FP7-285556 SafeCity Project

Draft Deliverable D7.1

Title: Social, Ethical and Legal Implications

Deliverable Type:	**CO**
Nature of the Deliverable:	**R**
Date:	**31/10/2012**
Distribution:	**WP7**
Editors:	**ARATOS**
Contributors:	**HI-IBERIA, MCC, KEMEA, EVERIS, CSSC**

***Deliverable Type:** *PU= Public, RE= Restricted to a group specified by the Consortium, PP= Restricted to other program participants (including the Commission services), CO= Confidential, only for members of the Consortium (including the Commission services)*

**** Nature of the Deliverable:** *P= Prototype, R= Report, S= Specification, T= Tool, O= Other*

Abstract: This document defines the set of implications found across the SafeCity project, with according reference to the respective regulations.

DISCLAIMER

The work associated with this report has been carried out in accordance with the highest technical standards and SafeCity partners have endeavored to achieve the degree of accuracy and reliability appropriate to the work in question. However since the partners have no control over the use to which the information contained within the report is to be put by any other party, any other such party shall be deemed to have satisfied itself as to the suitability and reliability of the information in relation to any particular use, purpose or application.

Under no circumstances will any of the partners, their servants, employees or agents accept any liability whatsoever arising out of any error or inaccuracy contained in this report (or any further consolidation, summary, publication or dissemination of the information contained within this report) and/or the connected work and disclaim all liability for any loss, damage, expenses, claims or infringement of third party rights.

List of Authors

Partner	Authors
ARA	Myrto Zacharaki, Giorgos Kostopoulos, Stauroula Stoumpou, Stratoula Kalafateli, Nikos Bogonikolos
CSSC	Dimitris Dimitriou
HIB	Anna Mereu, Roberto Gimenez, Roberto Gómez, Jaime Campos
EVE	Mario Carabaño Marí, Jose María Balboa
MCC	Sara Gutiérrez Olivera

Document History

Date	Version	Editor	Change	Status
20110518	0.1	[ARA] Myrto Zacharaki Giorgos Kostopoulos	First Draft of SafeCity WP7 D7.1 Template	Draft
20110903	0.2	[ARA] Myrto Zacharaki Giorgos Kostopoulos	Updated structure and ToC	Draft
29092011	0.3	[ARA] Myrto Zacharaki Giorgos Kostopoulos Stauroula Stoumpou [CSSC] Dimitris Dimitriou	Prefinal version, sent to internal review	Prefinal
20111010	0.4	[ARA] Myrto Zacharaki Giorgos Kostopoulos Stauroula Stoumpou [HIB] Anna Mereu Robert Gimenez	Reviewed Prefinal version	Prefinal
20111014	0.5	[ARA] Myrto Zacharaki Giorgos Kostopoulos Stauroula Stoumpou [HIB] Anna Mereu Robert Gimenez [EVE] Mario Carabano Jose María Balboa [MCC] Sara Gutiérrez Olivera	Reviewed Final Version for M6 Review	Prefinal for M6 Review
20111018	0.6	[ARA]	Final text and format adjustments	Final for M6 Review

		Myrto Zacharaki Giorgos Kostopoulos Stauroula Stoumpou [HIB] Anna Mereu Robert Gimenez [EVE] Mario Carabano Jose María Balboa [MCC] Sara Gutiérrez Olivera		
20111024	0.6	[AIT] Tassos Dimitriou	Internal Review	Commented for final editing
20111025	0.7	[ARA] Myrto Zacharaki Giorgos Kostopoulos	Final corrections based on internal reviewer's comments	Final M6 Draft Report
20120327	0.8	[ARA]Stratoula Kalafateli Giorgos Kostopoulos [HIB] Anna Mereu, Roberto Gimenez [CSSC]Dimitris Dimitriou [MCC] Sara Gutiérrez Olivera [EVE] Jose María Balboa Mario Carabano	Traceability matrices listing ethical priniciples and social concerns; update current version containing framework for the protection of individuals with regard to the processing of personal data and on the free movement of such data	A first draft of the new version, waiting for the contribution of all WP7 partners
20120402	0.9	[ARA]Stratoula Kalafateli, Giorgos Kostopoulos	Final integration of partners' inputs	Prefinal – Sent for internal review
20120416	1.0	[HIB] Roberto Gimenez	Final version for M12 release after peer review	M12 release
20120914	1.1	[ARA] Nikos Bogonikolos Giorgos Kostopoulos	Next version taking into account the reviewer's comments during the M12 EC review. Section 6 has been added accesing stakeholdres (DPAs, Data Controllers) and citizen's concerns regarding Safecity applications. Annexes of questionaires and telephone interviews have	Prefinal – Sent for Internal review.

			been added.	
20123009	1.3	[HIB] Roberto Gimenez	Final version for M18 release after peer review	M18 release

Table of Contents

List of Figures

List of Tables

Glossary

Acronym	Meaning
ICT	Information and Communication Technology
EU	European Union
FP7	Framework Programme 7
EC	European Commission
PS	Public Safety
UC	Use Case
PoC	Proof of Concept
ECHR	European Court of Human Rights
CFREU	Charter of Fundamental Rights of European Union
TFEU	Treaty of Lisbon on the Functioning of the European Union

References

Number	Reference
[1]	SafeCity Deliverable D7.2: SafeCity Policy Making
[2]	European Commission, "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", Official Journal of the European Communities, No L 281/31
[3]	European Commission, "Ethical Review in FP7: Data Protection and Privacy Ethical Guidelines", Experts Working Group on Data Protection and Privacy, Chaired by Caroline Gans-Combe, 18th September 2009
[4]	CLASNews, "Who's watching you -and when, Public Surveillance as a Social Issue", presenting the story of Social Scientist Tori Monahan and Professor of Women and Gender studies Jill Fisher, Issue Spring/Summer 2007, pg 13-14
[5]	European Commission, "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector", Official Journal of the European Communities, Official Journal of the European Communities, 31/07/2002,No L 201/37
[6]	European Commission, "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC", Official Journal of the European Communities, 13.4.2006, No L 105/54
[7]	Council of the European Union ,"Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters", Official Journal of the European Communities, 30.12.2008, No L 350/60
[8]	Organic Law 15/1999 of 13 December on the Protection of Personal Data, Spanish Official Journal, 14 December 1999, BOE núm. 298, de 14-12-1999, pp. 43088-43099
[9]	Spanish Data Protection Agency,"21648 INSTRUCTION 1/2006, of 8 November, by the Spanish Data Protection Agency, on processing personal data for surveillance purposes through camera or video-camera systems", Official State Gazette number 296,12 December 2006
[10]	Ministry of Justice of Sweden, "Personal Data Act" ,24 Octomber 1998
[11]	Ministry of Justice of Sweden,"Personal Data Protection", 21 December 2006
[12]	TriData Division, System Planning Corporation, "Mass Shootings at Virginia Tech, Addendum to the Report of the Review Panel", Nov 2009 (Revised Dec 2009)
[13]	European Commission, "Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.", Official Journal of the European Communities ,12.1.2001, L 8/1

[14]	DIRECTIVE 97/66/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector
[15]	Council of Europe member states, "The Convention for the Protection of Human Rights and Fundamental Freedoms", 4 November 1950, Rome. Available online at http://en.wikisource.org/wiki/European_Convention_for_the_Protection_of_Human_Rights_and_Fundamental_Freedoms
[16]	Institutions and member states of the European Union, "Charter of Fundamental Rights of the European Union", 7 December 2000. Available online at http://en.wikisource.org/wiki/Charter_of_Fundamental_Rights_of_the_European_Union
[17]	EU Member States, "The Treaty on the Functioning of the European Union", 13 December 2007, Lisbon Portugal. Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0047:0200:en:PDF
[18]	Spiekermann, S. and Pallas, F., "Technology paternalism. Wider implications of ubiquitous computing" in Poiesis Prax, vol. 4, 2006, pp. 6-18
[19]	DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009, available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF
[20]	The Charter of Fundamental Rights of the European Union. Available online at http://www.europarl.europa.eu/charter/default_en.htm
[21]	The Stockholm Programme. 5 May 2010. Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:0038:en:PDF
[22]	Spanish Organic Act 1/1982, 5th May, about civil protection of Honor, Privacy and Self-Image Rights, available online at http://noticias.juridicas.com/base_datos/Admin/lo1-1982.html
[23]	Instrument of Government Act of 1974 of the Swedish Constitution. Available online at http://www.riksdagen.se/templates/R_Page____6307.aspx
[24]	Spanish Constitution. Ratified by referendum of the Spanish people on December 7, 1978 and sanctioned by His Majesty the King before the Cortes Generales on December 27, 1978.
[25]	Organic Law 4/1997,of 4 August. On the use of videosurveillance by security forces in public places
[26]	Law 18/1989 of 25 July for Motor Vehicle Traffic and Road Safety, approved by Royal Decree Legislation 339/1990 of 2 March
[27]	Gary T. Marx, *"An Ethics For The New Surveillance", The Information Society, Vol. 14, No. 3, 1998*
[28]	Communication from the Commission to the Council and the European Parliament of 10 May 2005 – The Hague Programme: ten priorities for the next five years. The Partnership for European renewal in the field of Freedom, Security and Justice [COM(2005) 184 final – Official Journal C 236 of 24.9.2005]
[29]	European Parliament, Tampere European Council 15 and 16 1999, http://www.europarl.europa.eu/summits/tam_en.htm
[30]	European Commission, "Communication 'Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century", COM(2012) 11 final

[31]	Antisurveillance, Brian Martin, Published in Anarchist Studies, Vol. 1, 1993, pp. 111-129
[32]	Rachels J (1975), 'Why Privacy is important' Philosophy and Public affairs 4
[33]	Sandberg, A. & Bostrom, N. (2008): Whole Brain Emulation: A Roadmap, Technical Report #2008-3, Future of Humanity Institute, Oxford University
[34]	Jacobi, Anders, and Mikkel Holst, "Synthesis Report _ Interview Meetings on Security Technology and Privacy", PRISE Deliverable 5.8, 2008
[35]	TNS Opinion & Social, "Attitudes on Data Protection and Electronic Identity in the European Union", Special Eurobarometer 359, Brussels, 2011.
[36]	The Gallup Organization, "Data Protection in the European Union: Citizens' perceptions", Flash Eurobarometer 225, Brussels, 2008. http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf
[37]	European Parliament and the Council, "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 on the free movement of such data", *Official*Journal*of*the*European*Communities*, Vol. L 281, 23 November 1995, pp. 31_50.

1. Introduction

1.1 Scope and purpose of this document

During the course of research for designing and implementing the Safe City project, the consortium focused not only on technical and user requirements, but also on concerns of ethical, social and legal nature. Indeed, Public Safety and Surveillance applications are marked by a thin line separating the citizens' security and privacy and a potential abuse of their individual rights. An example set of criteria presented by the Madrid City Council (MCC) when installing new technology is:

- **Applicability:** Is it feasible to achieve the aimed objectives through the use of a certain technology?
- **Need:** Is this the only feasible way to achieve the objectives?
- **Proportionality:** Is this causing more harm than good to the citizens concerned?

The SafeCity project makes use of advanced networking and situational awareness technologies, studied at the level of functionalities (SafeCity WP2), an analysis of technical requirements (SafeCity WP3) and an actual experimentation plan (SafeCity WP4). We have in parallel looked into the transparency of the planned developments and technical definitions, so as to ensure their compliance with personal rights protections and respect of social and legal integrity. In fact, the current research upon social, ethical and legal implications looks into the general framework of the SafeCity concept and although most references shall be defined with respect to the WP4 trials, we will also consider the definitions and plans to be developed in Phase 2 Implementation. Indeed, the current document is developed in parallel with SafeCity deliverable D7.2 [1] which explores the design of policies for the SafeCity project and according Public Safety UCs.

Public Safety Use Cases make use of surveillance techniques and modern ICT technology which introduce a lot of considerations regarding legal, ethical and even social implications. Social exclusion, trespassing of individuality and privacy, malicious use of sensitive data and decisions made towards their management are only some general indicators of potential misguidance when applying new technological innovations. Additionally, the use of personal data, such as acquisition of images and location information by Public Safety applications, entails the risk and responsibility of being aware of a citizen's profile. When this citizen is considered as being a criminal, would monitoring his/her actions be legal? Up to which level? Using which applications? And how can we define a priori who is to be monitored or not? Even so, how can we be sure that the technology applied to capture such criminal profiles ultimately does not result in the burdening of the other citizens' well being?

All these considerations have been defined with reference to existing legislations, regulations, ethical discussions and social concerns and analyzed in Sections 2, 3 and 4, respectively. Section 1.2 introduces an overview of all these "hot" topics while Section 5 is the heart of the deliverable. Based on the legal, social and ethical analysis presented in the previous sections, Section 5 aims in shaping the frameworks upon which the SafeCity project needs to operate, and analyzing the implications found across the SafeCity development. Basic descriptions and considerations are included in that part while more in depth analysis and long-term expectations are further discussed in [1].

1.2 Sensitive Cases and Implications raised in Public Safety Scenarios

In the following sections we present an analysis of social, ethical and legal considerations met in Public Safety Use Cases, as these have been identified by EU and nation-wide legislations, FP7 ethical

guidelines and other relevant research. Additional inputs have been received from end-users analyzing city scenarios in the project (SafeCity WP2, T2.1).

Section 2 presents the **legal implications** found with respect to the technology and methodologies used. Our research focused initially on an EU-wide scale, searching for legislations that must be followed by each member state. Then we emphasized on the national specifications of Spain and Sweden, the two areas where the SafeCity project shall be tested in practice. Legal implications include issues which are too severe and sensitive to be handled by personal judgment and thus, appropriate rules need to be followed by all their respective citizens. Examples of such sensitive cases include (1) the permission or not of sensor cameras to be installed in public places for citizen behavior surveillance (clear identifications of no alternate means to capture crime should be justified), (2) the temporal storage capacity of the data being acquired, which should not exclude a given timeframe (usually varies per member state), (3) the responsibility of data collectors for the security of the data against theft, corruption and malicious use, etc.

Section 3 presents the **social implications** that have been investigated. Social science looks into the relationship of citizens with technology and the interaction amongst them. In that sense, social implications are related to the problems raised within the society from the application of new policy, methodology and technology, given that citizens are not passive but rather reactive beings. As a result, the society's equilibrium as a whole could be in question when human relations lose trust. Our research focused on related social research projects and examined how advances in technology need to be carefully regarded with respect to the social consequences they cause. Examples of such consequences include (1) mistaken re-assurance of the reliability offered by surveillance technology, (2) social divide, being translated in national, religious and other categorizations based upon the criteria found to unite criminal behaviors, (3) digital divide, arising from the heterogeneity of technology access across citizens, etc.

Finally, **Section 4** presents the **ethical implications** met**.** Ethical considerations are related to social concerns but, while the latter focus on the societal well-being, ethical questions are related to individuals. Although many of the considerations met in ethical implications are pretty much covered by legislations, many decisions are often left to the management of the technology and methodology delivery. Ethical considerations relate to the ethical concerns which should be followed by providers, practitioners and decision-makers so as to ensure a fair research framework. Examples of such concerns include (1) commitment to the protection of the ethical data acquired from the source to the processing end (secure protocols, authorized databases, responsible sharing, etc), (2) definition of objective criteria (upon processing algorithms, data mining techniques, etc) towards characterization of a suspect, (3) respecting citizens' rights, even when suspected, with regards to the access of their own personal data, etc.

2. Legal Framework

Following the EU's FP7's guidance for ethical and respectful research, we need to ensure that the technological solutions that we provide are indeed **beneficial** and **human-driven**. The legal aspects analysis that has to be taken into account starts with an overview of Human Rights, described in Section 2.1, which **explains everyone's right to privacy**. In Section 2.2 the Right to Data Protection in the Legal Framework is described. The general regulatory framework of European Union for Telecommunications is described in Section 2.3.

However, while EU provides a set of uniform policies concerning individual rights to be followed by all member states, Public Security, Defense and State Security are outside the competence of EC. As different regional, cultural and political frameworks exist across the member states, some more specific national-level laws and regulations are also being reported in order to describe each area's restrictions and tolerances [2].

The Stockholm Programme [21] sets forth the European Union's (EU) priorities regarding the areas of justice, freedom and security for the period 2010-14. Building on the achievements of its predecessors, Tampere [28] and Hague [29] programs, it aims to further strengthen the area of justice, freedom and security with actions focusing on the interests and needs of citizens. This Programme defines strategic guidelines for legislative and operational planning within the area of freedom, security and justice in accordance with article 68 of Treaty of Lisbon on the Functioning of the European Union (TFEU), attributing the Commission only the right of initiative, without prejudice to the possibility that Member States take initiatives in accordance to article 76 TFEU. For this reason, in Section 2.4 we have also referenced a set of national-level legislations regarding the cities explored under the scope of the SafeCity project's PoCs: Madrid, Spain and Stockholm, Sweden.

2.1 Right to privacy: The Human Rights Perspective

Human rights, pursuant to the Universal declaration on Human Rights, the European Convention on Human Rights (ECHR)[15] and to the Charter of Fundamental Rights of the European Union (CFREU)[16], constitute a first layer of general constrains. Among Human Rights, the following sections (2.1.1-2.1.3) elaborate on those that are particularly relevant in the hypothesis of public safety applications, as these are objects of investigation in the SafeCity project. The following are also valuable points to be considered in the ethical and social implications raised.

