D7.1 Ethical and Legal Requirements

Start Date of Project: 01/01/2014  Duration: 24 months

<table>
<thead>
<tr>
<th>Project Funded by the EC Directorate General for Home Affairs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Due date of deliverable</td>
</tr>
<tr>
<td>Actual submission date</td>
</tr>
<tr>
<td>Lead partner</td>
</tr>
<tr>
<td>Participant(s)</td>
</tr>
<tr>
<td>Work package</td>
</tr>
<tr>
<td>Classification</td>
</tr>
<tr>
<td>Version</td>
</tr>
<tr>
<td>Total number of pages</td>
</tr>
</tbody>
</table>
DISCLAIMER

The work associated with this report has been carried out in accordance with the highest technical standards and SAMi2 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

<table>
<thead>
<tr>
<th>Partner</th>
<th>Authors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Middlesex University</td>
<td>Dr. Carlisle George &amp; Dr. Penny Duquenoy</td>
</tr>
</tbody>
</table>

© SA Mi2 Consortium
Table of contents

List of Authors ........................................................................................................................................... 3

1 Introduction ........................................................................................................................................... 14

2 SAMi2 Description ................................................................................................................................... 15
  2.1 Introduction and processes .................................................................................................................. 15
  2.2 Use cases ............................................................................................................................................ 17

3 Ethical Issues ........................................................................................................................................... 18
  3.1 Background ......................................................................................................................................... 18
  3.2 Ethics within co-funded European Research Technology projects .................................................. 19
  3.3 EU Co-funded projects within the Security Domain ......................................................................... 20
    3.3.1 The DETECTOR Project ............................................................................................................. 22
    3.3.2 The INDECT Project ............................................................................................................... 23
    3.3.3 The ETTIS Project ................................................................................................................... 24
    3.3.4 The SurPRISE project .............................................................................................................. 24
    3.3.5 The SURVEILLE Project ......................................................................................................... 25
    3.3.6 The SAPIENT Project .............................................................................................................. 27
    3.3.7 The PRISMS Project ............................................................................................................... 28
    3.3.8 The PACT Project ................................................................................................................... 29
    3.3.9 The ASSERT Project ................................................................................................................ 31
  3.4 Summary of EU security projects and ethics ..................................................................................... 31
  3.5 Discussion .......................................................................................................................................... 32
  3.6 Ethics of research on Social media .................................................................................................... 35
  3.7 Ethical use of Twitter data .................................................................................................................. 37

4 Legal Issues ............................................................................................................................................ 42
  4.1 Online Social Networks ..................................................................................................................... 42
  4.2 Twitter and Legal Aspects .................................................................................................................... 42
    4.2.1 Terms of service for Twitter users .............................................................................................. 42
    4.2.2 Twitter Privacy Policy .............................................................................................................. 44
    4.2.3 Twitter Developer Policy and Agreement ............................................................................... 45
    4.2.4 Legal rights in tweets ............................................................................................................... 46
  4.3 Privacy and Data Protection Rights ................................................................................................... 49
    4.3.1 Introduction .............................................................................................................................. 49
    4.3.2 European Convention on Human Rights ............................................................................... 50
    4.3.3 Charter of Fundamental Rights of the European Union ....................................................... 52
  4.4 EU Data Protection Legal Framework ............................................................................................... 52
    4.4.1 Introduction .............................................................................................................................. 52
    4.4.2 Recommendation R(87)15 ...................................................................................................... 53
    4.4.3 Council Framework Decision 2008/977/JH .............................................................................. 55
    4.4.4 EU Data Protection Directive (Directive 95/46/EC) ................................................................. 56
    4.4.1 Proposed EU Data Protection Directive for the Police ............................................................. 61
  4.5 Spain: Data Protection Legal Framework .......................................................................................... 64
    4.5.1 Introduction .............................................................................................................................. 64
    4.5.2 Organic Law 15/1999 and Royal Decree 1720/2007 ................................................................. 65
List of Figures

Figure 1 - Simplified processing flows in SAMi2 ................................................................. 15
List of Tables

