smartphone location tracking ..... 31
Figure 14: Overall I believe surveillance-oriented security technologies should be routinely implemented to improve national security (Percentages) ..... 32
Figure 15: General attitudes toward technology to foster security ..... 33
Figure 16: Future developments of SOSTs ..... 34
Figure 17: Substantive privacy concerns ..... 34
Figure 18: General attitudes on privacy at the end of the summit ..... 35
Figure 19: Social proximity compared in the case of SLT ..... 35
Figure 20: Institutional trustworthiness – DPI ..... 36
Figure 21: Institutional trustworthiness - SLT ..... 37
Figure 22: Regulation, intrusiveness, trade-off ..... 38
Figure 23: Alternative approaches to security which do not involve surveillance-oriented security technologies should be given higher priority ..... 39

# 8 List of Tables

Table 1: Random extraction requested to the City of Florence for the sampling of citizens. ..... 15

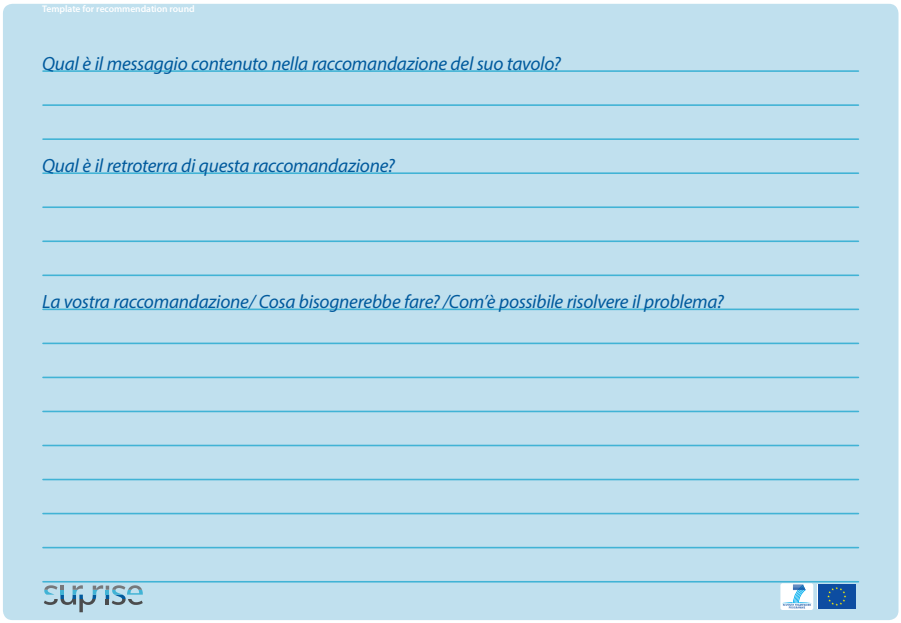
# 9 List of Abbreviations

| Abbreviation | Definition |
|---|---|
| AISE | Agenzia Informazioni e Sicurezza Esterna ("External Intelligence and Security Agency") |
| AISI | Agenzia Informazioni e Sicurezza Interna ("Internal Information and Security Agency") |
| CCTV | Closed circuit television |
| CED | Centro elaborazione dati (“Data Center”) |
| COPASIR | Comitato Parlamentare di Controllo per i Servizi di Informazione e Sicurezza e per il Segreto di Stato (“Parliamentary Committee for the Intelligence and Security Services and for State Secret Control”) |
| DIGOS | Dipartimento Investigazioni Generali e Operazioni Speciali (“General Investigations and Special Operations Division”) |
| DNA | Deoxyribonucleic acid |
| DPI | Deep Package Inspection |
| EC | European Commission |
| ECHR | European Convention on Human Rights |
| ENAC | Ente Nazionale Aviazione Civile (“Italian Civil Aviation Authority”) |
| ID | Identification |
| ISP | Internet service provider |
| ISTAT | Istituto Nazionale di Statistica (“Italian National Statistical Institute”) |
| NATO | North Atlantic Treaty Organization |
| NSA | National Security Agency |
| OECD | Organisation for Economic Co-operation and Development |
| OVRA | Organizzazione per la Vigilanza e la Repressione dell'Antifascismo ("Organization for Vigilance and Repression of Anti-Fascism") |
| RFID | Radio-frequency identification |
| SIS | Sistema d’informazione Schengen |
| SLT | Smartphone Location Tracking |
| SOST | Surveillance-oriented security technologies |
| TULPS | Testo Unico Leggi Pubblica Sicurezza (“Consolidated Public Security”) |