2.1.1 European Convention on Human Rights (ECHR)

Article 8, ECHR: **Respect for private and family life, home and correspondence**. The scope of **the right to privacy, from the intimacy of the home, has been gradually extended** by the European Court on Human Rights to portions of peoples' lives that are not necessarily "intimate" strictly speaking, **and may be relevant to personal behaviors, attitudes, held outside personal homes and private premises**. In fact, the scope of privacy is thus not limited by the non-intimate nature of personal information or acts concerned, nor by their public occurrence. **Individuals enjoy a right to privacy even with regards to behaviors, attitudes and communications in public spaces like streets, shopping malls, airports or even at work.** This means that recording, storage and use of information related to individuals in these places constitutes an invasion of their privacy that must, in order to be lawful, comply with the conditions set at article of the European Convention of Human Rights:

> *"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security,*

public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Article 9, ECHR: **Freedom of thought, conscience and religion** including freedom, either alone or in community with others and in public or private, **to manifest one's religion or belief, in worship, teaching, practice and observance**;

Article 10, ECHR: **Freedom of expression** including freedom to hold opinions and to receive and impart information and ideas, without interference from a public authority, regardless of frontiers.

Article 11, ECHR: **Freedom of peaceful assembly** and freedom of association with others, including the right to form and to join trade unions for the protection of his interests.

Article 14, ECHR: **The right to enjoy these freedoms without discrimination on any ground such as sex, race, color, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.**

2.1.2 Charter of Fundamental Rights of the European Union (CFREU)

Article 1, CFREU: **Human dignity is inviolable**. It must be respected and protected. The principle of human dignity attests to the fundamental and guiding role occupied, in our western legal culture, by the ethical imperative of conceiving and **dealing with human beings always as ends in themselves and never as means to an end**.

Moreover, Article 8, CFREU says that "*Everyone has the **right to the protection of personal data** concerning him or her. **Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified***."

Article 26, CFREU states t**he right of persons with disabilities to benefit from measures designed to ensure their independence**, social and occupational integration and participation in the overall community life.

2.1.3 Treaty of Lisbon on the Functioning of the European Union (TFEU)

On December 2009, with the entry into force of the Treaty of Lisbon, The Charter of Fundamental Rights became legally binding on the EU institutions and on national governments, offering the European Union new instruments regarding the protection of fundamental rights and freedoms.

Article 16 of the Treaty of Lisbon on the Functioning of the European Union (TFEU) [17] enacts a general constitutional provision on data protection by stating the following:

*"**Everyone has the right to the protection of personal data concerning them.***

*The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the **rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data**."*

2.2 EU Legal Framework for Data Protection and Privacy

The protection of personal data is one of the most important issues raised in the European Union Regulatory Framework and an extensive work has been carried out in order to obtain a comprehensive European Directive that regulates the management of personal data in the European Union. In fact, personal data is collected and used in many aspects of everyday life and can be collected directly or indirectly from the individual or existing databases; moreover, these data can be used for different

purposes than the ones initially appointed. Additionally these data may be available in places different from the original location, so that data related to the citizens of one Member State can be used in other Member States of the EU. This raises the necessity of a European regulation framework to handle and protect this data by overcoming potential discrepancies among national laws. Furthermore, some Member States did not have laws on data protection. For these reasons, there was a need for action at European level, and this took the form of EC Directives.

2.2.1 Directive 95/46/EC

The Protection of Private Data Directive 95/46/EC is a directive adopted by the European Union designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data [2]. It includes all key elements from article 8 of the European Convention on Human Rights, which states its intention to respect the rights of privacy in personal and family life, as well as in the home and in personal correspondence. The Directive 95/46/EC was developed to harmonize national laws for personal data protection and movement of data, based on the existing national legislations of the EU Member States.

The Directive 95/46/EC is the reference text, at European level, on the protection of personal data. It sets up a regulatory framework which seeks to strike a **balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union (EU)**. To do so, the Directive sets strict **limits on the collection and use of personal data** and demands that each Member State sets up an independent national body responsible for the protection of these data. The Directive 95/46 EC includes the main legislative principles applicable to all processing of personal data and all the use cases and scenarios of SafeCity project will have to be subject to this directive.

In the context of the Directive, **personal data is defined as *"any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"*** (Article 2a).

2.2.1.1 Legitimacy of Data Processing

Article 7 of the EC Data Protection Directive 95/46 lists the following basic principles to be followed for the protection of personal data:

(…) personal data may be processed only if:

- The data subject has unambiguously given his consent; or
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- Processing is necessary for compliance with a legal obligation to which the controller is subject; or
- Processing is necessary in order to protect the vital interests of the data subject; or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1

2.2.1.2 *Obligations for Data Quality*

Article 6 of the Directive 95/46/EC specifies the following requirements relating to the data quality:

- Member States shall ensure that personal data must be:
  - Processed fairly and lawfully;
  - Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
  - Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
  - Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
  - Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.
- The controller must ensure compliance with paragraph 1. This means that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. An acceptable way of dealing with the apparent contradiction between the requirement of purpose-specificity of personal data processing and the need for incremental adjustment of whatever system is in place, may be continuous monitoring of the system evolution as well as evolving personal data protection needs.

2.2.1.3 *Exemptions and restrictions*

Article 13.1 of the Directive 95/46/EC sets up a restriction to the obligations and rights provided for in article 6.1 (data quality), 10 (information in cases of collection of data from the data subject), 11.1 (information where the data have not been obtained from the data subject), 12 (right of access) and 21 (publishing of processing operations) when necessary to safeguard:

a. national security;

b. defence;

c. public safety;

d. the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions.

2.2.1.4 *Security of processing*

According to articles 16 and 17 of the directive 95/46/EC, the controller "must, where processing is carried out on his behalf**, choose a processor providing sufficient guarantees in respect to the technical security and organizational measures governing the processing to be carried out, and must ensure compliance with those measures**." (article 17, §2). Furthermore, "**Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to**

personal data, must not process them except on instructions from the controller, unless he is required to do so by law" (article 16).

2.2.1.5 Entry into force and implementation by national legislations

Pursuant article 32 "*Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the end of a period of three years, the latest, from the date of its adaptation*"

The European countries have complied with this Directive by means of the national acts collected in the table below:

COUNTRY	STATUS OF LEGISLATIVE PROCEDURE	ENTRY INTO FORCE OF 1st REGULATION
Belgium	Consolidated text of the Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data Modified by the implementation law of December 11, 1998 (O.J. 3.2.1999) Secondary legislation adopted on 13 February 2001 and published in the Official Journal of 13 March 2001.	1992
Bulgaria	Law for Protection of the Personal Data promulgated in the State Gazette 1/4 Jan 2002, Amended in State Gazette, 70/10 August 2004, Amended in State Gazette 93/19 October 2004, amended in State Gazette 4/20 May 2005 Amended in State Gazette 103/ 23 December 2005, amended in State Gazette 30/11 April 2006 Amended in State Gazette 91/10 November 2006, amended in State Gazette 57/13 July 2007	2002
Czech Republic	Consolidated version of the Personal Data Protection Act 101 of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts	2000
Denmark	The Act on Processing of Personal Data (Act No. 429) of 31 May 2000	2000.
Germany	The Federal Data Protection Act (Bundesdatenschutzgesetz) was adopted 18 May 2001, published in the Bundesgesetzblatt I Nr. 23/2001, page 904 on 22 May. The Federal Data Protection Act applies to the federal publicsector and the private sector	2001.
Estonia	Data Protection Act passed on 12 February 2003	2003
Greece	Implementation Law 2472 on the Protection of individuals with regard to the processing of personal data	1997
Spain	Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. ("B.O.E." núm. 298, de 14 de diciembre de 1999	2000
France	Law 2004-801 modifying law 78-17 of 6.1.1978	2004
Ireland	Data Protection Act 1988 Data Protection (Amendment) Act 2003 enacted on 10 April 2003	1998

Italy	Protection of individuals and other subjects with regard to the processing of personal data Act no. 675 of 31.12.1996 New Data Protection Code - 2004	1997
Luxembourg	DPL approved on 2 August 2002 and published in Memorial A 91 of 13 August 2002	2002
Hungary	Act LXIII of 1992 on Protection of Personal Data and Disclosure of Data Public Interest	1992
Malta	Data Protection Act of December 14 2001 (Act XXVI of 2001), as amended by Act XXXI of 2002 -	2003
The Netherlands	Personal Data Protection Act (Wet bescherming persoonsgegevens), Act of 6 July 2000 -	2001
Austria	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000), BGBl. I Nr. 165/1999, idF. BGBl. I Nr. 136/2001 of 17.08.1999 that applies to all processing by automatic means. Amendment to the "Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000) by Bundesgesetz, mit dem das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert wird (DSG-Novelle 2010), BGBl. I Nr. 133/2009 of 30.12.2009".	2000
Poland	Act of August 29, 1997 on the Protection of Personal Data, amended January 1, 2004, March 1, 2004, May 1, 2004	1997
Cyprus	The Processing of Personal Data (Protection of the Individual) Law of 2001 (Amendment (Law No. 37(I)/2003)	2001
Latvia	Personal Data Protection Law Amended by Law of 24 October 2002	2002
Lithuania	Law on Legal Protection of Personal Data of 21 January 2003, No. IX-1296, With amendments of 13 April 2004	2003
Portugal	Directive implemented by Law 67/98 of 26.10.1998. 'Lei da protecçao de dados pessoais'-	1998
Romania	Law no. 677/2001 of 21st of November 2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data Law no. 102/2005 regarding the setting up, organisation and functioning of the National Supervisory Authority for Personal Data Processing	2001
Slovenia	Personal Data Protection Act (Published in Official Gazette of the Republic of Slovenia No. 9/1990; New Personal Data Protection Act (Published in Official Gazette of the Republic of Slovenia No. 59/1999; Entry into force: 07.08.1999) Amending the Personal Data Protection Act (Published in Official Gazette of the Republic of Slovenia No. 57/2001 New Personal Data Protection Act (Published in Official Gazette of the	1990

	Republic of Slovenia No. 86/2004;	
Slovakia	Act No. 428/2002 Coll. on Protection of Personal Data, as amended by the Act No. 602/2003 Coll., Act No. 576/2004 Coll and the Act No. 90/2005 Coll.	2002
Finland	The Finnish Personal Data Act (523/1999) was given on 22.4.1999 Act on the amendment of the Finnish Personal Data Act-2000 Finnish data protection act in working places -2004	1999
Sweden	Directive implemented by SFS 1998:204 of 29.4.98 and regulation SFS 1998:1191 of 03.09.98 -	1998
United Kingdom	Data Protection Act 1998 Secondary legislation passed on 17.02.2000	1998
Liechtenstein	Gesetz vom 17. September 2008 über die Abänderung des Datenschutzgesetzes Verordnung vom 9. Dezember 2008 über die Abänderung der Datenschutzverordnung Gesetz vom 11. Dezember 2008 über die Abänderung des Datenschutzgesetzes Verordnung vom 14. Juli 2009 über die Abänderung der Datenschutzverordnung	2008
Norway	Act of 14 April 2000 No. 31 relating to the processing of personal data	2000

Table 1 EU Countries complied with the Directive 95/46/EC

2.2.2 Regulation (EC) No 45/2001

The regulation focuses on issues concerning the protection of individuals with regard to the processing of personal data, by Community Institutions and bodies, and on the free movement of such data [13]. This Regulation contains guidelines aiming to secure personal data processed by European Union (EU) institutions and bodies. These provisions aim to ensure a high level of protection for personal data managed by Community institutions and bodies. In particular, as stated in Directive 95/46/EC, such data have to be (a) **processed fairly and lawfully**, (b) **collected for specified, explicit and legitimate purposes** and not further processed in a way incompatible with those purposes, (c) relevant and **not excessive in relation to the purposes for which they are collected and/or further processed**, (d) **accurate and, where necessary, kept up to date**, and (e) kept in a form which **permits identification of data subjects for no longer than is necessary** based on the purposes for which the data are collected or for which they are further processed, (f) processed for purposes other than those for which they have been collected if the change of purpose is expressly permitted by the internal rules of the Community institution or body.

In the scope of this Regulation, personal data may be processed only if: (a) it's necessary for the performance of a task carried out in the public interest, (b) it's necessary for compliance with a legal obligation, (c) it's necessary for the performance of a contract, (d) the data subject has given him/her consent, or (e) it's necessary to protect the vital interest of the data subject

This Regulation also provides for the establishment of a "**European Data Protection Authority**", an independent Community authority which monitors the correct application of the data protection rules

by the EU institutions and bodies. Citizens are able to deliver complaints directly with that authority if they consider their data protection rights under the Regulation have not been respected. Each Community institution and body will define at least one person as **Data Protection Officer** for cooperating with the Data Protection Supervisor and ensuring that the citizens' rights are not jeopardized upon their data processing. Citizens receive legally enforceable rights under the Regulation, such as the **right to access, rectify, block or delete personal data** relating to them in files held by the Community institutions and bodies.

Exemption and restrictions of articles; **4.1** (data quality), **11** (Information to be supplied where the data have been obtained from the data subject), **12.1**(Information to be supplied where the data have not been obtained from the data subject), **13** to **17**(rights of the data subject) and **37.1** (traffic and billing data) are allowed to Community Institutions where such restrictions are a necessary measure to safeguard the **prevention, investigation, detection and prosecution of criminal offences.**

2.2.3 Council Framework Decision 2008/977/JHA

The Decision focuses on issues concerning the **protection of personal data processed in the framework of police and judicial cooperation in criminal matters [7]**. This framework decision aims to protect the fundamental rights and freedoms of natural persons when their personal data are processed for the purposes of preventing, investigating, detecting or prosecuting a criminal offence or of executing a criminal penalty. It concerns personal data that are processed in part or entirely by automatic means, as well as personal data forming part of a filing system that are processed by non-automatic means. More specifically, we mention the following areas related to the SafeCity project:

- **Data Processing;** The authorities of Member States may collect personal data only for specified, explicit and legitimate purposes. The processing of these data is permitted only for the purposes for which they were collected and processing for other purposes is allowed only under certain circumstances. In principle, personal data that reveals a person's racial or ethnic origin, political opinions, etc may not be processed. Their processing may be allowed only if it is absolutely necessary and under the condition that appropriate safeguards have been established. Inaccurate personal data must be updated or completed if possible. Once the data are no longer needed, they must be erased, made anonymous or, in certain cases, blocked. The need to store personal data must be reviewed regularly, along with according time limits set for their erasure. Finally transmissions must be logged or documented.
- **Data transmission;** Personal data received from another Member State will be processed only for the purposes for which they were transmitted. In certain cases however, they may be processed for other purposes, for example the prevention of threats to public security. The receiving Member State must respect any specific restrictions regarding to the data provided by the law of the transmitting Member State. Under certain circumstances, the receiving Member State may transfer personal data to third countries or to international bodies, under the Member State's that first made the data available consent.
- **Rights of data subjects;** The data subject must be informed of any collection or processing of personal data relating to him/her, with the exceptional cases of data transfer across member states. However, the data subject may request confirmation on whether data concerning him/her have been transmitted, who the recipients are, what data are being processed, as well as a confirmation that the necessary verifications of that data have been made. In certain cases, Member States may restrict the subject's access to information. Any decision restricting access must be given in writing to the data subject, together with the according legal reasons why. The data subject must also be given legal advice on his/her right to appeal such a decision. The data subject may demand that personal data relating to him/her be rectified, erased or blocked. Any

refusal to that end must be given in writing, along with information to the subject's right on declaring a complaint or seeking a judicial remedy.

- **Safeguarding data processing;** The authorities must take the necessary security measures to protect personal data against any unlawful form of processing. This includes accidental loss, alteration and unauthorized disclosure of, as well as access to, personal data and particularly concerning automated processing of data. Official national supervisory authorities in Member States monitor and advise accordingly upon such applications. To that end, they are granted investigative powers, effective powers of intervention, as well as the power to pursue legal proceedings.

2.2.4 EU New proposed Legal Framework for the protection of personal data

The new legal framework for protection of personal data arises from the need of harmonizing the custody of data protection rights across European Member States; acknowledge under the 95/46/EC Directive. This means that actually exercising such rights is more difficult in some Member States than in others, particularly online. These difficulties are also due to the volume of collected data, and the fact that users are often not fully aware that their personal data is being collected.

This proposed regulation concerns the new legal framework for the protection of personal data in EU as set out in Communication COM "Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century". [30]
The goal of this new legal framework proposed by the Commission is to strengthen data protection rights, to give individuals efficient and operational means to fully inform the data subject about the processing of their personal data and to enable them to exercise their rights in a more efficient way.

It consists of two legislative proposals:

- a proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), and
- a proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

This legal framework proposed about data protection legislation has been previously consulted, by the Commission on the following events:

- Joint High Level meeting on Data protection "Data protection: from European to international standards" on 28 January 2011, where the European Commission, the Council of Europe and its Member States celebrated Data Protection Day for the fifth time. This event gave the opportunity to discuss about future European rules on data protection as well as international standards.
- Strategic Communication on November 4th 2010: the Commission adopted a comprehensive strategy on data protection in the European Union highlighting its main ideas and key objectives on how to revise the current rules on data protection.