Table 1 – Twitter information elements in SAMi2 index ...............................................................16
Table 2 – Relevant EU co-funded projects in the Security domain .............................................22
# Glossary

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASSERT</td>
<td>Assessing Security Research: Tools and Methodologies to measure societal impact</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>DETECTOR</td>
<td>Detection Technologies, Terrorism, Ethics, and Human Rights</td>
</tr>
<tr>
<td>ECHR</td>
<td>European Convention of Human Rights</td>
</tr>
<tr>
<td>ECtHR</td>
<td>European Court of Human Rights</td>
</tr>
<tr>
<td>ETTIS</td>
<td>European security Trends and Threats In Society</td>
</tr>
<tr>
<td>EGE</td>
<td>European Group on Ethics</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>INDECT</td>
<td>Intelligent Monitoring for Threat Detection</td>
</tr>
<tr>
<td>PACT</td>
<td>Public Perceptions of Security and Privacy</td>
</tr>
<tr>
<td>PRISMS</td>
<td>Privacy and Security Mirrors</td>
</tr>
<tr>
<td>SAPIENT</td>
<td>Surveillance, Privacy, Ethics</td>
</tr>
<tr>
<td>SurPRISE</td>
<td>Surveillance, Privacy and Security</td>
</tr>
<tr>
<td>SURVEILLE</td>
<td>Surveillance: Ethical Issues, Legal Limitations, and Efficiency</td>
</tr>
</tbody>
</table>
References

Laws and Regulations


Council Framework Decision 2008/977/JH on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.


Criminal Procedure Act (Spain) - Ley de Enjuiciamiento Criminal. Available at: http://www.elra.eu/wp-content/uploads/file/Civil_Procedure_Act_%28Ley_de_Enjuiciamiento_Civil%29%5B1_%5D.pdf


EU 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 or the safeguarding against and the prevention of threats to public security, and the free movement of such data. Available at: http://data.consilium.europa.eu/doc/document/ST-12555-2015-INIT/en/pdf


Law 9/2014 on telecommunications which regulates the secrecy of communications and the protection of personal data within electronic communication networks and services among others. This law also replaced the General Telecommunications law 32/2003
Maastricht Treaty (establishing the European Union). Available at:

Organic Law 15/1999 on Personal Data Protection (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal or LOPD). Available at:
http://www.legislationline.org/documents/id/9044

Resolution 1373 (2001), Adopted by the Security Council at its 4385th meeting, on 28 September 2001. Available at:
http://unispal.un.org/UNISPAL.NSF/0/392A001F254B4B9085256B4B00708233

Resolution 1456 (2003) Adopted by the Security Council at its 4688th meeting, on 20 January 2003. Available at:

Royal Decree 1720/2007 relating to Organic Law 15/1999 on Personal Data Protection. Available at:

Spanish Constitution. Available at:
http://www.congreso.es/portal/page/portal/Congreso/Congreso/Hist_Normas/Norm/const_espa_texto_ingles_0.pdf

Spanish Law 22/11, of 11 November of 1987, on Intellectual Property. Available at:

The Charter of Fundamental Rights of the European Union. Available at:

UK Copyright, Designs and Patents Act 1988. Available at:

U.S. Copyright Act, 17 U.S.C. Available at:
http://www.copyright.gov/title17/circ92.pdf

UK Trade Marks Act 1994. Available at:

Case Law


Dick v Yates (1881) 18 Ch D 76.
Exxon Corp. v. Exxon Insurance Consultants International Ltd [1982] Ch. 119.
Francis Day & Hunter Ltd v Twentieth Century Fox Corp Ltd [1940] AC 112.
Feist Publications Inc. v. Rural Telephone Service Co, 499 U.S. at 345.
Kirk v Fleming [1928-35] MacG Cop Cas 44.
Rotaru V. Romania: (application No. 28341/95); Judgment; Strasbourg, 4 May 2000, European Court of Human Rights [ECtHR]
Sinanide v La Maison Kosmeo (1928) 139 LT 365.
Walter v Lane [1900] AC 539.