# 10 Annex

## 10.1 Table recommendations

*Template*[156]




*Recommendations – content*[157]

| 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? |
|---|---|---|
| Transparency in regard of the technologies taken under consideration, with traceability of all the data. | We found that there is a need to implement measures for ensuring transparency in regard of the technologies taken under consideration, with traceability of all the data. | Investments in consumer protection should be increased and increase consumer awareness as concerns use of these technologies should be enhanced. |
| | | It is necessary to define precisely who can use these data and, at the same time, identify special monitoring agencies, taking care to eliminate conflicts of interest between the subjects that use said data and those responsible for monitoring. |
| | | There is also deemed to exist a need for detailed definition of how these data may be used by law enforcement, in order to avoid inappropriate data use. |
| | | Furthermore, at the legislative level, it would be advisable to provide for harmonisation among the various legal systems in order to guarantee uniform protection of consumer rights. |

[156] 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.

[157] Translated from Italian

| | | |
|---|---|---|
| Laws common to all the various countries, supra partes international guarantee institution and alternatives. | Legislative vacuum. | Avoid a legislative vacuum with laws common to all the various countries. |
| | | Establish a supra partes international guarantee institution to ensure application of the laws (on privacy and on transparency), which can apply sanctions in case of violations (in particular, against service providers which manage and have access to user information) and which can promote awareness and publication of the relevant laws. This body must guarantee that personal data are not accessible. |
| | | Identifying alterative monitoring mechanisms for guaranteeing security. |
| Information, European regulation, European Agency. | There is a perceived need and advantage in use of the new surveillance technologies for security reasons. With this premise, it is deemed indispensible that every user/citizen be provided with the information needed to understand DPI and smartphone location tracking. | We propose that a social advertising campaign be launched to inform all citizens of the fact that they may be inspected or geographically located. |
| | | On DPI. Clear and visible warning that any user's data may be 'unpacked', read, and monitored. |
| | | On geolocation. On every smartphone, install a device (which may be switched on or off) to communicate when a user is localisable and when he/she is not. |
| | | Urgently, draft a European regulation providing protection for citizens and providing precise rules for use of DPI and geolocation by private/public companies and public bodies. |
| | | Institution, by the European institutions, of a European Guarantee Institution / European Agency for monitoring and policing observance of the regulations governing use of the DPI and geolocation technologies. |
| There should be created legislation/regulations on protection of data and privacy in relation to security-oriented surveillance tools, regulated by an international-level body. | Responding to the legislative vacuum in which private subjects currently operate. | There should be created legislation/regulations on protection of data and privacy in relation to security-oriented surveillance tools, regulated by an international-level body: rules valid in all the countries and therefore capable of responding to the legislative vacuum in which private subjects currently operate. |
| | | The legislation should afford the option for persons (without criminal records) to decide whether or not they consent to being tracked via SOSTs. |
| | | The legislation should be integrated by establishment of a supra-national independent authority acting as guarantor of individuals' human rights and protection of their personal privacy. |
| | | Security forces should be permitted to make use of SOSTs only after criminals (or suspects in a criminal case) have been identified via investigations conducted by other means. To this end it would be necessary to develop and enhance the alternative investigative tools available to public security forces. |