- Targeted stakeholders' consultations in 2010.

- Organization by the Commission in May 2009 of a wide stakeholders' conference on data protection and launch of a public consultation about the future legal framework for the

fundamental right to protection of personal data in the EU. The public consultation was concluded in December 2009.

2.2.4.1 *Proposal for a Directive of the European Parliament and of the Council (COM 2012.10 FINAL)*

The scope of this Directive is the processing of personal data by competent authorities with the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, clearly related with SafeCity Project.

The main issues, related to the Project, are:

Regarding rights of the data subject and its limitations and/or restrictions:

- **Information and Access right** can be limited by Member States in the following situations:
    a. to avoid obstructing official or legal inquiries, investigations or procedures ;
    b. to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties;
    c. to protect public security;
    d. to protect national security;
    e. to protect the rights and freedoms of others.
- **Rectification and Erasure right** can be refused by the national controllers by means of writing notice containing the reasons and the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.

Regarding the controller and the processor, that shall adopt appropriate measures for:

- Keeping the required documentation for the processing of personal data
- Prior consultation of the supervisory authority, in particular when using new technologies
- Security of processing
- Designating a data protection officer

2.2.4.2 *Proposal for regulation of the European Parliament and of the council (COM 2012.11 FINAL)*

According to the Article 1 of the proposed Regulation, it *"lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data. This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data".*

The regulation defines as processing of personal data *"any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction".*

Although the scope of this Regulation does not apply to the processing of personal data "*by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties*", closely related to SafeCity Project, its analysis, described hereunder, is interesting because of the target of the solution.

The Regulation applies to the controller or processor establish in the European Union, and as novelty regarding legislation in force, applies to "the processing of personal data of data subjects residing in the EU by a controller not established in the EU"

2.2.4.3 Principles regarding Personal Data Processing

The article 5 of the regulation defines the principles concerning personal data processing as reflected in Article 6 of the Directive 95/46/EC, expressed on previous paragraph **2.2.1.2 Obligations of Data Quality**, and Regulation (EC) No 45/2001, but adding the following:

"*Personal data must be: […]*

(f) *processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation*".

2.2.4.4 Rights of the data subject

Chapter III of the proposed Regulation develop the subject rights (access, rectify, block and delete rights), established by the Directive 95/46/EC and the Regulation (EC) No 45/2001, for the scope of this new legal European framework.

The Regulation incorporate the **right to be forgotten**, not contained in legislation in force, meaning "the abstention from further dissemination of such data".

2.2.4.5 Data protection by design and default

The proposal of Regulation introduces the concepts:

- Data protection by design, meaning that the controller shall implement and adopt measures "at the time of the determination of the means for processing and at the time of the processing itself" for meeting the requirements establish in this Regulation.

- Data protection by default, meaning the implementation by the controller of mechanism "for ensuring that only those personal data are processed which are necessary for each specific purpose and are especially not collected or retained beyond the minimum necessary for those purposes".

2.2.4.6 Restrictions of data subject rights

European Union or Member States can restrict the rights established in the proposed Regulation with legislative measures by means of one the following circumstances related to security issues:

a. Public security

b. The prevention, investigation, detection and prosecution of criminal offences

c. Other public interests of the Union or of a Member State

2.2.4.7 *Remedies, liability and sanctions*

According to the Regulation every data subject has the right ***to file a complaint with a supervisory authority*** if they consider that the processing of personal data relating to them does not comply with the Regulation. Moreover every data subject has the right ***to a judicial remedy against a supervisory authority.*** Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established. Furthermore the Regulation gives the right to the data subject ***to a judicial remedy against a processor or controller.*** Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.

2.3 EU Legal Framework for Telecommunications

The legal framework that has to be taken into account is the European Legal Framework for Telecommunications. Since the liberalization of the European telecoms market in 1998, the European Commission performs a regulation activity in order to counterbalance the significant market power of former monopolies, ensure universal service and protect consumers, especially those social groups that may otherwise face exclusion. To ensure that telecoms markets benefit from continued market regulation, the Commission oversees the correct implementation and enforcement of the Directives.

It was in 2002 when the European Union adopted a regulatory framework for electronic communications networks and services, covering all forms of fixed and wireless telecoms, data transmission and broadcasting (2nd telecom package). The directives covered different aspects: from consumers' rights to open markets and from radio waves to broadcasting. The regulatory framework was made up of a package of legal instruments:

- Directive (2002/21/EC) on a common regulatory framework
- Directive (2002/19/EC) on access and interconnection
- Directive (2002/20/EC) on the authorization of electronic communications networks and services
- Directive (2002/22/EC) on universal service and users' rights relating to electronic communications networks and services
- Directive (2002/58/EC) on **privacy and electronic communications**
- Directive (2002/77/EC) on competition in the markets for electronic communications services
- Regulation (2000/2887/EC) on unbundled access to the local loop

Since these rules were agreed in 2002, and due to the fact that this is a fast-developing sector, the European Commission decided that the regulatory framework needed to be revised to ensure that it would continue to serve the best interests of consumers and industry in today's marketplace. An agreement on the EU Telecoms Reform was reached by the European Parliament and Council of Ministers on 4 November 2009, after two years of discussion during the legislative process. The new rules will now need to be transposed into national laws.

The new Telecom Reform package is composed of the following documents:

- "Better Regulation" Directive (DIRECTIVE 2009/140/EC)
- **"Citizens' Rights" Directive (DIRECTIVE 2009/136/EC)**
- Regulation establishing the BEREC (European Body of Telecoms Regulators) and the Office (REGULATION (EC) No 1211/2009)

The agreed Telecoms reform is the result of four years of discussions. In 2007, the Commission proposed a review of the telecoms framework following two years of consultations with stakeholders, with national regulators and with users of telecoms services. The whole telecoms reform package has entered into force with its publication in the EU's Official Journal (18 December 2009). The European Body of Telecoms Regulators BEREC has been established in spring 2010. The next step is the transposition of the telecoms reform package into national legislation in the 27 EU Member States (due by June 2011).

2.3.1 Directive 97/66/EC

The Directive 97/66/EC [14] of the European parliament and of the council of 15 December 1997 concerns the processing of personal data and the protection of privacy in the telecommunications sector [14]. This Directive provides for the harmonization of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community. For SafeCity project purposes, the following articles are of particular interest.

Article 4, **Security**: The provider of a publicly available telecommunications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications network with respect to network security. In case of a particular risk of a breach of the security of the network, the provider of a publicly available telecommunications service must inform the subscribers concerning such risk and any possible remedies, including the costs involved.

Article 5, **Confidentiality of the communication**: Member States shall ensure via national regulations the confidentiality of communications by means of a public telecommunications network and publicly available telecommunications services (this does not apply for any legally authorized recording of communications in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication).

The 1997 directive was replaced in 2002 by Directive 2002/58/EC which updated the data protection rules for this sector.

2.3.2 Directive 2002/58/EC

The directive focuses on issues concerning the **processing of personal data** and **the protection of privacy** in the electronic communications sector [5]. The following definitions apply (article 2 of the directive):

'Traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

'Location data' means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

More specifically, we mention the following areas related to the SafeCity project:

- **Processing Security;** Electronic communications services must be securely protected by their provider by (a) ensuring authorized only personal data access, (b) protecting personal data integrity and (c) ensuring the implementation of a security policy on the processing of personal data. In the case of a personal data breach, the provider must inform the person concerned, as well as the National Regulatory Authority (NRA).

- **Data retention;** The Directive determines that traffic data and location data must be erased or made anonymous when they are no longer required, except if the subscriber has given their consent. Regarding data retention, the Directive states that Member States may withdraw the protection of data only in the exceptional cases of criminal investigations or in order to safeguard national defence and public security. Such action may be taken only where it constitutes a "necessary, appropriate and proportionate measure within a democratic society".
- **Controls;** Member States must implement a system of penalties, in the case of data breach to the provisions of this Directive, and ensure that the national competent authorities have the necessary powers and resources to monitor and control compliance with the national provisions

2.3.3 Directive 2006/24/EC

The directive focuses on issues concerning the **retention of data generated or processed** in connection with **the provision of publicly available electronic communications services or of public communications networks and amending [5]**. The EU Data Retention Directive 2006/24/EC additionally to the directive 2002/58/EC, defines that at member state level each EU country should have their own version of the “data retention” directive embodied and incorporated into their national laws.

The data retention regulations will impact public communication providers (fixed, mobile telecoms, ISPs) that have communications data generated or processed on their networks or from using the services they provide. The regulations require traffic, location and subscriber data to be maintained for a minimum of 6 months up to 4 years. The regulations also outline four data security principles that should apply to retained data:

- **Security;** Data must have the same security levels and quality during their retention period
- **Responsible Management;** Technical and organizational measures must protect against accidental or unlawful disclosure and data loss
- **Accessibility;** Retained data must only be able to be accessed by authorized persons
- **Destruction;** All data retained must be completely destroyed at the end of the retention period
- **Transmission;** When data is requested by law enforcement the data must be able to be transmitted "without undue delay"

2.3.4 Directive 2009/136/EC

The Directive 2009/136/EC [19] amends the Directive 2002/58/EC: the most important corrections are described in the following paragraph. First of all the focus of the directive is enlarged in order to ensure not only the right to privacy but “right to privacy **and confidentiality**”, so as to stress that equal importance has to be devoted for ensuring that “information is accessible only to those authorized to have access” (as from definition of ISO/IEC 27002). Moreover, it corrects the definition of location data by including also the data processed “in an electronic communications network **or by an electronic communications service**”. Processing security will have to ensure that personal data can be accessed only by authorized personnel **for legally authorized purposes**; to protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorized or unlawful storage, processing, access or disclosure; **the implementation.**

2.4 National Level

2.4.1 Spanish Regulations

The usage of images containing identifiable people in the various fields of activity has a series of legal implications. Firstly, anonymous people have the right to not be filmed in public places (nor private ones obviously) unless the filming is covered by the fundamental right to freedom of expression (article 20 of the Spanish Constitution), which includes image rights with the economic element preventing commercial exploitation without the individual's permission. This principle is based on the fact that capturing an image of a recognisable person constitutes personal data and must, therefore, be treated in compliance with relevant data protection laws. Nevertheless, video recordings of the street and of passers-by, is allowed in certain cases for security reasons.

The right to one's privacy, honour and self- image is guaranteed under section 18.1 of the Spanish Constitution and established by Organic Law 1/1982, of 5 May on Civil Protection of the Right to Honour, Personal and Family Privacy and Image. If a person is identifiable or could easily be identified from an image, this is considered personal data. Data protection principles must be applied to the field of video surveillance whenever technical means are used to record, capture, process, store and broadcast images of identifiable individuals, be it live or pre-recorded. **This obligation is not applicable in the following situations**:

- When filming in personal or family surroundings, for example family celebrations, providing the setting remains personal. Internet broadcasting of personal or family recordings would mean going beyond these limits
- When performing informative tasks carried out by media professionals based on article 20 of the Constitution for freedom of information

Any organization that installs a video surveillance system to capture or process images in which identifiable people may appear, must abide by some general principles of conduct in accordance with data protection laws and the Spanish Data Protection Authority's (AEDP) Circulars and Resolutions. It is interesting to note the video surveillance laws differentiation depending upon their subject of surveillance. Below we present two basic overviews regarding Video Surveillance for Public Safety (i.e. crime detection and identification) and Video Surveillance for Road Safety (i.e. traffic cameras).

2.4.1.1 Video Surveillance for Public Safety

Video surveillance carried out by the Law Enforcement Authorities aims at guaranteeing public safety, as well as preventing crime and offences related to public safety. Regarding the video surveillance system and processing controller, the Autonomous Regions are authorized to regulate and allow the Law Enforcement Agencies to use video cameras in this case as well as take custody of the recordings and control image access. Applications regulations to this video surveillance framework are:

- The Organic Law 4/1997 of 4 August specifically regulates the installation of video cameras and recordings carried out by the Law Enforcement Authorities.
- The Organic Law 15/1999 of 13 December for Personal Data Protection (LOPD), Royal Decree 1720/2007 of 21 December Regulation of LOPD, and Instruction 1/2006.

Accordingly, considering the obligations of the controllers, the Organic Law 4/1997 stipulates:

- Authorization for the installation of fixed and mobile cameras
- Provide Public Administrations, Judges and Courts with the images captured
- Offences and fines related to the development of police activity

2.4.1.2 *Video Surveillance for Road safety*

The object of this type of system is to control, regulate, monitor and discipline traffic, as well road safety. Regarding the video surveillance system and processing controller, Public Administrations are authorized to regulate traffic and enable the installation and use of video cameras, a decision marked by the according regulations:

- The Organic Law 4/1997 of 4 August considers the controller to be the person in charge of carrying out the installation and use of video cameras and any other means to capture and reproduce images for the control, regulation, monitoring and discipline of traffic
- The Law 18/1989 of 25 July for Motor Vehicle Traffic and Road Safety, approved by Royal Decree Legislation 339/1990 of 2 March in its Title I, refers to the authorities with the power for carrying out and coordinating motor vehicle traffic and road safety issues
- The LOPD Royal Decree 1720/2007 of 21 December Regulation of LOPD and Instruction 1/2006

Regarding the obligations of the controllers, the Organic Law 4/1997 stipulates:

- Authorization for the installation of fixed and mobile cameras.
- Identification of public roads.
- Measures that guarantee the availability, confidentiality and integrity of the images.
- The body in charge of the custody and processing.
- Provide Public Administrations, Judges and Courts with the images captured.

2.4.1.3 *Data Protection and Processing*

The LOPD, Royal Decree 1720/2007 of 21 December Regulation of LOPD, and instruction 1/2006 complement the above, noting the general data protection obligations according to the general obligations of the video surveillance system controller, as well as the creation of files by means of general regulations. Further to that, we present below a brief overview of the applicable Spanish laws concerning sensitive data management:

In relation with data protection rights, the information presented is acquired from the **Official Spanish Data Protection Agency**, based on the recent increase in premises with cameras and video cameras installed for surveillance purposes in Spain, which has given rise to doubts involving the image processing these systems include.

Precisely, the Spanish Data Protection Agency [9] introduced the Instruction 1/2006 in the International Conference of Data Protection Authorities held in London, November 2006 that deals with the need to adapt video-surveillance to the demands of the fundamental right to data protection and to ensure image processing for the purposes of surveillance complies with and reflects the principles of Organic Act 15/1999 (Spain) [8].

The Spanish Organic Act 15/1999 establishes its scope, between others, is to guarantee Honour, Privacy and Self-Image Rights. It is in overall defined that:

- **Images are considered personal data** (Law 15/1999, article 3) and **graphic or photographic information as also** (Royal Decree 1332/1994, article 1.4)
- **Cameras or video cameras must not amount to the initial means of surveillance**. These systems should be applied only in cases that:
    - It is impossible to adopt other moderate means less intrusive to personal privacy (Principle of proportionality)
    - It is a liable way to achieve the objective proposed

  - It is providing more benefits or advantages for the general interest than damages to other clashing assets or values

- **Omnipresent surveillance must be avoided**
- Creation of a video-surveillance file **requires prior notification to the Spanish Data Protection Agency**

Specifically the articles of the Instruction, based on the principles of the Spanish Organic Act 15/1999, describe the following main areas of focus:

- **Scope;** Processing personal data from images obtained by the Security Forces and Bodies will be governed by the provisions on the matter
- **Legitimacy;** Processing personal data requires the unambiguous consent of the data subject unless the cases:
  - Where the personal data are collected for the exercise of the functions proper to public administrations within the scope of their responsibilities
  - Where they relate to the parties to a contract or preliminary contract for a business, employment or administrative relationship, and are necessary for its maintenance or fulfillment
  - Where the purpose of processing the data is to protect a vital interest of the data subject
  - Where the data are contained in sources accessible to the public and their processing is necessary to satisfy the legitimate interest pursued by the controller or that of the third party to whom the data are communicated, unless the fundamental rights and freedoms of the data subject are jeopardized
- **Information;** Controllers who have video-surveillance systems must place at least one informative sign in the zones under video-surveillance, in a sufficiently visible location, in open as well as enclosed spaces and have forms available to the person/s concerned in which it details the information provided in Article 5.1 of Organic Act 15/1999
- **Principles of quality, proportionality and purpose of the processing;**
  - Images may only be processed when they are adequate, relevant and not excessive with regard to the scope and purposes determined that have justified installation of the cameras or video-cameras
  - Installation cameras or video-cameras will only be considered admissible when the purpose of surveillance may not be achieved by other means that, without requiring disproportionate efforts, are less intrusive to personal privacy and to the right to protection of personal data
  - Cameras and video-cameras installed in private spaces may not obtain images of public spaces except if it is indispensable for the surveillance purpose intended, or if it is impossible to avoid this due to their location
- **Cancellation;** The data will be cancelled within the maximum term of one month from being gathered
- **Notification of files;** Persons or entities intending to create video-surveillance files must previously notify the Spanish Data Protection Agency, for their inscription at the General Registry of same

Further to the above, we also mention the **1978 Spanish Constitution**, under which **data privacy rights are set as Fundamental** ones, fact that reveals the importance of said rights. Additionally, the **Spanish Organic Act 1/1982 upon Civil Protection of Honour, Personal Privacy and Self-Image Rights**, establishes these **rights as no waived, inalienable and indispensable**, and also states that there will be an intromission except otherwise agreed by Law, or by Cultural, Scientific or Historical interest.