Articles and Reports
Bieter, M (2013), The Rise and Fall of ETA, The Blue Review. Available at: https://thebluereview.org/rise-fall-eta/
Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System, Version 1.0. December 2011. (c) Crown Copyright 2011.


Lagazio, M (2012), The evolution of the concept of security. Thinker 43 (9), 36-43.


SurPRISE Project, Draft Report on Key Factors. Available at: http://surprise-project.eu


1 Introduction

The work presented in this deliverable D7.1 is aimed at discussing ethical and legal issues applicable to SAMi2 in order to identify relevant constraints and requirements.

To achieve this goal, in Section 2, this deliverable provides a brief explanation of the functioning of SAMi2 to provide a basic technical context in order to understand the ethical and legal issues that may arise, especially with regards to privacy and the processing of personal data.

Section 3 discusses relevant ethical issues associated with SAMi2 and articulates ethical requirements and guidelines. The section begins by setting the background context of ethics as expressed by the European Commission, and is followed by an overview of European projects addressing security, privacy and ethics. Following that will be a synthesis of the key points from those projects from which the key ethical principles will be derived. Finally issues related to ethical regarding research on social media and use of Twitter data will be discussed.

Section 4 discusses relevant legal issues with regard to the use of data from online social networks (and Twitter in particular), the right to privacy and the processing of personal data. This section will focus on relevant EU legal frameworks in addition to Spanish law. It will also briefly discuss future developments, in particular, the proposal for an EU Directive 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.
2 SAMi2 Description

2.1 Introduction and processes

The primary aim of SAMi2 is to gather and process information and data from Online Social Networks (OSN) in order to help prevent and fight Internet crime and become alerted to potentially dangerous situations in order to protect citizens and their surroundings. The gathering and subsequent processing of any information and data must be based on sound ethical principles and be in compliance with existing laws and regulations.

In order to understand the relevant ethical and legal issues that relate to SAMi2 a brief description of the system is outlined below.

Figure 1 shows a simplified flow of processes in SAMi2.

First the system actively seeks information from online information sources (Social Networking sites) via a web Crawler (a component of the SAMi2 system). With regard to Twitter, this is achieved by accessing the Twitter Application Programming Interface (API)\(^1\) made available to the public under specific terms.

The web crawler gathers different types of online information. With regard to Twitter, there are three categories of information/data that can be collected namely: structured data; non-structured data and semi-structured data. Only the first two categories will be collected for purposes of this project.

The information gathered by SAMi2 is first indexed by an Indexer component. Indexing consists of making the large volume of information searchable and retrievable according to certain criteria. The different types of elements included into the index built for Twitter messages in the SAMi2 application are shown in Table 1 (below).

---

\(^1\) https://dev.twitter.com/overview/api
### Twitter information elements in SAMi2 index (del Peso et al, 2015)

| Structured fields (from JSON message object fields) | Language  
geoLocation information:  
longitude, latitude, countryCode, countryName, placeName, placeFullName, placeBoundingBox, boundingBox, placeId, placeType  
timestamp  
social information:  
userid, profileImage, profileBackgroundImage, userScreenName, userMentions, inReplyToStatusId, statusesCount, followersCount  
hashtags  
messageld | Basic NLP:  
Text chunking, tokenization, normalization: translation from Twitter specific language, formatting, lemmatizing  
Include synonyms (from WordNet\(^3\) (Miller, 1995) or similar lexical databases like MultiWordNet\(^4\)) |
| Non-structured text | Multimedia information | Image hashes, audio and video labels.\(^5\) |

#### Table 1 – Twitter information elements in SAMi2 index\(^6\)

SAMi2 also consists of an Anonymizer component that is used to anonymize (i.e. remove any identifiable personal data) the information to be indexed if necessary. The anonymizer will only be able to anonymize data in a structured form (e.g. userScreenName), therefore, it is possible that the contents of individual tweets may contain personable data.

After indexing and anonymising the collected information is then further processed by a number of specific semantics based modules in order to provide deep information processing and knowledge modeling.

Based on specific scenarios, the SAMi2 system will produce outputs in the form of a set of messages of interest to law enforcement to help: alert them to potentially

---

\(^2\) These elements are used to build up a network model of relations between tweets and users.