| | | |
|---|---|---|
| Information and protection from abuses. | Abuses that incorrect use of these technologies could cause if they are not adequately regulated and monitored. | More information concerning individuals' privacy in relation to DPI and smartphone geolocation is required, as are greater certainties in regard of protection against the abuses that incorrect use of these technologies could cause if they are not adequately regulated and monitored. |
| Transparency/communication, but also more 'community'. | If we cannot do without these technologies, they can be subjected to more stringent regulation and return to being tools at the service of citizens, and not vice-versa: currently, citizens are at the service of technology. | 1. Provide more/better information relative to the risks and opportunities inherent in these tools. The information campaign must be broad-based and capillary, and include: a. Education in the schools, and, in particular, monitoring of forms of learning which make use of technological means; b. Use of traditional tools, such as informative brochures and pamphlets distributed via the postal service; c. Use of participatory tools, in the city governments, for collecting communications / suggestions / opinions from citizens and contributing to capillary spread of the information by word of mouth.<br>2. Develop a uniform legislative reference frame which is clear and universally accessible and which sets strict limits on the uses which may be made, by economic entities (such as the telephone companies), of the data provided by/relating to users, who before being 'users' are 'citizens'. The legislative framework must also guarantee: a. The above-mentioned provision of information to citizens; b. Monitoring/supervision of data disclosure by law enforcement; c. Limitations on marketing of data packages.<br>3. From the point of view of social development, the European institutions are invited to promote joint actions and projects targeting a return to more 'personal' relationships which are less 'mediated' by technologies: the citizen must regain a sense of community that has been all but lost, and 'social control' must not be exercised through data packages transiting the Internet but through personal acquaintance and trust as well as social and legal sanction of inappropriate behaviours. |
| Rules, sensitisation and respect of individual rights. | Use of DPI and geolocation technology for security and commercial purposes. | We request regulation of use of DPI and geolocation technology, limiting such use to security, and excluding any commercial and advertising use; enhancement of security methods alternative to use of DPI and enhancement of use of geolocation for personal safety purposes. |
| | | Via broad-based information channels, sensitisation to and provision of information about these two technologies and their how they operate. |
| | | We recommend that these technologies be used only in respect of individual rights and individuals' privacy and that any type of abuse of power be discouraged. |
| Common international rules, limitations. | Use of DPI and geolocation technology for security and commercial purposes. | Identify common European and international rules for regulating data processing and accessibility. |

| | | |
|---|---|---|
| | | Limit access to DPI technology only to public institutions with network protection functions (against viruses, etc.) without interfering in citizens' private lives. As concerns geolocation, it is acceptable that this technology be in the hands of private subjects as long as the data are protected against theft and are not resold to other private parties for commercial use. |
| | | Intensify use of surveillance devices in sectors besides law enforcement: works of art, natural calamities, etc. |
| Greater control over SOSTs. | Use of DPI and geolocation technology for security and commercial purposes. | Definition of a national-level authority to act as data controller and monitor use of technologies/devices. |
| | | Monitoring to ensure that data are not freely usable (for example, for commercial purposes). |
| | | Greater control over monitoring of geolocation of minors. |
| | | Harmonisation of pertinent legislation in all European Union countries. |
| Transparency, laws and alternatives. | Legislative vacuum and Use of DPI and geolocation technology for security and commercial purposes. | Greater transparency in the legislation regulating use of personal data. |
| | | More specific discipline of use of data for commercial purposes. |
| | | Greater investments by governments in research into solutions alternative to those which call for monitoring of information (crime prevention). |
| | | Greater transparency in privacy policies and privacy policy statements that are easier for citizens/consumers to read and understand. |
| European laws, education, transparency and alternatives. | Guaranteeing fundamental personal data protection rights. | There is a need for European legislation guaranteeing fundamental personal data protection rights, an international regulation – such as a 'charter of fundamental rights' – which endorses democratic freedoms and that it be ratified by the single countries to guarantee the right to privacy in the different specific areas of utilisation. |
| | | There is a need to provide information on how the SOSTs operate and how they are used, to explain to citizens the operational processes involved in monitoring and definition of the risk factors and the efficacy of intervention options. |
| | | It is absolutely necessary that there be greater transparency and clarity as concerns the subjects that collect, hold, and monitor data, and, in particular, private companies; user awareness must be heightened and users must be permitted to express or refuse their consent. Each individual citizen should be able to request which of his/her data are recorded and who holds said data and must be provided with formal and inviolable guarantees in this regard. |