2.4.2 Swedish Regulations

Sweden's Constitution, which consists on several different legal documents, contains several provisions that are relevant to data protection; Section 2 of the **Instrument of Government Act of 1974** provides for the protection of individual privacy establishing that "*Everyone shall likewise be protected against body searches, house searches and other such **invasions of privacy**, against examination of mail or other confidential correspondence, and against eavesdropping and the recording of telephone conversations or other confidential communications*" and "*everyone shall be protected in their relations with the public institutions against **significant invasions of their personal privacy**, if these occur without their consent and involve the surveillance or systematic monitoring of the individual's personal circumstances*".

Privacy right, according to their Constitution, can be limited in law in case of: "*protection against any physical violation in cases other than cases under Articles 4 and 5, against body searches, house searches and other such invasions of privacy, against violations of confidential items of mail or communications and otherwise against violations involving surveillance and monitoring of the individual's personal circumstances*" but "*The limitations may be imposed **only to satisfy a purpose acceptable in a democratic society**. The limitation must never go beyond what is necessary with regard to the purpose which occasioned it, nor may it be carried so far as to constitute a threat to the free shaping of opinion as one of the fundaments of democracy. No limitation may be imposed solely on grounds of a political, religious, cultural or other such opinion*".

Section 3 of the same chapter of the Swedish Constitution provides for a right to protection of personal integrity in relation to **automatic data processing**. The same article also prohibits non-consensual registration of persons purely on the basis of their political opinion.

The European Convention on Human Rights has been incorporated into Swedish law in 1994. The ECHR is not formally part of the Swedish Constitution but has, in effect, similar status.

The 1998 Law on Secret Camera Surveillance restricts the use of video surveillance. Permits must be obtained, and clearly visible notices posted, for video surveillance of public places.

It is interesting to note that the Prosecutor General's Office submits a report to Parliament every year with details of all of electronic surveillance conducted. The Swedish Helsinki Committee has concluded that the state interference in the private lives of its citizens lacked in legal rights and transparency. They have recommended better oversight by Parliament of these surveillance techniques as well as an independent assessment of their necessity and effectiveness.

In Sweden, the Data Inspection Board is the public authority responsible for the protection of private data. It guarantees the enforcement of the 1998 Personal Data Act (PDA) which describes the overall legal guidelines enforced in processing of personal data. Related to the protection of private data in surveillance systems it determines additionally to the EU instructions the following [10, 11]:

- **Permitted processing of personal data;** Relating to issues regarding
    - Personal data may only be processed if the registered person has consented to the processing or the processing is necessary in order. If sensitive personal data, data concerning violation of laws, etc. or personal identity numbers or temporary personal identity numbers shall be processed, the processing must always be permitted under the provisions applicable to such data. If personal data is to be transferred to a third

country outside the EU and EEA, processing must also be permissible under the provisions applicable to transfer

- It is illegal to process personal data that could lead to discrimination due to race or ethnic origin, political opinions, religious or philosophical convictions and membership of trade unions. Personal data may be processed without the permission of the citizen involved for research only in the case that the processing has been approved by an ethical review board along with a specific regulation of ethical consideration of research relating to people
- Only authorities should be able to process personal data concerning violations of laws. The prohibition does not apply in civil disputes. Such exemptions will be made by the Government or the Data Inspection Board

- **Certain decisions through data processing;** In the case of automated decisions, there are special cases to request that such decision should be manually monitored. If a decision that has legal consequences for a natural person or has other manifest effects for the person has been acquired solely upon automated data processing, that person is entitled on request to have the decision by a person. Additionally, anybody who has been subject to such decisions has the right to request information concerning what has governed the data processing that generated the decision
- **Rectification;** The controller is liable, upon request, by the registered person, to correct, block, restrict or erase personal data which has not been processed in accordance with the Personal Data Act or regulations issued under the Act
- **Security when processing data;** A person working with personal data may only process the data in accordance with instructions from the controller. If a statute or other enactment contains special provisions concerning the processing of personal data in public operations on such matters, these provisions shall apply. It is the controller who is responsible in relation to the registered person as regards the processing, even if an assistant has been engaged
- **Transfer of personal data to a third country;** In principle, it is forbidden to transfer personal data that is being processed to a third country that does not have an adequate level of protection for personal data. When the transfer is necessary in order that legal claims should be established, exercised or defended, the Government may issue regulations concerning exemptions for transfer of personal data to certain states. As regards matters of computer processing, the Government may do this if it is shown that a third country has a sufficient level of protection for personal data to be transferred or if the transfer is regulated by an agreement that provides sufficient guarantees of the rights of the registered persons or if it is provided that there are sufficient safeguards to protect the rights of the registered persons
- **Notification of processing of personal data;** The PDA defines that it is obligated for the controller to notify all data processing to the Data Inspection Board, which maintains and registers the notifications. The Data Inspection Board and the Government are able to regulate exemptions to bar processing that would result to violation of personal integrity, as also to regulate that in particularly sensitive processing cases the authority must be notified three weeks earlier. The controller is also obligated to provide the information noticed to the authority, to anyone else who expeditiously appeals for it
- **Supervision;** The Data Inspection Board is responsible for entering premises connected with the processing and may banish a processing of personal data that is not fully established as lawful and also apply for the erasure of the data that has been processed in an unlawful manner

The Data Inspection Board has made also made many decisions that concern camera surveillance and form them to special regulations. The 1998 Act on General Camera Surveillance is the most specific and demands a prior permission or just notification in some cases to admit camera monitoring in public places.

3. Social Considerations

Social implications are neither imposed by some legal party nor are they referenced in relevant legislations. They are driven by the social acceptance of the wider public and represent the social opinion and impacts, focusing attention not on the individual, as this is more apparent in ethical considerations, but rather on the society, i.e. the interactions of the individuals.

Under this context, one needs to question the definition of a society, which can be realized under the application of according criteria, such as (a) the **size of the society**: city wide/nation-wide/EU-wide, (b) the **categorization of the society**: spatial/temporal/language-driven/regilious-driven/education-driven (c) the **level of commitment of the society's members**: actors/observers/contributors, etc.

In fact, we believe that there does not exist a single direction to follow and that we therefore need to apply a more complex and dynamic approach. Our goal is to consider the different criteria and determine how these are enforced as a consequence of the technological innovations being studied. In the following, we explore a set of challenging issues related to social balance and well society-living. These are being considered with respect to three of the main technical areas that are catalytic in the SafeCity project's implications:

- **Surveillance**, expanding to
    - *holistic awareness*, being realized by the integration of different sensors allowing information acquisition on multiple levels
    - *city-wide coverage,* implying to ability of a surveillance system to be applied to multiple locations where the citizen may appear
- **Internet and other ICT technologies**
- **Automations**, resulting to minimum human interventions (motion, cognition, creation, etc)

3.1 Implications raised by Surveillance technologies

A first consideration regarding social implication of surveillance systems is related to the fact that most of the these systems change the value and/or meaning of the body from a very private and personal entity to an **exploitable thing**, object of public use and object of study and analysis. Another point is the **invisibility** of the surveillance systems: surveillance systems aim at capturing the identity of an individual the more objectively as possible. For this purpose, the observer must be invisible in order not to influence the observed persons. These concepts mainly have an impact on **democracy** since freedom is limited when individuals are restricted to being bodies without subjectivity.

Another concern arises in correspondence with the analysis of the data about emotional states (where source is facial expressions), whenever the system tries to **give meaning to body motion or expression**. These interpretation results are mostly obtained by means of statistical models. This processing relies on classification and clustering means that are based on the idea of building profiles that allow the control and set up of decisions about people categories: this idea is closely related to the concept of social ordering that excludes people not able to conform to predefined order. In this sense, the processing of body and face video undermines an individual's self-determination due to the categorization of the individual and his/her lack of ability to change the automatic assessment results or contributing to the definition of the categories.(Increased risk of inaccuracy from the use of technology, as more layers of context exist that can be interpreted only by humans.)

Based on the overall considerations related to surveillance societies, social considerations also question **whether such applications are indeed necessary and up to which level**. Many cases exist where attacks

of smaller or greater magnitude have been successfully detected in early stages and prevented a crisis/ crime from occurring. Additionally, many analysts suggest that surveillance technology could have respectively prevented other cases which have tarnished a society's safety, e.g. the Virgina Tech Massacre [12].

Moreover, social scientists insist that in these cases we have to take into consideration the **benefit-cost ratio** e.g. to think about if the social and ethical cost is greater than the benefits we gain using surveillance systems.

However, opposite opinions, like the ones presented by social scientist Torin Monahan [4] point that surveillance cameras can detect and inform a crime scene, assist police officers on capturing a criminal quicker, but **they cannot prevent the crime itself from occurring, nor do they examine the underlying social interactions which have led to the occurrence of the crime in the first place**. Further, they don't deal with the underlying social issues that cause these tragedies to happen in the first place. Worse yet, they can lull us into a false sense of security that may ultimately be counterproductive and even dangerous. Monahan defines surveillance broadly: there's the type of surveillance that's obvious and that is signaled to the citizens with alerts and panels—security cameras, guard gates, tracking devices and even photo radar. And then there's the type that's not so obvious, that pass unnoticed, perform a more subtle surveillance and that seldom are perceived by the citizens as effective means that actually survey and track a person's action or status —intelligent transportation systems, Website cookies and even grocery store "loyalty" cards.

Looking at the issue as a whole it raises questions about how far a society should be allowed to go in scrutinizing its members. "Just because we can do it, doesn't mean we should do it," says Monahan. "For me, it comes down to a question of whether we're looking at the root causes of societal problems or whether we're creating a society that's devoid of trust. At a minimum, I think this deserves to be out there in terms of public debate."

The same source discusses how the advances in technology may not necessarily imply advances in social security and well-being, by saying "**often we, as a society, implement things just because we can. What's possible becomes inevitable. When we're talking about surveillance, we're really talking about control. Sometimes that can be a good thing and sometimes not**" and finally reaching to a question of whether all the related applied technologies do in the end deliver their initial scope, that is making our cities a better place to live, or whether they in the end jeopardize our freedom and quality of life. Notably, Tori Tonahan in this interview poses questions about **whether the new technologies make our lives easier or not, whether citizens end up feeling enabled or limited and in the end of the day more or less secure**.

The LSS Project[1] also recognizes that surveillance technology, and in turn the created "surveillance societies" should be looked on further, beyond the technical achievements, down to the level of social values and interactions.

They argue that the problem cannot be seen as "black and white", meaning that assumptions that technological developments will lead to positive (by reducing criminal attacks) or negative (reconstruction of a "big-brother" society) impacts are both extreme and **ignore the social-technical perspectives and relations between humans, societies and technical innovations**. For that reason, they

[1] Living In Surveillance Societies, funded under the European Cooperation in Science and Technology (COST)

suggest to develop a parallel understanding of technological advances and social experiences/ perspectives in surveillance and respective alternative.

Mr. Brian Martin, a professor of Social Sciences at the University of Wollongong in Australia, in his article "AntiSurveillance" [31] points out that "Opinion surveys regularly show that most people attach great value to their own privacy". According to him codes of professional ethics, laws and regulations have given only an illusion of protection. He states that the basic problem is the digital databases of personal data which are far from secure. He also points out the inaccuracy of these methods and technologies by citing examples of false alarms and incorrect arrests.

When people live together, they observe a lot about each other, and this can be considered a type of surveillance. It occurs in families, among friends, and in close-knit communities. Some of the attention in these circumstances may be resented, but much of it is an inevitable consequence of living as a member of a community. It can be a joy to see friends along the street or in a restaurant or to have them visit your home, even though they thereby know more about what you are doing at any particular time.

Most people are not concerned about "surveillance" in such situations. Why not? In some of the cases, such as meeting friends, there is both a **mutual agreement** to participate and a rough equality of power. But in the case of a parent and a small child, there is an enormous difference in power and no real possibility of informed consent on the child's part. What makes the close watching in this situation acceptable is the trust implicit in the relationship: **the trust** that the parent will look after the child.

According to the above the surveillance systems social implications and concerns apply to cases when either there is a substantial power difference or a lack of a trust relationship, or both between the person the privacy information is related to and those who have access to this information.

Behaviour is shaped according to the function each surveillance system serves, and this is an important parameter.

SafeCity tries to implement the necessary security infrastructure in the smart cities of the future, for *"ensuring people feel safe in their surroundings at time that their surroundings are protected"*. At the end of the day, it all comes down to **assuring a good quality of life**.

Even though authorities warn that only criminals have anything to fear from surveillance equipment, a lot of **citizens feel discomfort** when they know they are being monitored and/or photographed when they are walking on the streets, doing their shopping, going to work and generally living their lives, because technology goes beyond people's reach, and they feel unsafe as to "where" their data will be used, and for what purpose.

Many suggest that the many surveillance societies present symptoms of **lost trust** directed either to the respective authorities, or to their fellow townsmen, ultimately incarnating an Orwellian society[2]. First of all, many citizens question the necessity for these surveillance infrastructures and they do not trust that governments will handle such data fairly, but rather they **fear of corrupted authorities** and twisted evidences towards the accusation of specific groups. Moreover, citizens loss their sense of freedom and they feel imposed under this continuous surveillance. Finally, other groups are strongly influenced by these security measures and thus **lose trust to their neighbors**, people walking on the street, etc,

[2] George Orwell, "1984", New York : Plume, 2003

believing that someone might be a criminal. Under this point, fall many cases of discrimination, falsely arising upon religious, national, etc criteria.

One way proposed to protect privacy is to ensure that all the people who have access to information collected about members of the public deal with it in a "responsible" fashion. This means that those who deal with or have responsibility for information -- such as computer administrators, police, government bureaucrats, telephone technicians and personnel managers -- should have the highest personal standards. For example, they should use the information only for the purposes for which it was collected. Ethics codes are sometimes proposed to set a standard of behavior. But all it takes is a minority of less responsible people for serious breaches of confidentiality to occur. This influences the **confidentiality** of the citizen, which may cause a break with the society. A lot of people doubt the legal implications about privacy assuming that it is risky to rely mainly on governments to provide protection against surveillance when governments themselves are responsible of some misuse of the information or lack of mechanisms to effectively protect private data of the citizens.

According to Bostrom and Sandberg [32]"Hiding an identity is an aspect of privacy, but privacy is actually about controlling who can access an identity, not prevent all knowledge of it. Privacy is not absolute – there are sometimes ethical or legal reasons to limit it – but it is often highly desirable that people can control how their identity can be observed or used."

One could argue that the above are excessive and that they rise from a wanting to a search for a conspiracy behavior, but the truth is that this is the way the general opinion is formed, either due to lack of knowledge, objective experience, personal believes, etc. The importance lies on the **resulting isolation**, **questioning the quality of life produced and whether the citizens do feel safe in the surroundings after all**.

3.2 Implications raised by Internet and other innovative ICT technologies

Globalization and digital convergence in the emerging knowledge society has raised complex ethical, legal and societal issues. We are coming up against complex and difficult questions regarding the freedom of expression, access to information, the right to privacy, intellectual property rights, and cultural diversity. ICT constitutes an instrumental need of all humans to gather information and knowledge, and as such, should be guaranteed as a basic right to all human beings. All over the world, already legally recognized rights are daily being violated, either in the name of economic advancement, political stability, religious causes, the campaign against terrorism, or for personal greed and interests. Violations of these rights have created new problems in human societies, such as digital divide, cyber-crime , digital security and privacy concerns, all of which have affected people's lives either directly or indirectly.

In fact, while technology advances, not all people manage to keep up in speed with it, or even gain basic access to it. A common effect that is present even in developed societies is the phenomenon of **digital divide**, being raised by the heterogeneity of the population and the basic differences and barriers they have to overcome in order to acquire awareness and knowledge on new technological means. For example, in the case of SafeCity, alerting technologies are described to provide direct alerts to subscribed citizens over a cellular-telephony service, online social networks and other social media. However, many groups cannot access or make use of such technology, e.g. low income families, the elderly, etc., and thus they are automatically being excluded from this alerting service. **This digital exclusion holds a strong social character and results to a smaller security assurance for these groups**.

Digital divide can also appear to the work place, referring to older workers who are required to adapt to new technologies and user interfaces, work protocols and procedures. The employee may not be able

to cope with the new advances. Yet, even if the worker is able and willing to adapt, he will be likely to keep his position, even though new generations would be far more competitive.

Finally, the effect of digital divide does not only strike groups unable to cope and access new technologies; **many individuals choose to** live a certain way of life, which is in turn characterized by minimum and/or traditional use of technology, implying that they also **become excluded of some technological privileges**. Even though this is their own choice, the respective authorities should regard that the **innovative routes should not be the sole alternative towards the security assurance of the citizens**.

3.3 Implications raised by Automation technologies

As mentioned above, one important consideration is **whether advancements in technology work in parallel with advancements in the quality life of the citizens**. In the case of the technology studied under the scope of SafeCity project and similar Public Safety UCs, we also examine the potential effect of the use of automated technologies. Many people question the effectiveness of CCTV cameras, suggesting that their actual effectiveness as deterrent crime or even detection of it is still to be justified, and that automated designs and intelligent algorithms could support and optimize these operations. Indeed, end users require that **minimal human intervention** should be needed in the process of detection and perhaps even response phases.