\(^3\) [http://wordnet.princeton.edu/](http://wordnet.princeton.edu/)


\(^5\) These elements are not currently extracted by SAMi2 application, but are expected to be included into the next development iteration of the system.

dangerous situations; prevent and fight crime; and protect citizens and their surroundings.

2.2 Use cases

The SAMi2 project will focus on six use cases (scenarios) involving the use of Twitter:

1. “Escrache”: Unauthorized spontaneous demonstrations at the personal residences of public figures such as politicians and government officials. Output from SAMi2 will enable the police to detect upcoming escrache events organized via tweets.

2. Gang activity: especially related to fights and vandalism during sporting events. Output from SAMi2 will enable the police to collect information on meeting times, dates and locations.

3. Illegal events: activities such as concerts and raves organized without the required authorization. Output from SAMi2 will enable the police to collect information on events including meeting times, dates and locations.

4. Hate speech: harassment or targeting of minorities, vulnerable groups or any subsection of society. Output from SAMi2 will enable the police to collect information on the contents of the tweet and other information that would lead to judicial authorization in order to identify and prosecute offenders.

5. Post mortem analysis: doing analysis after a crime has taken place. Output from SAMi2 will enable the police to reconstruct events in order to carry out further investigations and to gather intelligence on how to deal with future similar crime.

6. Terrorism: detecting any activity that may be involve terrorism. Output from SAMi2 will provide information and intelligence that can be useful to relevant security services.
3 Ethical Issues

3.1 Background

Ethics as a topic is a highly complex notion that encompasses philosophies coming from a variety of philosophers and religious movements. The scope of this deliverable is to provide an ethical basis for the analysis of technologies which are specifically designed for use in a European context, that is, to take an ‘applied ethics’ approach. As such the aim is not to attempt to unravel the complexities of ethical theory or movements, but to refer to a theoretical base in order to understand the underpinning of ethical norms that find their expression in practice. This section presents the perspectives on ethics taken from the perspective of funding bodies meeting ethical requirements, and professional bodies setting standards on ethics. The section begins by setting the background context of ethics as expressed by the European Commission, and is followed by an overview of European projects addressing security with some ethics component. Following that will be a synthesis of the key points from those projects from which the key ethical principles will be derived. Codes of conduct relevant to these types of projects will be analysed and discussed, and from there some recommendations regarding the SAMi2 case studies will be given. The position taken follows that of Peter-Paul Verbeek:

“If ethics is about how to act and designers help to shape how technologies mediate action, designing should be considered a material form of doing ethics. Every technological artifact that is used will mediate human actions, and every act of design therefore helps to constitute moral practices.” (Verbeek, 2011, P.91)

With the increased uptake and capacity of information and communication technologies particularly over the last 10 years, and the use of the Internet and social media by the general public introduced by Web 2.0, the awareness of the impacts of technology development both socially and ethically has also increased. In particular has been a raised awareness of the impact on privacy in the public arena, by academics and by funding bodies. Consequently technical development projects co-funded by the European Commission, committed to upholding the European Convention on Human Rights (through the European Charter of Human Rights) are required to consider privacy as well as other human rights issues that could be potentially challenged by technical developments. The consideration of ethics in proposals put forward for funding has always been a requirement but has moved from a focus on aspects relevant to medical research, to issues arising from Information and Communication Technologies (ICT) such as the protection of personal data and confidentiality of research participants and more recently with an increased focus on the societal impact.

---

7 Ethics: the science of morals and human conduct; moral principles; rules of conduct (The Oxford Encyclopedic English Dictionary, 1991)
and associated ethical issues, as expressed in the guidelines of the Framework 7 program.

This section sets out the background to the consideration of ethics in technology development projects funded by the European Commission and other research agencies, and the rationale for the inclusion of ethics with regard to information and communication technologies (ICT) development. In terms of this deliverable on legal and ethical requirements as ‘non-functional’ or ‘soft’ requirements, the inclusion and embedding of ethics in the technology development design and implementation is where the abstract notions of ethics meets applied ethics and design practice.