| | | |
|---|---|---|
| | | Development of the SOSTs must be only one of the actions taken to ensure security; improving social conditions and security in the territory could have better effects in terms of instilling a sense of security in the population. |
| Information channel for citizens | There are no easily accessible and -understandable supra partes sources of information. | It is necessary to create an information channel for citizens, couched in simple, clear language. Information channels must exist at both the European and national levels. |
| | | It is therefore important to establish uniform legislation throughout the European community. |
| | | Additionally, it would be useful were the Authority to invest in periodic publications or in any media-mediated information material which can reach everyone, including the schools. |
| There is a need for clear rules concerning regulation of the security technologies and greater transparency in communication of the laws and regulations is necessary. | Balance the usefulness of technology with the right to privacy and security. | Clear rules concerning the limits on use and collection of personal data by technological means. In particular, it is necessary to establish rules concerning who may access personal data, for how long, under what conditions and for what purposes. Additionally, it would be useful to coordinate with the legislators of other countries. |
| | | Citizens must be informed of the rules, in order to encourage informed use of the technology (perhaps via media campaigns). If possible, it would be useful to create a 'label' to attach to websites that respect certain rules. This 'label' could be especially important in the case of providers of email services, Facebook, Amazon, Google and other sites through which great quantities of personal information are transmitted. |
| At the European level, provide for laws and regulations for filling the legislative vacuum inherent to use of the new technologies. | Legislative vacuum inherent to use of the new technologies. | Addressed to: President of the European Parliament, the European Parliament and the President of the European Agency for Network and Information Security. |
| | | At the European level, institute, a supervisory body for monitoring the operators that make use of the technologies in question and for directing data use only for collective security purposes. |
| | | Provide for transparency and accessibility, for all European citizens, in relation to the manners in which their personal data may be used. |
| Legislation, wellbeing of the citizens, no to national security used as alibi for violation of rights. | Legislative vacuum and Use of DPI and geolocation technology for security and commercial purposes. | Legislation based on an ethical code, to protect the constitutional rights of individuals. |
| | | Monitoring, information concerning privacy and acquisition of personal data must target the wellbeing of citizens and not pursue the political or commercial or more general economic aims of government institutions or private bodies. |
| | | Furthermore, national security and crime fighting must not become alibis for violation and/or abuse of individuals' constitutional and other rights. |

| | | |
|---|---|---|
| Increase regulation | Legislative vacuum | The ways in which data is collected and used must be defined by law by the countries/European Union and must be limited to specific cases (terrorism, emergencies). There must be an institutional subject which carries out control activities and which also evaluates the security/efficacy of the technologies employed (DPI and GEOLOCATION software must be open-source to permit monitoring the real scope of these programs). Any regulation must require service providers to inform citizens of which third-party institutions may access their information, and in what cases. Regulation must provide citizens with the possibility to sell/share their DPI/GEOLOCATION data to receive services: in this case, however, the service provider must quantify the economic benefit which the user may receive from possession of data, in full transparency, and provide guarantees that the data will not be used outside of the scope of the agreements with users. |
| We are willing to surrender some elements of our privacy in exchange for greater security and services which can improve our lives, on condition that there be total transparency as regards processing of our data and the reliability of the data processors. | Use of DPI and geolocation technology for security and commercial purposes. | We want technologies such as smartphone geolocation and DPI to be used to make our lives more secure; in no case do we want our information to be transferred to companies which will use said data for profit. |
| | | It is also our hope that the laws and regulations which regulate these processes will be shared at the European level, in order to guarantee our freedom to make use of all the services offered over the Internet without fear of losing control of our privacy. |
| Supervisory, surveillance, and monitoring techniques are useful and necessary, but it is fundamental that we be able to obstruct and sanction parties which use our data for reasons other than security-related functions. | The life of the individual citizen is different from that of individuals who hold important posts or people who have committed illegal acts. People who do not hold important posts or who have not broken the law have no problem with being monitored. On the contrary, these tools can provide protection and safeguards. The only problem perceived is that we do not know to whom we must address ourselves when we do not want personal data and images to be used inappropriately (for commercial purposes or with malicious intent). | We must be able to identify those who use our sensitive data inappropriately.<br>We must be protected against these abuses, perpetrated for commercial purposes or out of mere malice.<br>We need to create an international body which can impose sanctions on those who make use of our data without our consent. Data in this connection is understood not as mere identification but as information pertinent to any aspect of our lives: lifestyles and purchasing patterns, health status.<br>It is, nevertheless, important to not limit surveillance and monitoring of public events; that is, of all those situations which represent a potential source of risk to society. |