This is expected to reduce the authorities' reaction time and to manage more information effectively, as a human operator can only study limited amount of input data per minute. Additionally, objective estimations upon the definition of a criminal behavior can be limited if such decisions are translated into machine language and video processing algorithms. However, while this is an innovative approach we should consider its effect not as much to the citizens, but rather to the human operators being replaced. Machine automation ultimately results causing inertia in certain groups. Such inertia can be described across the following directions:

- **Actual activity process**, meaning that a human operator could lose his/her job since most of the work can be done by a machine
- **Cognition effort and overall judgment**, meaning that machine frameworks is expected to relief human operators, but ultimately leadings us in too much dependency and reliance for producing a result and generating an opinion; this is overall very important, let alone in cases of Public Safety

While there are arguments against the first point, suggesting that new technologies sustain and recreate labor positions and relations instead of causing mass unemployment, the second point is still in question: Will too much dependency in surveillance systems, lull us into a **false sense of security**, ultimately being counterproductive, or worst yet even dangerous? What would happen in case of **a system breakdown**? Are computers and cameras **error-free**? What is the number of false positives? To which level can we trust that this technological innovation would indeed untie our hands?

Another important concern that is related to the presence of advanced automation technology is the so called Technological Paternalism [18]: the fact that people become both more dominated by it and confident in using even more complex and autonomous technology.

This questions directly peoples' capability for self-determination and, consequently, the vitality of our Society. Two risks arise:

- **Increase of stress that this 'technological eye' could bring on the surveillance professionals;** this is in line with the implicit control those technologies can make on the professionals operating them. Thus, security agents could cope with more stress and a more controlled work, due to recording of the video streams in the database. But this stress could also be related to the over-

expectation of the public, due to the presence of this technological system, for rapid and efficient intervention.

- **Decrease of vigilance of the human operators due to the presence of this technological eye**; this comes as a result of the risk of the increased confidence in the technology. If operators notice themselves that something strange is happening, must they intervene even if the automatic detection systems did not notice anything? This issue raises serious concerns upon the level of confidence and the human-independent operations, resulting in risks of false readings and also very important of lack of participation from the operator.

3.4 Traceability matrix of social implications

The following table contains a summary of the social considerations studied in this document.

Identifier	Social Implications	Compliance to legal framework
SI.1	The human and democratic need for privacy	Article 6 of the Directive 95/46/EC Article 5 of the Regulation EC COM (2012)
SI.2	The privacy policy	Article 6 of the Directive 95/46/EC
SI.3	The invisibility of the surveillance systems; the observer has to be invisible in order to not influence the subjects	N/A
SI.4	The processing of body and face video streams undermines an individual's self determination	Council Framework Decision 2008/977/JHA Article 7 of the Directive 95/46/EC Directive 2002/58/EC
SI.5	The citizens do not feel secure but limited	N/A
SI.6	Human rights (lack of freedom, respect to the other's privacy, freedom of the speech)	Article 6, 9 of the Directive 95/46/EC Article 5 of the Regulation EC COM (2012)
SI.7	Questions about the necessity of these implications	N/A
SI.8	Questions about the impact of this kind of technologies (They can't prevent the crime from occurring nor do they examine the underlying	N/A

	social interactions which have led to the occurrence of the crime)	
SI.9	Creating a society devoid of trust with respect to its citizens	N/A
SI.10	People feeling discomfort knowing that they are monitored	N/A
SI.11	Citizens are losing their trust towards authorities because they feel that they cannot be protected or because authorities can misuse private data	Section VIII of Directive 95/46/EC
SI.12	Concerns of the quality of life	N/A
SI.13	Digital exclusion of citizens not allowing them to have access in smart technologies (smart phones, social media, etc.)	N/A
SI.14	Exclusion of some target groups which want to live a simple and traditional life. It can even lead to compulsion in following the technological privileges (Social Sorting)	N/A
SI.15	Concerns about the minimal human intervention. A machine takes important decisions of e.g. a criminal behavior-Is the machine error free? – Accountability in case of error	Article10 of the Directive 95/46/EC
SI.16	Increase of stress on the surveillance professionals	N/A
SI.17	Decrease of vigilance of the human operators due to the presence of this technological eye	N/A
SI.18	The citizen is considered an object of study and analysis	Article 6, 9 of the Directive 95/46/EC Article 5 of the Regulation EC COM (2012)
SI.19	Not democratic as individuals are restricted to being bodies without subjectivity	Article 6 of the Directive 95/46/EC Article 5 of the Regulation EC COM (2012)
SI.20	Benefit-cost ratio	N/A
SI.21	Creation of a “Big Brother” Society	N/A
SI.22	Insecure data protection	Article 16, 17 of the Directive 95/46/EC
SI.23	Intellectual property rights	Article 9, 10, 11, 12 of the Directive

	95/46/EC

Table 2 Social considerations

3.5 Madrid City Council (MCC) Experience

In the framework of the Deliverable 7.1 which investigates the Social, Ethical and Legal Implications of Public Safety Applications, we summarize the experience of the MCC obtained from the integration of surveillance cameras in Madrid as a live example of already installed surveillance systems.

The Video Surveillance Platform of Madrid City Council centralizes the available video signals and offers the possibility of having an overview of the images on request. From 2005 till now the video system has been growing, reaching approximately the integration of 2.000 cameras.

The centralized video system receives video information from several sources like traffic cameras, main security buildings, Police District offices, and cameras in police vehicles and video surveillance systems in well known places with historical and commercial interest (Plaza Mayor, Montera Street, Ballesta, Lavapiés …)

From the social point of view, MCC has found several challenges, especially regarding video surveillance in the street, taking into account two basic premises:

- **To be under the legal framework:** Any system installed has to be compliant with the legal national framework, which is mandatory.
- **To meet the demands of the society:** The installation of cameras in any area of Madrid is considered only if the neighbors of that area demand to do so.

In fact the areas where the video surveillance has been installed had been carefully analyzed from a social point of view taking into account, among other indicators, the crime rate of the area. The success factor of the project lays in the fact that each installation has the approval of the local area citizens where the video surveillance system is installed.

For instance Montera Street, a very touristic area near the main square of Madrid, has been a hot spot for incidents. Previous to the video surveillance installation, neighbors of that area had even installed home webcams and published those images directly on the Internet, with the idea of preventing crime incidents. After considering every single aspect, Madrid City Council has decided to deploy sufficient cameras in this region.

In relation to video surveillance and criminality rate, the following chart is a proof of how the demand of police intervention has decreased in areas with street video surveillance. These types of systems are installed in specific risky areas of Madrid. Right now there are 118 cameras in the street and probably this number will increase during 2012.

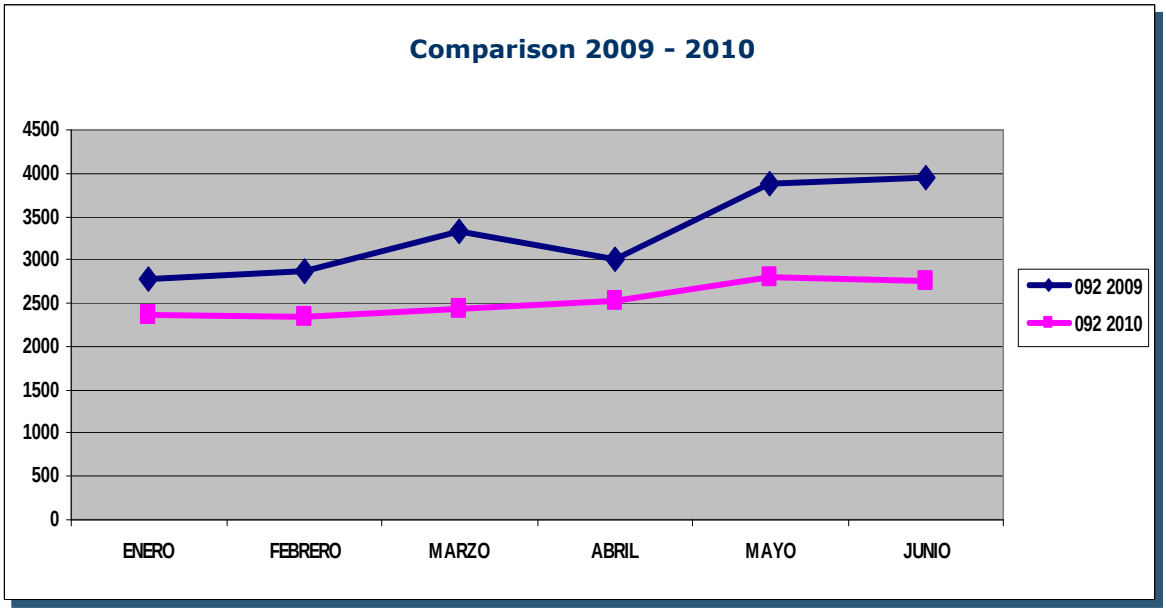

Figure 1 Incidents before (2009) and after (2010) surveillance systems installation

It is interesting to analyze other aspects, as well. For instance, the next figure shows the decrease of the criminality percentage from 2003/2009.For MCC meanwhile the results are not as positive as for Madrid Region while for the Rest of Spain the results was the increase of this ratio. There has been many strategies carried out by Madrid City Council in order to achieve these results, the technological ones like video surveillance have been one of them, and they have contributed to the final results.

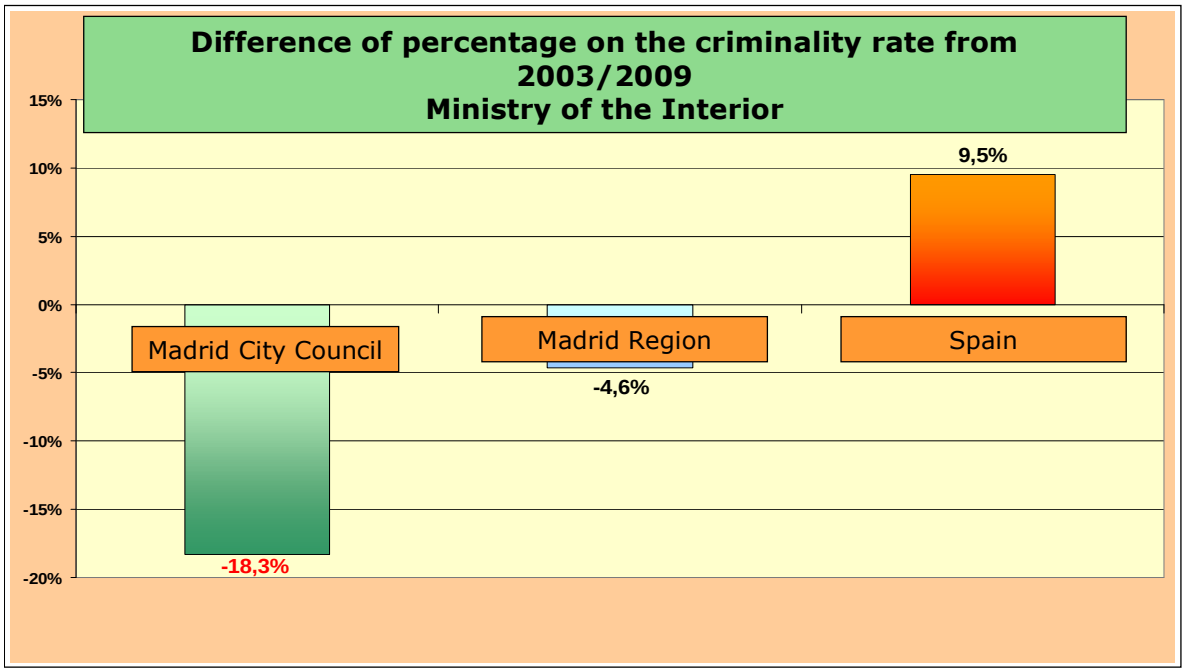

Figure 2 Criminality rate. 2003/2009

A very important result is what is actually perceived by citizens. In this case citizens feel much safer year by year in Madrid. Every year The Security Observatory of the city launches a survey to measure how Madrid citizens feel about security and safety.

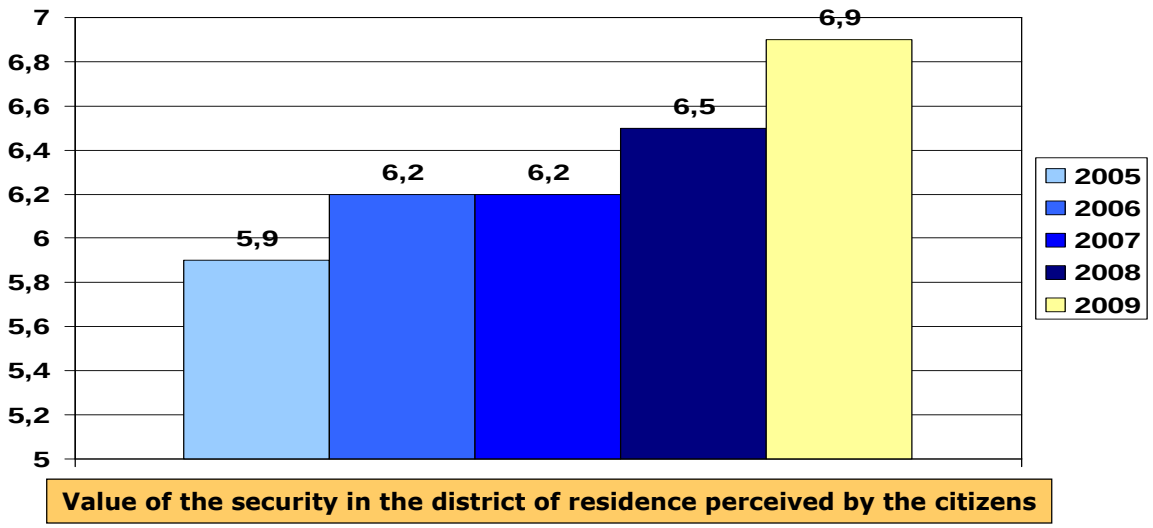

Figure 3 Security in Madrid districts

Regarding the automation technologies in video surveillance, there are no such systems installed in Madrid video platform, but the idea is to integrate these kind of video analysis in next installations, with the purpose of helping and complementing the police tasks (police operators are not able to manage more than 6 video signals at a time) and being a subsidiary tool and in any case the final decision on any incident is the operator responsibility.

Furthermore, these systems will be installed in certain strategic cameras that allow automated detection of suspicious patterns and abnormal behavior, sending the corresponding alarms to the police operators in order to act.

4. Ethical Considerations

4.1 Views and considerations upon an ethical framework in ICT and surveillance technologies

Surveillance at present can take various forms (e.g. CCTV, Biometrics, GPS, monitoring devices) and this creates an even more complex platform for ethics, as moral, societal and political values are being tested and reshaped with the advancement of technology. Incorporating ethics in ICT and surveillance research is vital for protecting fundamental values for both the individual and the society, ensuring that values such as dignity, equality and respect, are not violated or jeopardized at any case.

Generally speaking, in order to address more effectively ethical considerations in relation to surveillance technologies, one ought to review academic papers as well as the literature on the topic of surveillance, in the pre-technological era. This shall help as a first approach towards the ethics of surveillance, raising issues relevant to privacy and necessity or functional purpose of surveillance. In other words, the drivers and motivation for introducing surveillance technologies in a particular setting need to be carefully examined.

Privacy and surveillance technologies are two sides of the same coin and particular attention should be given in this relationship. Technological surveillance comes in many forms nowadays, and boundaries for privacy often become blurred under the cloak of security. There are surveillance technologies that require coming in physical contact with the individual for collection of data, and that of course raises ethical considerations. Fundamental values such as human dignity, autonomy and non-discrimination may be violated for purposes of public safety or the "greater good", and this should be carefully considered by those operating ICT and surveillance technologies. One may become benefited by surveillance, but in exchange of loss of privacy by another; an ethical consideration that needs to be addressed.

In connection to the above, it needs to be taken into account the fact that the ethical framework and the legal framework that governs ICT and surveillance do not always walk hand in hand. In security and healthcare context, it is common for moral values and ethical principles (based on cultural, religious, socioeconomic or other background) to be either neglected or not being successfully incorporated into the legal framework. At times, there is no clear distinction made as regards the surveillance targets and there could be entire ethnic groups under close surveillance. This is an action that raises again ethical issues with regards to privacy and dignity of the individual it could be fear-provoking and further could lead to stigmatization and other negative outcomes.

4.2 Ensuring ethical designs

The EU Directorate General for Research Directorate General establish, in connection with the European Legislation Framework explained in the current document, eight enforceable ethical principles related with personal data:

- Fairly and lawfully processed
- Processed for limited purposes (being strictly pre-defined)
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance

- Secure
- Not transferred to countries without adequate data protection

European citizenship must be transformed from an abstract idea into a concrete reality. It must confer on EU nationals the fundamental rights and freedoms set out in the EU Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms. EU citizens must be able to exercise these rights within as well as outside the EU, while knowing that their privacy is respected, especially in terms of protection of personal data.