| | | |
|---|---|---|
| Future developments of DPI for citizens' security. | There is a lack of regulation (laws, regulations, etc.) as regards DPI / there is a lack of clarity in the information provided / data subjects do not know who is in possession of their personal information / there is a lack of clarity between the producers of DPI technologies and the users. | We request greater clarity and information concerning use of DPI technology, a clear differentiation between producers and users of DPI technology; there is a need for uniform regulation, at the European and international levels, to guarantee the security of personal information. |
| Information on transparency, protection of users' rights, need for international regulation (the European community interfacing with the international community). | Redefine the concept of security (in relation to the technologies discussed); lack of information and need for awareness. | 1) Regulate personal data use at the international level.<br>2) Make public (visible) the bodies (public or private) which use and have access to data and make it possible to know what they are doing with the data.<br>3) Regulate the technologies discussed and make it possible to choose whether or not to be 'tracked' or geographically localised. |
| European laws and information campaign. | Legislative vacuum. | The European Commission must promote a law to provide, on the one hand, that data collected by the telephone companies and App and social network providers not be usable by extra-EU governments (or by countries in which there are not equal guarantees of protection of human rights) and, on the other, to promote a campaign to provide simple and clear information on the operation of security technologies and what limits they entail for our confidentiality and on how we can limit access to our data by those intending to put said data to commercial use. |
| Information, security, regulation, trasparency, qualification of the agencies that use data. | All things considered, security cannot be guaranteed without technology, but rights should be guaranteed. We would like to be able to respond as the Danish and the Norwegians do when asked about the security of their country. | 1) We request more information on how citizens can protect themselves against unscrupulous technological interference. We request that, if possible, alternative, non-invasive security measures be sought.<br>2) All things considered, security cannot be guaranteed without technology, but technology must not detract from the contribution of the human element.<br>3) It is essential that there be a technically-competent organisation, elected directly and from various sectors, responsible for legislating in accordance with a constitution which respects the fundamental rights of individuals to regulate the DPI and GEOLOCATION technologies.<br>4) Requirement of transparency in data processing.<br>5) The bodies responsible for application of the collected data must be highly qualified and their first priority must be activities useful for protecting social and individual rights.<br>6) It is suggested that the example of the U.S. as regards compulsory use of GPS devices on smartphones NOT be followed. |

| | | |
|---|---|---|
| People have faith in information technology but no faith in the people who, within the institutions, manage the data, and little faith in the capacity of the institutions to exert control over these subjects. Also lacking is a clear regulatory framework and an adequate system of sanctions. | Technology is inevitable, but it must be monitored/supervised intelligently and in respect of the rights of all individuals. | 1) Specific campaigns providing information to citizens;<br>2) Citizens must be aware that their personal data is being used and by whom;<br>3) There is a need for a single, clearly-defined, European-level legislative framework which calls for clear indication of what subjects use the data;<br>4) A clearly-defined system of administrative and criminal sanctions;<br>5) Specific training for data users;<br>6) Monthly reports to each, concerning data use;<br>7) Possibility to use data in specific cases (e.g., disappearances) and above all for monitoring minors. |
| Regulation and control, information. | Legislative vacuum. | Regulate use of the new security technologies and establish an independent supervisory body appointed by the European Court of Justice. The entire process must be accompanied by a campaign for providing information to citizens. |
| Use of 'surveillance-oriented security technologies' must be governed by common, transparent rules which can provide strong guarantees. | The participants expressed several shared perplexities concerning these technologies, not only in regard of respect for privacy but also as regards their efficacy. Since several of these technologies, and deep packet inspection (DPI) in particular, do not significantly increase security but instead pose a sharp loss in terms of privacy, the rules governing their use must be especially severe. | 1) Identify mechanisms for safeguarding the security of European citizens which are alternative to technological methods;<br>2) Coordinate the rules concerning 'surveillance-oriented security technologies' at the European level and identify ways in which to a enforce European citizens' right to privacy even against governments and companies operating from offices registered outside of the European Union;<br>3) Make the personal data collection process as transparent as possible and the data controller as identifiable as possible;<br>4) Limit the amount of personal data collected to that strictly necessary;<br>5) Request authorisation for collection of personal data from the citizen or, in the case of investigations of suspects by law enforcement, from the courts. |