4.2.1 Surveillance technologies as a means to ensuring security

Classical perspectives on the development of social control are generally described as the shift from overt, external and punitive to covert, internal and preventive control and may be subsumed as 'from reactive to proactive social control'. However, the diffusion of advanced technologies supported by effective data management systems has provided a more encompassing, more obscure but less intrusive and more powerful means of surveillance. Given these circumstances, the mode of social control tends to move towards pseudo self-control that relies heavily on the deterrence effect of external agencies or devices. Particularly, in a highly transparent society where most activities are 'captured' by an online network of data surveillance, invasion of privacy becomes an integral part of our daily life and the natural attitude that takes the 'surveillance way of life' for granted is expected to prevail.

4.2.2 The collection of personal data as a mean of identifying crime

The EU FP7 Research and Development regulations clearly state the importance of sensitive handling of personal data. In fact great care needs to be taken so as to ensure the secure handling treatment of sensitive information at all times and under all potential cases. Under this scope, we examine the possibility of dual use, leading to improper usage of the data acquired, being different from the original goal of the development. Thereby identification of potential misuses need to be realized and if this is the case, of the safeguard measures required to protect this data flow.

Personal data, also referenced as sensitive data, apply to the set of information which allows the distinct identification of an individual. Such information may be related to an individual's physical appearance, mental, economic and/or social identity, location status and history, etc [3]. Sensitive data also involve data obtained after suspicious personal behavior surveillance and particularly data referred to person tracking in monitored areas following the detection of a suspicious action. The factor that increases the sensitivity and demands exclusive notice is the fact that the project acts in public places and therefore monitoring could be misguided to inappropriate target groups. Thus, Safe City makes use of a wide network of city sensors able to acquire images and videos of citizens in public places and algorithms to determine logic behind movements and location awareness, but in the same time, it aims on ensuring the quality of European citizens' democracy following citizens' right to be treated as innocent until proven guilty and guaranteeing them a safe urban mobility.

4.2.3 Respect for privacy and individuality

Further distinctions are made in the ethical framework and surveillance technologies, in relation to the purposes and ways that surveillance occurs. For instance, there is a difference between surveillance technologies been used for motivational purposes or encouraging positive behavior and surveillance for secretly monitoring people for less obvious reasons, and without their own consent. Also, it is the physical setting where surveillance takes place that raises ethical issues. An example would be surveillance at the workplace, where privacy of the employee may become violated across different levels, in the physical as well as the web environment.

Citizens' awareness issue arises when private data is collected. On the other side, public awareness of the exact surveillance procedure may obstruct the overall activities. With respect to human rights, people should definitely be aware of the monitoring areas. Certain informative signs will be implemented in these regions and citizens will be aware of the threats detected so far. Person or object tracking without citizens' consideration will be allowed only under certain circumstances and under certain permission, following the detection of a validated threat.

4.2.4 Trust and autonomy

Closely linked to the issue of privacy is that of trust. As highlighted by Rachels (Rachels 1975) [32], privacy is often held in an inverse relationship to trust such that the more trust exists between two people, the less need there is for privacy. Nonetheless committed relationships are often marked by a higher degree of trust and a reduced level of privacy. When one of those elements is breached, either through intruding on (limited) privacy or through a breaking of trust, the relationship is damaged. Conversely, the discovery of increased surveillance, especially when the surveilled party is innocent, may also lead to decreased levels of trust. At a personal level trust is often reciprocal: Why should I trust you if you don't trust me? In addition, negative predisposition about the physical environment is created, i.e. where there is surveillance, is associated with criminal activity (preventive measures or reactions to it), and this affects behaviour of people, acting more unnatural than usually since their perceived autonomy is limited. The discovery of surveillance could well therefore damage personal relationships and the citizen's – society relationships.

Surveillance also limits the opportunity to present oneself in the manner of one's own choosing. It is hence limiting on the individual's autonomy, impacting how that individual interacts with the world. If the surveilled is suspicious of or conscious of the surveillance then they might conform to the expected norm, but this will not necessarily reflect their character.

Surveillance therefore diminishes the need to trust the surveilled person. Its presence will pressure that person to conform and so render his/her actions more predictable.

4.2.5 Objective interpretation of data context

Another important ethical consideration in ICT and surveillance technologies is related to the sensitive information that becomes stored in the system. G.T. Marx in his work Ethics for the New Surveillance [27] poses 29 questions which can help determine the ethics of surveillance, broadly categorized as a) means of data collection, b) context and c) use of data. It has to be made explicit who is the operator of the surveillance system and under which legislative framework this system operates. There is a great difference having a system for surveillance being operated by the State or the Media. Further to the data collection through use of surveillance technologies, there's an ethical perspective on the strict and "mathematical" process for collection of data, since human subtlety cannot be codified into technological language, and thus misjudgments might occur by the operating system.

Accordingly, the definition of threats deals with the ethical constrains of marking a behavior, object or situation as suspicious or normal. A plurality of factors should be gathered to crossover the detection of the threat. Therefore a scalable and flexible alarm of threat is also needed. A situation should be considered suspicious in the beginning and some overall data should be acquired. If the case is validated as unusual further, more specific data should be permitted to be obtained. Sensitive data will be received only in case of serious threat definition and anonymisation will be abolished.

4.2.6 Rightful data privacy and protection

The personal and sensitive data acquired by the surveillance systems is subject to the relevant EU data protection standards to enforce data privacy and protection. Data restrictions are initially referred to a

regional level but there are also overall guidelines to be followed. The first restriction that is forced is the collection of sensitive data to be reduced to the minimum level, to be in an encrypted form and to enable scalable and flexible levels of security. The access to this sensitive information is strictly limited to the Command Centers and to some authorized civil protection experts. The confirmation to these few members to gain this data will be validated after specific permission and under certain and highly confidential circumstances. All users of the data, the purpose and the impact of their use will be registered and evaluated continuously and be informed of the consequences of their actions. The ability to detect a non-proper use of them will also be evolved.

4.2.7 Responsible management and storage of sensitive data

Data is considered personal when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot make that link. Examples of such data include address, bank statements, credit card numbers, and so forth. Processing is also broadly defined and involves any manual or automatic operation on personal data, including its collection, recording, organization, storage, modification, retrieval, use, transmission, dissemination or publication, and even blocking, erasure or destruction (Directive 95/46/EC, Article 2b). Recommendations are separated on seven categories, following the EU Directive 94/46/EC categorization:

- **Notice;** Subjects whose data is being gathered should be notified of this action.
- **Purpose;** The collection of data should be preferred only for specific purpose(s).
- **Consent;** Personal information should not be transmitted to third parties without permission from its subject.
- **Security;** Once acquired, personal data should be retained in safe and secure place, protected from potential abuse, theft, or loss.
- **Disclosure;** Citizens whose personal data is being obtained, should be informed of the authorities collecting such data.
- **Access;** Citizens are enabled to demand access to their personal data and allowed to reform any wrong information.
- **Accountability;** Citizens should be able to set the personal data collectors responsible for the application of all seven of these principles above.

EU FP7 Research ethics [3] focus on the importance of secure storage, management and accessing of the related information; data must be stored in a secure environment with control access and other security measures obeyed (e.g. proper temperature control). Additionally, sensitive information needs to be stored in the appropriate hardware means, in the appropriate structure and format, corresponding to the related requirements (e.g. paper, disk, etc). Accessibility to the information needs to be maintained controlled and the networking configurations should not allow data duplication of circulation.

Data transfer in both electronic and other ways will therefore be monitored. Data storage and management considerations also impose thoughts concerning a) the duration of storage of the sensitive information and b) if any back up policies shall be implemented. For example the duration of the storage should define the extent of time needed until destruction of the data occurs, in accordance with the level of importance of the data. This procedure ensures avoidance of the inappropriate use and dissemination of the information.

4.2.8 Social consequences

Adherence to human rights implies taking into consideration the criteria under those a citizen or an object is marked as suspicious. SafeCity characterizes a case as suspect in relevance to the area

monitored, the movements of the person or the object, the extent of the activity e.t.c. These specified criteria are applied on all circumstances, regardless to the race, age, gender, origin or occupation of the person detected. Exceptions will be allowed only under circumstances of extended threat or in cases of diagnosis or expression of dangerous initiatives of distinct groups.

4.2.9 Citizens' rights to access data concerning themselves

Correspondingly to humans rights, any citizen found under a surveillance area will be permitted to access the data acquired related to its behavior. A specific procedure and legislation should be defined to allow citizens become aware of any information containing their sensitive data and the circumstances under which their behavior was monitored. Of course, these rights are in doubt in terms of observation of illegal actions and during the study of a legal case of a citizen's movement. Political protection then retains the right to protect its information. Therefore, analyzing each incident separately, citizens should be enabled to set under investigation their case of surveillance.

4.2.10 Secure data destruction

In order to prevent the crack of sensitive data and the leak of insecure information, the project intends to apply safe methods for destructing its data after the extent of their need. The aim is to guarantee that data is completely destroyed with absolutely no chance of retrieval and deny unauthorized access to any information. The way of destruction depends on the type of the files. Various techniques will be applied in paper, CDs, DVDs, floppy disks, USB drives etc. The responsible deconstruction staff that will deal with encrypted data, will be examined and have signed confidential agreements.

4.2.11 Need to keep up with new technologies for security reasons

The security of precious data demands the ability to avoid data theft regardless of the level of cracking techniques. Therefore, the encryption, file and record locking, integrity, the passwords mechanisms as well as the traceability of the data acquisition systems will have be constantly updated to prevent the possibility of decoding the data management system in any level and disseminating private information.

4.3 Traceability matrix of ethical considerations

In the following table we have summarized the ethical considerations studied in this document

Identifier	Ethical Considerations	Compliance to legal framework
EC.1	Fairly and lawfully processed personal data	Article 6 of the Directive 95/46/EC Article 5 of the Regulation EC COM (2012)
EC.2	Processed, for limited purposes, personal data	Article 7, 8 of the Directive 95/46/EC
EC.3	Adequate, relevant and not excessive personal data	Article 6 of the Directive 95/46/EC

EC.4	Accurate personal data	Article 6 of the Directive 95/46/EC
EC.5	Data should not be kept longer than necessary	Article 6 of the Directive 95/46/EC
EC.6	Data have to be processed in accordance	Article 7 of the Directive 95/46/EC
EC.7	Data must be securely exchanged via encryption mechanisms	Article 16, 17 of the Directive 95/46/EC
EC.8	Data must not be transferred to countries without adequate data protection	Article 25 of the Directive 95/46/EC
EC.9	Data must be securely destroyed after their usage with absolutely no chance of retrieval	Article 12 of the Directive 95/46/EC
EC.10	Citizens must be aware of being under surveillance and have access to their personal data	Articles 6, 12 of the Directive 95/46/EC
EC.11	Define the criteria under those a citizen is marked as suspicious	N/A
EC.12	Secure storage and management of the personal data	Article 16, 17 of the Directive 95/46/EC
EC.13	Objective interpretation of data content	N/A
EC.14	Respect the citizen's privacy and individuality – try to keep the anonymity	Article 6 of the Directive 95/46/EC Article 5 of the Regulation EC COM (2012)
EC.15	The cameras should be located in such way so as to not record through a resident's window	N/A
EC.16	The citizens must be aware of the fact that they are monitored , of their legal rights and of the impact on their lives	Article 6 of the Directive 95/46/EC Article 5 of the Regulation EC COM (2012)
EC.17	Information input into the databases is prone to human and device error	N/A
EC.18	Respect to the citizen's autonomy and trust	N/A
EC.19	Use of personal data according to human rights and democratic	Article 6 of the

	practice	Directive 95/46/EC Article 5 of the Regulation EC COM (2012)
EC.20	Ensure the end-users that their personal data will not being used against them (Confidentiality)	Article 16 of the Directive 95/46/EC
EC.21	Consider the ethical cost of the applied technologies, the advantages and disadvantages (benefit-cost ratio)	N/A
EC.22	Ensure that dignity is not violated or jeopardized at any case	N/A
EC.23	People must feel free. Danger of people feeling less free because legal public behavior like attending a political rally, entering a doctor's office, or even joking with a friend at the park will leave a permanent record, retrievable by authorities at any time.	N/A

Table 3 Ethical Considerations

4.4 Madrid City Council Experience

Regarding the management and storage of sensitive data, the Madrid's City Council experience and basic procedures are presented in the following lines. The centralized video system of Madrid City Council integrates images from cameras and video recorders, from different sources. In the case of street surveillance, prior to installation of any camera in the street it is required an authorization from the Commission of Surveillance Guarantee of the regional government. This Commission is formed by the President of the Superior Justice Tribunal of the Region, the Director of Public Prosecutions of the Region, two members of the State Public Administration, among other high qualified members. For usage of street surveillance cameras, MCC is authorized to record images for 7 days, and then it is mandatory to erase the older images.

The Center is operated by policemen, who are the only authorized personnel to view on-line real images on the police operator consoles or on a video wall. The extraction of images on a digital source can be made only from a dedicated terminal and has to be authorized by the police officers or injunctions made by the judge court by the official form petition, and it has to be registered on the digital official file for video images extraction. The extraction of the images has to be done by the police unit chief, responsible of the Center. The whole process is technologically secured. On the other hand the citizen's rights are guaranteed since the strict application of the Organic Low on the Protection of Personal Data is required.

5. SafeCity implications and balancing acts

5.1 Definitions and considerations on personal data and processing

In what follows, we present an overview of the basic definitions and considerations related to personal data and the processing techniques that may be performed on them. Scenarios where these definitions are applicable raise ethical and legal implications and they need to comply with respective regulations (as these were studied and referenced in Section 2).

Personal data: ”any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”

Notion of identification or identifiability: when a person may be recognized among a small group of individuals. No data protection issues arise whenever captured images are blurred immediately and original, clear, images are immediately deleted. Except when the data is anonymous or automatically anonymised from the start (it will not be the case if the images are blurred only after their transmission to the central security office) then, any collection, storage and use of coded or personal data relating to human subjects must comply with the 95/46/EC Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The finality of the data processing is not a relevant criterion for the applicability of the data protection regime. In fact, in the public safety scenario, although the aim of the image capture is not to identify, control or monitor individuals, the captured images are nonetheless personal data if, on the basis of these images, individuals are or can be identified. The necessary condition for excluding the application of the data protection directive is that the data is anonymous (that is, that it cannot be traced back to an identified or identifiable person, **reliable anonymisation of the processed data** must be ensured).

Some types of personal data, **sensitive data**, may never be processed or may only be processed under severe and strict conditions. Article 8 of the Directive 95/46/EC makes it in principle illegal to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.

It is important to **correctly identify the data that is subject of processing**, independently from their role in the scenario: it can be the “user” of the infrastructure (car driver in the M30 tunnel), or the police man assisting the traffic jam situation.

Any “operation” (collection, storage, use,…) involving personal data is considered a **“processing”** under the EC Directives and relevant national laws. Any collection, or storage (including in images repositories) of texts, images, sounds, etc. is considered “processing”. It must be underlined that the simple fact to collect, through CCTV, clear images of persons, even though these images are blurred immediately after they have been recorded, is sufficient to consider these captured images personal data (at the capture stage). The anonymisation is in that context a second operation applicable to the personal data collected.

The **data controller** must be identified taking into account all types of delegations of service provision that may happen. So, in the public safety scenario for example, the data controller may be the Command and Control center operator, the provider of technical services, or third parties having been made responsible for the data processing, or all of these actors simultaneously. (Art. 6) Due account must be taken of the fact that the scenario involves a network of actors, and of applications, and therefore complexities regarding the ascription of responsibilities among actors. It is the duty of the data controller to assess the quality of the data processor and his ability to provide adequate security

measure. Furthermore the data controller has to define precisely, in a written contract, the missions of the data processor, and to check if the data processor does respect entirely the limits of his contractual duties.

Whereas safety and security (detection and intervention) scenarios will most probably rely, to establish their legitimacy, on either « the vital interest of the data subject », or the « public interest or exercise of official authority vested in the controller », marketing and convenience (profiling) scenarios will more probably rely on « consent » or the « legitimate interests of the controller ».

Prior Determination of the purposes: The data controller has the duty to define precisely the purposes of his processing and to make them explicit.

Compatibility: In evolving systems, like most of the automated processing techniques taking place in Public Safety scenarios, it is very easy to apart from an original application, existing at the moment of the data collection, and to imagine a new one that will allow new purposes. The question is then the following: Is that a new usage or might this usage be considered as compatible with the former one? The criterion to distinguish the compatible use versus the incompatible use has been defined by the criterion of the reasonable expectation. In other words, would the data subject have had the possibility at the initial moment of the data collection to imagine this future usage as included in the purpose of the processing? If yes, the processing is deemed compatible and is legitimate without new formalities. If not the processing is a new one and has to find a basis for its legitimacy and the data subject must be at least informed or even agree to this processing.

Data minimization is another legal requirement implying that only the personal data that is necessary for the implementation of the system should be collected, processed and/or stored, and that the data must be deleted when no longer necessary and after the legal conservation requirements. The data controller is, moreover, responsible for ensuring that the processing complies with the data quality requirements.

5.2 SafeCity Public Safety Use Case

The legal, social and ethical analysis presented in the previous sections, aimed in shaping the frameworks upon which the SafeCity project needs to operate. Based on the considerations regarding personal privacy and value of private data, we define below a set of implications to be considered.