| | | |
|---|---|---|
| We must be sure who is handling our security, and how. | The group hopes, above all, for a more secure, peaceful future in which there will be less need of measures which propose a trade-off between privacy and security. The current situation creates a dichotomy between security and privacy, the preference is in favour of security, and therefore the table concludes that the tools under discussion are important for individual and public security but that recommendations for their use are required. | Prohibit all commercial uses and uses not relevant to maintenance of security, provide information on the tools and use of data, clear and accessible information. Establish which bodies are responsible for use of the tools and data, and the competences of each. Define a system of sanctions for non-conformant or erroneous use of the tools and data. Those who err, even unintentionally, must be punished and the system for providing compensation to those who suffer damage must be clear. |
| Guarantee of data protection, clarity in information to citizens, more flexibility, greater choice of options for choosing privacy 'settings' for one's data | Fear of losing control over one's personal data | • Guarantees and transparency concerning data collection methods (when data is collected and why).<br>• Possibility of giving partial consent for acquisition (use) of data, without precluding use of the technologies (e.g., use of applications).<br>• The request for authorisations for data processing must be made in a concise and universally easy-to-understand language (e.g., in table form).<br>• Laws that guarantee the above and protect citizens' data. |
| Consent, Clarity, Harmonization of laws, limit use by private entities, stimulate innovation. | Use of DPI and geolocation technology for security and commercial purposes. | 1. Consent – Provide greater possibilities to citizens to give their consent to use of these technologies: in the case of geolocation, provide more than one option for excluding the possibility of being located<br>2. Clarity – Clearer information and regulations are required, above all in the field of privacy, so that citizens will know what to expect when they give their consent to use their personal data<br>3. Harmonisation of laws – Common regulations and possible international agreements, beginning with EU-U.S. but extensible to the rest of the world, are necessary in order to guarantee a common system of regulation of online spaces<br>4. Limit use by private subjects – Certain invasive technologies such as DPI should be used only by institutions clearly responsible for guaranteeing citizens' security. Use of certain invasive technologies by private subjects should be limited if not prohibited.<br>5. Stimulate innovation – The system of regulations must not interfere with research and technological innovation. |

| | | |
|---|---|---|
| The participants are in agreement on use of SOSTs and request that use be strictly circumscribed to national security. | The participants feel that DPI and geolocation are highly effective tools for identifying criminals and therefore feel that use by countries, for national security, is desirable. Nevertheless, they feel that it is necessary to identify limits beyond which surveillance becomes infringement. | The recommendation is addressed to European stakeholders. We recommend a specific regulatory system for the SOSTs, with clear and transparent laws. In particular, we recommend a form of 'control of the controllers', including recourse to super partes figures which can supervise and control the use made by national governments of the technologies examined. In this sense, a European Guarantor could fill this role. |
| International regulation. | Use of DPI and geolocation technology for security and commercial purposes. | Provision for a regulation, a sort of code which must be signed by all the countries and which calls for:<br>- Greater information for citizens concerning surveillance systems;<br>- Greater transparency concerning who manages data and how data is managed;<br>- A requirement for the data controllers to respect citizens' right to privacy. |
| Regulation and ways of controlling technologies. | Use of DPI and geolocation technology for security and commercial purposes. | Greater transparency by the telephone companies, software and applications companies<br>Create educational initiatives to raise awareness, among children, of the SOSTs and give them the tools to select and use them correctly.<br>PROVIDE THE OPTION OF DECIDING WHEN TO DEACTIVATE SURVEILLANCE AND MAKE IT EASY TO DEACTIVATE<br>Request the administrators to make clear and applicable laws which balance security and transparency |
| Regulation and protection of rights. | Use of DPI and geolocation technology for security purposes. | To the European Parliament and the European Commission.<br>Regulate and define, by law, the subjects who may collect data and may access data, in what measure, and for what purposes.<br>Establish the duty to inform citizens of the fact that they are monitored, and by whom and by what means.<br>Restrict the possibility to collect data in certain places or data on certain categories of persons, or data on religious, political, and social affiliations except when by judicial authorisation. |

| | | |
|---|---|---|
| Proposal for a framework (fundamental) law for safeguarding citizens' rights | Legislative vacuum. | We propose drafting a proposal for a fundamental law protecting citizens' rights at three levels:<br>1) identification of subjects authorised to manage data which transits via use of SOSTs, thanks to a public register which identifies the scope and functions of the subjects' activities. Drafting of a list of cases in which said subjects are authorised to collect and use data.<br>2) Extension of these regulations even to countries in which the data transits but which do not subscribe to European laws and regulations.<br>3) Protection of the rights of citizens to be informed: through sensitisation campaigns to raise their awareness of the 'weight' of the capabilities of the new technologies to capture their data; requesting the collaboration of the manufacturers of technological apparatuses (smartphones, etc.) to include, with the products, of written notes and manuals which inform citizens of the monitoring activities which can be carried on via the SOSTs. |
| Information and education for citizens. | Lack of information. | The citizens recommend that politicians and competent bodies prepare courses for providing information and instruction about the technologies discussed and how they operate, and about the forms of monitoring correlated with each. Additionally, in the name of transparency and completeness of information, the above-mentioned courses should also provide information relative to the activities carried on by private and public companies which have recourse to use of these technologies.<br>The above-mentioned courses could be held, first of all, at the level of the schools, but not be limited thereto. We recommend holding courses at the municipal level as well, for the entire citizenry and, obviously, free of charge. The citizens feel that these courses would have the advantages of heightening awareness, encouraging informed use, and imparting the information technology skills needed to use these technologies, among/to the entire population. |
| National and international laws. | Legislative vacuum. | We recommend that Italian and European politicians legislate national- and international-level laws which can guarantee:<br>- Efficacious use of the technologies for security purposes;<br>- Transparency concerning access to the data collected via use of these technologies;<br>Legitimatise individual citizens to take action against private bodies and public institutions to oppose abuses arising in connection with/from use of the technologies and the data collected using them. |

## 10.2 Postcards

### *Template*



### *Postcards - content*[158]

| **Recommendations to European Policy makers** |
|---|
| More information to citizens, who are sometimes excluded from the developments, be them positive or negative, of the Internet because of their age or their social status. |
| I would recommend to politicians to read "Discipline and Punish: The Birth of the Prison" by Foucault and "Panhopticon" by Bentham on social control. This would teach them to evaluate the risks of an economic and social system that controls and directs our lives and in which security is of little or less importance. |
| Do something for the school in Italy!! |
| I would like to suggest an awareness raising campaign for users aimed at protecting their rights, alerting them of the risks connected to the use of the different devices and advising them on how to use the devices safely. Technology producers could participate, by adding an informational booklet on the tracking of data and people to the users manual. |
| The following things would be needed:<br>Urgent regulation on websites and shocking content.<br>Stronger protection of minors and educational programs on public sharing of personal images. |

[158] Translated from Italian

| |
|---|
| Prevention of stalking (regulation of smartphone location tracking).<br>Thank you for this opportunity. |
| It is very important to use the new technologies or alternative methods for the security of all the citizens but the people who use them should guarantee opennes, efficiency and transparency. |
| Taking into consideration that we are entering a situation of erosion of rights and of entrusting decision making to non-elected organs (ECB, European Commission, the new Senate envisioned by the Renzi reform, metropolitan cities) it is important not to allow any endangerment of individual rights and freedoms. The advantages for security have to be clear and proved, not just alleged. They cannot be used to justify the erosion of individual freedoms. |
| The new European Commission should issue a directive to:<br>Request every member state to identify an authority in charge of these issues;<br>Establish common rules;<br>Establish a supervision authority at the European level;<br>Set sanctions for violations. |
| The current system does not even guarantee the security of the European politicians! How can we trust and give our data to people who can not protect themselves?! |
| Promote information campaigns aimed at a greater awareness and participation of citizens in public life. It is of the utmost importance to have a detailed regulation and supervision/monitoring of the application of the laws and of the "controllers". |
| I would like to know alternative procedures instead of DPI.<br>I would also like to know better how to defend myself from DPI abuses, if any. |
| To enact laws for the protection of the privacy of citizens. Increase controls on public bodies and against crime. |
| I would like to add something on medical data collection: the easy access via microchip to our own medical situation is not possible yet. There is no meritocracy in Italy. |
| We need to ask ourselves what is more important between privacy and security. Technology needs more regulation and security and this means a necessary "violation"of privacy. |
| To reduce the sphere of influence of surveillance we need to have more information. |