In particular, following we present a more high-level analysis of the implications founds across the overall SafeCity concept, being an innovative Public Safety Use Case; following the parallel technical research, the work presented below highlights requirements to be considered and dealt with from the developers as well as practitioners of the SafeCity framework. For example, legislations regarding the secure storage and transfer of data must be guaranteed under definition of the necessary security protocols, while in turn authorized access needs to be designed upon the according policies followed by a Public Safety Organization with respect to its national laws.

As opposed to this study, Section 5.3 presents a more detailed and pragmatic analysis of the technical developments to be realized in the proof of concepts trials in Madrid, Spain and Stockholm, Sweden. Section 5.3 explores the sensitive cases which need to be clarified and validated by the technical developers during the design of their applications and during realization of these trials.

The implications presented are assigned (whenever possible) relevant balancing acts, aiming to cope with them effectively. Proposed measures are defined in relation to the nature and the type of the implications raised, i.e. whether we refer to (a) technical implementations (e.g. security policies) and/or (b) concrete policy making (i.e. management acts). In Section 5.3, balancing acts present a more detailed overview of the sensitive points needed to be covered by the PoCs, while further analysis on policies to be adopted is presented in [1].

5.2.1 Acquisition of sensitive data, including incidental findings

SafeCity makes use of sensitive personal data with to identify and/or exclude an individual. This information is related to the behavioral patterns of the citizens in an area, their facial characteristics, their interactions with other individuals, their being part of a wider group, associated objects, identified history and awareness of their location over time. As described above, the acquisition and handling of sensitive data needs to be realized with extra care, acknowledging the underlying regulations and justifying their necessity.

Additionally, under the scope of the SafeCity framework as wider Public Safety Use Case, it is possible that incidental findings may be acquired during sensing operations. A critical example is the acquisition of data from private places (e.g. image of a house located near a central square; CCTV cameras installed in the square would be able to acquire images from the house's interior should that be within their range). Acquisition of incidental findings is very likely as it is not possible to forecast a priori every possible scenario falling under exceptions. However, we should look into defining concrete policies for managing these situations. "Data is a living material" [3] and the processes of handling any kind of information acquired needs to be clearly stated and justified. Incidental findings fall under serious legal questioning, given that the relevant application and accordingly controllers make use of data not authorized to do so. For example, when describing the acquisition of individual data beyond the original scope of the application's operations, it is immediately implied that any informed consent acquired is not valid. Additionally, questions regarding policies of how this data is going to be stored, distributed and in overall manipulated come forward. Based on the above considerations, we define the following key points:

- **Management and Control Policy;** The SafeCity Framework definition will have to validate and explain:
    - what kind of personal data are to be acquired
    - why the specific types of data need to be acquired
    - the places from where such data are to be acquired
- **Technical implementation;** The SafeCity Framework design would have to ensure that data not obeying the following criteria should not be furthered processed/stored/transmitted, etc:
    - data being acquired should fall only under certain pre-specified categories, as suggested above
    - data being acquired should not be forwarded towards resolution of different purposes than the reasons initially specified as suggested above
    - data being acquired should be identified upon their sensor inputs and real-place locations, and these should not differ from pre-specified definitions as suggested above
    - the sensors (cameras) used will have masking capabilities and they will be correctly programmed to avoid any incidental data collection, which could undermine personal privacy

5.2.2 Data Storage, Access and Distribution, Management and Control

SafeCity examines the temporary storage of sensitive data in order to allow their processing to take place. Such storage takes place in multiple levels:

- The first includes a cloud edge located in the area of the sensors network where local pre-processing is being realized. Even though data is stored for a very short time, obeying the latency requirements of Command and Control Centers, this interval may be crucial for their interception

- The second includes a heavy data storage facility where data are again temporarily stored towards being processed and also during a given allowed time interval (e.g. typical seven days)
- The final level includes a reference database holding known criminal records upon which detection of patterns, plate recognition, etc are being based.

In addition, SafeCity tries to address end user's requirements upon the enabling of a unified response system and a networking policy for sharing data among Public Safety organizations. The data being acquired and stored under the context of SafeCity, as well as future developments expected to take place upon Public Safety, need to be protected by clear policies regarding the bodies being responsible for their storage and distribution. Sensitive data need to be stored in secure places, specially selected to serve their purpose, posing access control and clear back-up policies. This is a vital concern to take under consideration both during the handling of test data in the project's trial cases, as well as when designing complete communication networks between mobile/fixed sensors in the city region and control and command area operations. The following key points should be considered:

- **Management and Control Policy;** The SafeCity Framework definition will have to validate and enforce the definition of:
    - the parties, authorities and personnel who should have access (and according level) to the different categories of the data being acquired
    - the design of clear policies for handling data amongst different organizations and different countries, including member states and non-member states
    - the parties accountable for the data management across all stages, liable to report the data's movements at any time
- **Technical implementation;** The SafeCity Framework design would have to ensure that:
    - the appropriate level of security is enforced across all communication channels, upon the according protocols, data monitoring and auditable data exchange
    - data access should be restricted to authorized personnel, via the introduction of authentication processes and dynamic password level accesses
    - sensitive data need to be stored in a secure located, interconnected only with private local network of high security

It is also mandatory that citizens have the right to access their personal data and obtain them when they feel that their human rights are violated.

In Madrid the video surveillance systems have been installed in 2008 and a whole operative procedure has been implemented. This procedure has constrained the systems to comply with the national and European regulation framework.

5.2.3 Data retention and secure expel

Based on the considerations defined previously, personal data cannot be retained further than a given timeframe. This usually differs nationwide and after than period, the data acquired need to be completely erased from the system. The following key points should be considered:

- **Management and Control Policy;** The SafeCity Framework definition will have to validate and explore:
    - the maximum allowed timeframe suggested nation-wide, upon the retention of data
    - frequent and automatic check upon the data stored, to define whether they are still of use or not (e.g. in Madrid City Council data is erased after a week period)

- **Technical implementation;** The SafeCity Framework design would have to ensure that:
    - records and data logs of the data acquired are being maintained and that these are being automatically destroyed after the allowed timeframe define above
    - data erase processes should be effective to ensure that there should exist no possible way for anyone to retrieve the data from the storage facility

5.2.4 Citizens awareness and informed consent

Under the scope of the wider SafeCity Framework as a complete system framework for Public Safety, we should mention the necessity of respecting the citizen's rights to lawfully being informed of when, where, upon what and from whom the citizen is being monitored. We define the following key points:

- **Management and Control Policy;** The SafeCity Framework definition will have to validate and ensure:
    - Citizens become aware of the surveillance technology applied in the respective places. Such information should also include brief remarks of the accountable authority and the means (e.g. microphones, CCTV cameras, etc) being deployed. Further to that, citizens should have access to contact information and/or direct information for acquiring justification of the reasons he/she is being monitored in the respective places
    - Informed consent should be acquired from the respective authorities of the area where the framework is expected to be applied, as well as in the cases where any new sensor would be deployed in new locations

In Madrid there are specific areas already under video surveillance by Madrid Police Department. For these areas it has been mandatory to process the legal authorization for each of the senor sites. Since the Proof of Concept is going to be held in a limited scenario and will use a fixed number of sensors (5 cameras) located in the same points as they are already installed for the city surveillance and therefore authorized by the competent authorities, no further permission will be needed.

5.2.5 Keeping up with new technologies

Despite the level of security applied, data loss and theft may take place. It becomes therefore necessary to ensure that the SafeCity Framework will obey policies of continuous update and validation. The following key points should be considered:

- **Management and Control Policy;** The SafeCity Framework definition will have to validate and ensure:
    - that the system is validated and checked frequently by authorized controllers
    - that system validation needs to be reported and monitored
- **Technical implementation;** The SafeCity Framework design would have to ensure that:
    - records and data logs of the system check is maintained
    - the system's respective protocols, applications etc versioning are clearly marked
    - potential threats and attacks on the system's security systems are reported. Such reports should be realized under constant checks upon the integrity of the system's components, information exchange and potential data loss

5.2.6 Social Responsibility

As mentioned above, many technical innovations do not correspond to the societal structure and can in that way cause disequilibrium, divisions and discriminations. We define the following key points:

- **Management and Control Policy;** The SafeCity Framework definition will have to validate and ensure:
    - social feedback upon the citizens' acceptance of the surveillance implementation is enabled frequently and that the best fit policies are accordingly being applied in each case
- **Technical implementation;** The SafeCity Framework design would have to ensure that:
    - traditional methods of mass approach and dissemination should be enabled for the publishing of alerts(e.g. publish to television/radio media, road-signs, etc)
    - definition of criminal activity should be based upon subjective criteria of suspicious behavior and should not in any case have relation and/or reference to religion, nationality, etc criteria

5.2.7 Additional considerations

The above presented some key considerations upon the main functionalities and design components of the SafeCity Framework, which need to be considered as sensitive and thus appropriate development actions should be defined. This will be realized with the form of enablers, either specific or generic, whenever applicable. Additional concerns include management policies to be defined towards protecting and validating the SafeCity Framework, the respective authorities it is being addressed to and the European citizens.

5.3 SafeCity Proof of Concepts

It has to be noted that the peaceful enjoyment of privacy requires that everyone be able, at certain times and in certain activities, to shield themselves from observation by unauthorized third parties. This requirement entails the "invisibility" of many aspects and acts of daily life against unauthorized parties, even using automated means and without the data subject being identifiable, as well as the inviolability of the home (conceived not only as a physical space but also from a virtual standpoint).

It is important to stress that Human Rights principles (or the specific conditions of their exceptions) must be followed unconditionally**. This is in contrast to data protection requirements, which only apply in the hypothesis specified in the relevant EU Directives, studying cases involving the processing of personal data.**

It should thus be noted right away that **even if some SafeCity application falls outside the scope of the data protection regime** (because the processed data are unambiguously anonymous, for example) **it may nevertheless be questionable from the broader point-of-view of other fundamental rights**, such as privacy (the right to data protection does not exhaust what privacy is about), freedom of movement, freedom of expression, non-discrimination etc. Identification issues (data protection) do not exhaust all potential issues arising from what one may broadly call surveillance and monitoring.

For instance, in the video surveillance use cases, besides potential data protection issues, and even when all data protection law requirements have been complied with, the mere presence of CCTV systems embedded in the infrastructure de facto decreases the level of privacy enjoyed when using these infrastructures; whenever the system's functioning results in **individuals feeling compelled to avoid using the infrastructure** at all, as to avoid being "recorded" by a CCTV system, their freedom of movement and right not to be discriminated against may also be an issue: **the blurring of faces on the images is therefore recommended**.

As mentioned above, the SafeCity project is aimed to realize two trial applications (Proofs of Concept). Based on this consideration we have explored the national regulations upon surveillance technology and data protection rights in the two cities to apply the PoCs: Madrid, Spain and Stockholm, Sweden.

Based on the above considerations, discussing the implications found across the development of the SafeCity Use Case, we analyze here in greater detail, implications concerned with the actual implementations to take place during the SafeCity trials, i.e. as opposed to its wider conceptual framework.

The PoCs are expected to provide limited and selected functionalities and to monitor volunteers with approved consent. Yet, a set of implications are raised a priori in order for the technical teams to take in account the sensitive nature of the data being handled and the applications to be designed. In this section, we briefly discuss these implications which in fact follow the same pattern as the considerations summarized above, although regarding the most specific and actual application of the SafeCity development.

The SafeCity trials are going to be realized with the aid of the SafeCity consortium and in particular they shall be supported by partners volunteering to participate. Real facial characteristics of the volunteers will be used as basis for identifying criminals, while these shall also be assigned fictional profiles (i.e. they should not correspond to real persons).

5.3.1 Acquisition of sensitive data, including incidental findings

Despite the acknowledgement of the volunteers to provide their personal data for the shake of this research, it is necessary to provide brief policies with respect to incidental findings, i.e. findings upon the persons being monitored, which are **unrelated to the pre-defined causes and intentions of the PoC scenarios**. Similarly, clear policies for data retention need to be introduced for the cases where **citizens and pedestrians' personal information** may be recorded.

5.3.2 Data storage, access and distribution, management and control

Clear policies and security mechanisms (encryption, authentication, etc) need to be defined in order to guarantee secure data storage. Additionally, clear policies need to be defined with regard to the management of the data acquired (e.g. **who will have access to the data, who will be responsible for any data loss, who will decide the routing of the data**, etc). Even though the personal records to be acquired will be fictional, facial characteristics will still be true personal information so it is necessary to **ensure that the SafeCity design will obey all respective legal and ethical aspects raised**.

5.3.3 Data retention and secure expel

Even though the data to be acquired are going to be fictional, facial characteristics will be acquired upon true persons and thus this information is considered highly sensitive. Security mechanisms need to be ensured so as to **a) provide secure and permanent expel of the data** and **b) break any potential linkages between the facial images used and the according fictional profiles introduced**.

5.3.4 Citizens' awareness and informed consent

Considering the SafeCity trials, we regard the following relevant groups to be fully aware of the surveillance applications to take place:

- The SafeCity **partners volunteering to take place**, as well as any other volunteer (personal consent)
- The **respective authorities** of the city where the trials are going to take place, providing formal consent on behalf of their citizens
- The **citizens and/or visitors of the area being monitored**; these should be informed at the time of the trial taking place with a clear notification within the area, that they may become monitored and where they should address further questions upon this issues.

In the first two cases, a formal, written, dully filled in and signed informed consent needs to be provided before the execution of the trials, so as to ensure that the PoCs will be in compliance with the respective legislations. Such informed consents should be examined and approved by external ethical experts and they should include information regarding:

- **What type of data are going to be acquired** (e.g. images, video, voice, etc)
- **What processing stages are the data going to be subject to?** (e.g. transfer from central square to central police station, storage in the main data repository system, video processing, etc).
- **What risks are the data being subject to** across each processing phase and what according mechanisms can guarantee their security and integrity.
- **How are these data going to be used against the monitored subjects** (definition of illegal and abnormal behaviors, patterns, etc).
- **What will happen to the data after the trial end.**
- **Who is responsible for the security of the data acquired.**
- **Who is responsible for the secure expel of the data acquired.**
- **Who is responsible for the deduction of results upon the data acquired.**

5.3.5 Keeping up with new technologies

The SafeCity project studies innovative applications and designs but it is necessary to ensure that the security mechanisms applied will be reliable and will not in any case be subject to data loss. This should also refer to the secure expel of the data after the trial end. The consideration presented in this section ultimately stretches the necessity to guarantee that **any potential threat has been taken into consideration and dealt with or at least that secure encryption mechanisms will prevents hackers from accessing the data acquired**.

5.3.6 Social responsibility

Overall, the design of SafeCity should follow an ethical and social responsibility plan and try to deliver applications taking under consideration the wider common good. Based on the consideration of the city trials, a review of the cities to be used should be provided with respect to the **social consequences of testing and applying the respective surveillance technology in a public space in each of the two scenarios**. In any case, the SafeCity PoCs should **respect the social impact and profile of the cities to host the trials**.

6. Privacy, data protection and ethical issues in Safecity use cases. Accessing Stakeholders perspective and concerns on ethical issues

This chapter focuses on citizen perceptions, concerns and knowledge. Our analysis is carried with a view on three stakeholders:

(1) Citizens: The analysis of citizen perceptions is split into two parts. The first considers citizens' concerns and apprehensions about new data collection technologies. The second considers citizens' knowledge and concerns regarding data storage and use. The first section firstly considers the factors that shape public opinion on technologies and more specific in surveillance means. Then it considers the comprehension deficit in the conception of technologies giving a base from which to finally analyze fears.

(2) Data Controllers: In this analysis we take a data controllers' perspective on the data subjects' right to be informed (article 10 and article 11 of Directive 95/46/EC), and the right of access to data (as enshrined in article 12 of the data protection Directive).

(3) Data Protection Authorities (DPAs): What role do DPAs play in reconciling the rights and interests of data subjects and data controllers?

For this reason we created questionnaires which were been sent by emails in perspective stakeholders (DPAs and Data Controllers), and also we performed telephone and personal interviews with Data Controllers and Citizens.

Major Concerns, fear and also accusations from Citizens, regarding data protection, as resulted from the interviews have to do with surveillance cameras, health data records and cyber attacks (personal data piracy).

The Best Interaction took place with the Hellenic Data Protection Authority. They provided us a lot of information, through telephone and also through many reports and statistics they provided to us. Rest European DPAs were approached through e-mails and questionnaire. Also information through the respective websites was collected.

We tried to determine whether European citizens have sufficient knowledge of what information is stored, for which purpose and for what period of time. We did that in two parts. The first considers citizens' concerns and apprehensions about new data collection technologies. The second considers citizens' knowledge and concerns regarding data storage and use.

6.1 Citizens concerns and apprehensions about Safecity technologies and applications

In this section we tried to determine whether European citizens have sufficient knowledge of what information is stored, for which purpose and for what period of time. We did that in two parts. The first considers citizens' concerns and apprehensions about new data collection technologies. The second considers citizens' knowledge and concerns regarding data storage and use.

For a variety of reasons, there is no single 'public opinion' on new technologies. Due to their varying contexts, capabilities, visibility, effect and comprehension, opinion can vary greatly. However it is possible to isolate certain more general factors which appear key, to the shaping of opinion. These come together (balanced differently dependant on context) to chart a background to each perception.

The outcome of the survey we performed was that the public opinion lacks technological understanding. Also due to this lack of understanding a lot of "fears" are created to the people regarding surveillance methods and systems.

When considered alone or as part of wider assemblages, it is evident that the technical capabilities of data collection technologies are not often understood, whilst in their presentation, the terminology is mixed and uncertain and the boundaries of discourse around and between technologies are fluid. As a consequence, the public has difficulty in forming images of the technologies themselves or of locating the significance of the data they collect, the data environment they operate in or their relevance in wider and equally complex social debates. It is thus very difficult for the public to evaluate technologies themselves or the wider systems of which they are part, based on relevant factual starting points.

As a result of this lack of clarity, other opinion shaping factors become significant in whether technology is accepted and the role it plays in wider debates (such as how technologies are presented in the media or the immediate reaction they elicit). Whilst the technologies and the systems in which they operate are active features in the significance of data collection and processing, it is, in fact, their references in relation to other debates or perceptions that play the active role in public opinion formation.

Accordingly, considering the lack of comprehension of the technologies themselves and therefore a difficulty in tracing paths of causation between their deployment and use, and their justification, consequence and legitimacy related to their declared aims as well as related to the social systems with which they interact, public fears took on two forms. First, uncertainty led to a general feeling of uneasiness related to the increased deployment of data collection technologies and what the trend toward increasing collection of personal data could be fostering, both on a societal level, and in terms of what this would mean for the individual in society. The individual manifestation of this uncertainty was perhaps personified best by the indefinable but uncomfortable expression of feeling under suspicion. Second, specific manifestations of abstract fears, guided and filtered through the above mentioned opinion formation factors, thus tended to be transferred onto each technology, with fears of ID fraud, function creep, secondary use and misuse being particularly prevalent.

From the above, one can identify certain public desires in relation to data collection technologies. First, the public wish the lack of knowledge and certainty about data collection technologies – what they are and how they are to be used – to be addressed.

Second, the public has the perception that there is little debate on the theme and on why, which and how to deploy each technology, and that policy makers should address this too. As it is perceived that the effects of technological deployment could be socially significant there should be wider debate on technological deployment and use. These debates should also include consideration of non technological solutions and should include a wider range of stakeholders in the decision making process.

Before the deployment of each technology, to reduce the potential for function creep and privacy impact, the public believe that the privacy impact should be carefully analysed and considered against potential gains [34].

Finally, there should be further transparency and controls on the operation and use of each technology. This can be seen as a reflection of the perceived need for control over the social impact of the technology, the consequences of its wider deployment and the potential for function creep and misuse.

6.1.1 Citizens Knowledge and concerns regarding data storage and use

Generally, the public does not seem certain which actors should be responsible for the safe handling of personal data. Indeed, opinion changes depending on the nature of entity or activity considered. When considering social networking sites, for example, 49% of respondents stated the individual should be primarily responsible with 33% suggesting the social network should be responsible, whilst in relation to online shopping sites, the percentages were 41% and 39% respectively. The difference is interesting not only as it demonstrates uncertainty in responsibility allocation but also as it suggests a difference in perception based on the nature of the specific data processing entity. Taking this logic one step further suggests the public may be basing its opinions more on the entity than on the processing of data. Equally interesting is the relatively low response listing public authorities as having primary responsibility (16% and 19% respectively). This allocation is, to some extent, in contrast with the relatively harsh penalties (if there is such uncertainty as to who should hold responsibility, it seems strange there should be a preference for harsh regulation) the public seems to wish on organizations that breach standards. Indeed, in the same Eurobarometer survey, 51% of respondents suggested organizations which misused data should be fined, with 40% believing such organizations should be banned from using such data in the future [35].

The public feels that personal data does not receive the protection it should, demonstrated most obviously by the fact that a large majority feel they have lost control over their data (as well as by other opinions on protection). For example, in Flash Eurobarometer 225, a majority of respondents believed that national legislation could not cope with the demands currently placed on it [36].

Theoretically, the public place a high value on data protection and by proxy appear to perceive the potential significance of data processing and the data environment on themselves and the societies in which they live. However, despite this awareness and even awareness of key aspects of the right, the public display a relatively superficial understanding (or at least a poorly enunciated understanding) of the broader social and legal significance of data protection.

This lack of enunciation and clarity as to the "why" of the significance of data protection parallels practical uncertainty related to the data processing environment. Whilst the public perceive certain actors as playing a key role in this environment and understand the general purposes for which these actors are using data collected, this remains an equally superficial comprehension – notably in the lack of clarification as to which connections exist between processing entities or sectors, how these connections might be of significance or how the collection of data alters the fulfillment and nature of the goals its collection seeks to achieve.

6.2 Data Protection Authorities

According to Art. 28 of the EU Data Protection Directive [37], each Member State shall "provide that one or more public authorities124 are responsible for monitoring the application within this territory of the provisions" of the Directive. These authorities shall "act with complete independence" (Art. 28(1)) in exercising their functions and powers.

The European DPAs showed a significant availability to participate and collaborate in this study. Sixteen authorities replied to the questionnaire, in written form or telephone interview. In the following lines the results of the analysis of the review are presented.

6.2.1 DPAs independence and competencies

With particular respect to the competencies of the national DPAs, in general, these include the following: to advise the legislator in the process of drafting legislation or regulations relating to the protection of the individual's rights and freedoms with regard to the processing of personal data; to create and maintain a public register of all processing operations notified by data controllers, in order to facilitate access to information for the data subject; to deliver prior_checking opinions before processing operations are carried out; to order the blocking, erasure or destruction of data, to impose a temporary or definitive ban on processing, or to warn or admonish the controller; to institute civil legal proceedings in cases where the provisions of the national data protection act have been or are about to be violated; to encourage the drawing up of suitable codes of conduct by the various sectors and to provide a data protection audit; to raise public awareness on matters of data protection and privacy; to collaborate with supervisory authorities of other countries or at the EU and international level to the extent necessary for the performance of their duties.

European DPAs are often confronted with the problem of limited resources to carry out their tasks. The lack of financial and human resources is often indicated as a major reason preventing the DPA to accomplish its duties.

6.2.2 Handling Citizens Complaints

In all European Union Member States, citizens have the right to request an investigation on the grounds of infringements of the data protection law. National supervisory authorities are entitled to launch a data protection procedure that may involve the correction of inauthentic personal data, the blocking, erasure, deletion or destruction of illegally controlled personal data, a prohibition of the transfer of personal data to third countries, or the obligation to respect the data subject access right.

The study showed that the DPAs are noticing an evolution in the number and type of complaints received. For many years, the number of complaints was quite stable and relatively low, but in the last decade there has been an increase. With regard to the types of complaints, there is an increasing trend in complaints related to data processing in online services**. Other sectors mainly include video surveillance in public spaces, surveillance at work, as well as data processing in the public health and financial sectors**.

Citizens usually address the DPA to pose questions on their rights in a specific case, to request assistance to access, rectify or delete information, and to report violation of data protection rules. In information requests, citizens ask about their rights or ask for advice and guidance in a particular case. There are also complaints about the lack of the right to information or inadequate way of obtaining consent.

With reference to the categories of citizens addressing the DPA, and to the question whether there are more vulnerable groups of people who are not able to address the authority, it has been difficult for the respondents to provide an accurate answer, since the DPAs do not collect information on sex, age and other personal details from the complainants. No statistics are therefore available on this issue. It might, however, be empirically stated that the complainants are mostly middle age people (30-55) and, in many cases, the number of young people is

increasing. Information on the categories of citizens addressing the DPA is, in the respondents' view, not related to any vulnerability or exclusion, but has more to do with awareness. In some cases, there has been a noticeable increase in interest in young people in data protection, compared to the previous decade.

Citizens increasingly access the DPA mainly through the DPA's website or email. The DPAs can receive complaints or information requests by post, fax or specific forms on their websites. In many cases, the DPAs also have a front office for receiving citizens or data controllers personally and a dedicated phone line to provide information.

With reference to the ability of the DPA to react on time to citizens' claims, the time to handle a claim may vary a lot depending on the nature of the complaint. In easy situations, a letter to the data controller might resolve the problem in a week. When the complaint needs to be verified in order to collect evidence, this may require an inspection. Some delays may also occur also when the DPA has to wait for information on data processing from a public institution, a private company or the DPA of another country.

6.3 Major Concerns raised for Safecity viability

In the following lines we will present the major concerns that had been raised, as of result of the research we made with Data Controllers, DPAs and of course citizens. These concerns affect directly the viability of Safecity applications. The following concerns were addressed mainly by the citizens and data controller's experts and are:

1. People **are negative to surveillance methods** and new technologies that are using personal data because they lose control over the way their information is collected and processed.
2. People **are doubt on the credibility that Organisations handle the infor**mation they collect about them in a fair and proper way.
3. Do the existing laws and organisational practices provide sufficient protection of our personal information?
4. Do the security companies that cooperate with public bodies or individually collect and keep our personal details in a secure way?

7. Conclusions

Following Decision No 1982/2006/EC of the European Parliament and of the Council of 18 December 2006 concerning the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007-2013) in order to manage and assess the impact of possible consequences between security and society, the current document presented an overview of implications raised concerning the application of Public Safety capabilities, under the implementation of the SafeCity Framework. The intent and scope of this research was to identify sensitive points to be considered upon the technical and functional design, as well as additional concerns to be studied across the SafeCity Policy Making activity [1].

7.1 Legal Considerations

The document included the main legislations and directives published by the European Commission, as well as the new EU proposed legal framework, and aimed in defining rules upon the handling and protection of sensitive data with respect to surveillance and ICT designs, staying respectful and true to the citizens' rights upon freedom and privacy. The current research highlighted existing legislations upon the protection of personal privacy, data, honor and self-image rights. A brief overview of the main frameworks applied across EU member states has been analyzed, so as to present the level of importance of handling sensitive data, and to accordingly define implications in the SafeCity Concept and technical development. In that sense, the current research has tried to stay in compliance with the European legal and ethical framework, thus ensuring that the SafeCity project follows correctly data protection and personal rights' principles.

During the legal analysis we have also discussed a clear overview of the current legislations applied at a national level in Madrid, Spain and Stockholm, Sweden. The two cities present great importance as being the places for the realization of the project trials and thus needed to be carefully examined with regard to the development of these planned PoCs. Additionally, the current study on national legal frameworks, as these are described by the respective formal national data protection authorities, explored the relation of each member state's basic principles to the EU legislations, as well as the unavoidable existing heterogeneity. This heterogeneity will be furthered studied so as to account for and analyze more detailed implications found across different city scenarios. National legislations are in accordance to the European ones, but there is a need for development of new policies in order to clarify the use of new technologies and its incidences in fundamental rights of citizens. Likewise, intromission in privacy and personal data are justified by means of public safety, security and fight against crime following the legal provisions expressed in this document, but confrontation between rights shall be analysed in more detail in SafeCity Policy Making [1].

7.2 Social Considerations

We have also looked into the social dimension of the technical innovation brought by SafeCity. Emphasis was given on the validation that the proposed designs improve the quality of life rather than burdening it. The social aspects of the technologies to be applied were studied, taking into account a more general perspective upon modern ICT, including automation, surveillance and web-based designs. Upon this analysis we highlighted the risk of a technical innovation becoming a burden to the society, arising from a divide which pre-exists (e.g. educational, economic, etc) and leading to wider social divides. The above ultimately introduces a strong paradox and "give-take" procedure which needs to be dealt with extra care: **technical innovations are introduced and found to be related to social prosperity yet malicious effects may also be found across different social groups**.

A “black-and-white” policy being in total favor or not of technical advancements cannot be applied, as this ignorantly shades the underlying parameters. Accordingly, a “justified-by-the-means” strategy also cannot be acceptable, as it still does not specify “the means”. Social implications are in fact rather complex as they depend upon social relations, which in turn can be expressed in terms of spatial allocations, temporal allocations, culture, history, etc. Each society is different, reflects upon different needs and presents different tolerances. Also, social relations need to be studied across different levels: citizen-to-citizen, citizen-to-technology application, citizen-to-technology provider, society-to-society, etc. In that sense, social scientists need to provide advices and insights upon the underlying relation mechanisms existing across different societies and within them as well (different society levels).

We have stressed the importance of defining social implications and according policies, which at a minimum should rely on parameters other than those causing such social effects, unless otherwise found necessary. Even in that case however, we have noted the importance of allowing alternative solutions to exist as well (e.g. citizens alerts should not depend only on web and/or cellular telephony channels, but also on altering mechanisms in the area).

7.3 Ethical Considerations

Accordingly, ethical considerations were explored, to describe the general accountable and responsible framework that should be obeyed when handling sensitive data and exploiting surveillance technology. Ethical considerations have emerged from both the social and legal analysis and they present a more gerenal framework to be considered for designing and applying new technologies.

As the name suggests, such considerations outline the basic *ethical principles* that developers, practisioners and policy makers should follow. Ensuring ethical designs is not an easy task as ethical burdens appear to exist on greater or smaller levels. Also, when a case cannot be concretely defined by legislation, ethics become an issue of personal judgment (“what is right”, “what is wrong”, “what is the common good”, “what constitutes a society threat”, etc). In that sense, ethical considerations also imply the necessity for modest designs, keeping in mind that the centre of attention should be *the citizen* (with no specific name, history, education, background, etc) and not the acquisition of results and technical achievements. Ethical experts need to overview and provide guidance on such considerations.

7.4 SafeCity Implications

Finally, an overview of such implications were mapped upon the SafeCity Concept and functionalities and suggestions were defined towards the adoption of technical methods assuring ethical designs, via the description of relevant enablers and features’ functionalities and also management and control policies. Implications on legal and ethical issues are dealt, and will be dealt, by the Consortium, through the Management, Control Policy and Technical implementation. Following the definition and description of technical functionalities (enablers) to describe the SafeCity innovative design, we have explored the sensitive cases (with regards to the aforementioned implications) which exist in Public Safety use cases and the technical developments that need to be ensured in order to ensure these. In the cases where technical developments could not be introduced and/or would not suffice, respective policies have been suggested. In that sense, the current research has tried its best to deliver a) definitions of the sensitive cases in SafeCity and b) respective alternative strategies for dealing with them. Further analysis of these considerations is explored in [1].

8. Annex 1: Interview questionnaire template

*Dear Madame/Sir,

Thank you for accepting to provide your contribution to this study, which is performed within the scope of the EU funded project **Safecity** http:/www.safecity-project.eu/

The purpose of this questionnaire is to gather contributions from Data Protection Authorities in Europe on citizens' attitudes towards data protection. We particularly aim to assess to what extent EU citizens have access to their personal information, if they are able to correct it and how DPAs are supporting these claims. We are proposing the following questionnaire to the Data Protection Authorities in all EU Member States. We believe that the collected contributions will be of the utmost importance for our study.

If you agree, the following questions will be posed to you during a short telephone interview. In alternative, you could choose to reply to the questionnaire in a written form. Please let us know, at your earliest convenience, what is your preference by replying to the email that accompanies the questionnaire.

About you and your institution

1) Please provide us with a brief introduction of your DPAs and an outline of your role
2) With respect to other activities, what is the effort your institution put in hearing and investigating citizens' complaints?

Categories of citizens addressing the DPA and types of complaints

3) Year by year, do you see a difference in the number/type of complaints received?
Which sectors are mainly involved? (e.g.: data protection in internet, video_ surveillance in public spaces, surveillance at work, etc)
4) How do people address your institution (e.g. through your website, through phone calls, trough mail)?
5) What types of claims do they more often pose? (e.g.: asking what are their rights in a specific case? Requesting assistance to access information? Requesting a prior checking opinion? Reporting violations of data protection rules?)
6) What are the main data protection issues at stake in citizen's complaints? (e.g. alleged violations relating to access and rectification; data misuse; excessive collection; request of deletion of data)
7) With reference to the complaints received, in how many admissible complaints do you find breaches of data protection rules?

Thank you for your patience

For further information please contact: safecity@aratos.gr

*This questionnaire was also used in Greek Language, alternated per different occasion.

9. Annex 2: Telephone interviews

The Netherlands

University Hospital Maastricht (azM). Telephone Interview with Mr. Leon Ubachs, expert in Data handling of patients.

July 5, 12:00-12:30

Greece

Civil Protection Authority of Grevena. Telephone Interview with Mr. Giorgos Kourellas. Chief of Civil Protection Department in Western Macedonia Region. Responsible for surveillance means in region and data handling.

August 1, 10:00-10:45

Greece

Emporio.Net. Private Company which installing surveillance cameras (e.g shops, private places, etc). Mr. Spiros Goudevenos, general manager of the company.

July 6, 13:00-13:30

Greece

DIVICO Security. Private Security Company which operates private surveillance cameras, receiving video and images from surroundings. Mr. Spiros Koutsogiannis, Marketing and Sales Manager

July 15, 17:00-17:30

Greece

Hellenic Data Protection Authority (HDPA). Interview with Mrs. Athina Burka. Public Relations Officer.

September 3, 9:45-10:15

Greece

Vodafone Hellas. Telecommunications Operator. Interview with Mr. Thanasis Ioannidis, Core Network Analyst.

September 6, 18:00-18:45