3.2 Ethics within co-funded European Research Technology projects

In their guidelines for funding within the Framework 7 programme, the European Commission provides ethical guidelines, including an annex applicable to ICT. The first sentence of this Annex states:

“In recent years there has been an increase in the importance of ethical issues related to ICT research and technological developments.”

Section 2.1 states that proposals must comply with Article 8 of the European Human Rights Convention, and in particular “given the pervasive and ubiquitous nature of ICT and the many opportunities if offers, researchers should consider the sensitive implications of their proposals for privacy and autonomy.” Further, under Section 2.2 on Privacy and informed consent, the guidelines state:

“The majority of European citizens view personal privacy as an important issue. ... Therefore, researchers must ensure that the manner in which research outcomes are reported does not contravene the right to privacy and data protection. Furthermore, researchers must carefully evaluate and report the personal privacy implications of the intended use or potential use of the research outcomes. Wherever possible, they must ensure that research outcomes do not contravene these fundamental rights.”

---

9 “1. Everyone has the right to respect for his private and family life, his home and his correspondence and 2. 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 wellbeing 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.”
The Horizon 2020 program followed Framework 7, and in the ethics guidelines for this latest program of research concerning human rights more specific guidance relevant to technologies is provided\(^\text{10}\). Of note to this project is that concerns regarding the impact on human rights are “primarily related” to the technologies relevant to this project as follows:

“**Research that could impact on human rights**—Concerns in this field are primarily related to research on surveillance technologies, new data-gathering and data-merging technologies (e.g. in the context of big data). However, social or genetic research that could lead to discrimination or stigmatization is also affected.”

The focus on human rights in the above guidelines does not mean that all ethical issues are covered however. Ethics and human rights are closely linked – for example personal autonomy, which is a necessary and fundamental requirement of ethics (the ability to determine how to live one’s life) is diminished if personal privacy is diminished. The argument being that people who are being watched alter their behaviour, that is to say, someone in the ‘privacy of their own home’ will behave differently to when they are in public (see e.g. Guelke and Sorrell, 2010 pp.8-9). Therefore, to deprive someone of ‘personal private space’ by operating surveillance (of various types) takes away their autonomy. Another ethical concept that can be affected by surveillance is human dignity, particularly so if the person under observation is not aware they are the object of attention. These ideas will be expanded upon later.

The guidance also provides some suggestions for risk mitigation, which include:

- a human rights impact assessment
- involving human rights experts in your research
- training of personnel and/or technological safeguards and
- caution when publishing or otherwise disseminating results, (e.g. through privacy by design)\(^\text{11}\)

### 3.3 EU Co-funded projects within the Security Domain

There were a number of projects funded by the European Commission under the FP7 security theme between 2009 and 2013 that have relevance to the SAMi2 project in terms of ethics and social impact (Table 2 below). The concept of ‘security’ is difficult to define as it can have different meanings in different contexts. The European Group on Ethics - accepting the ambiguity of the terms provides some general definitions for both security and surveillance – “security can be defined as ‘protecting people and the

---


\(^{11}\) The last bullet point is not very clear in its example of privacy by design, but could be interpreted as advising that publication of results may require anonymisation or other similar measures aimed at the protection of people who could be identified in the research dissemination materials.
values of freedom and democracy, so that everyone can enjoy their daily lives without fear"\textsuperscript{12}\textsuperscript{12} and for surveillance “the classic configuration sees surveillance presented as a means with security as an end”\textsuperscript{13}.

Many projects include in their discussions surveillance technologies, especially in relation to the funding remit which often focuses on counter terrorism. Although counter-terrorism is not in the scope of SAMi2, the types of technologies involved can be similar and the discussions in the projects around the types of technologies, and privacy and human rights issues have some relevance. The use of technologies that interrogate communications (as developed in this project) can be classed as a type of surveillance technology.

The projects listed in Table 2 below have particular relevance to this deliverable not only in terms of the focus on security and surveillance, but their focus on issues of human rights are aligned to ethical values of equality, autonomy, dignity among others. One project (ETTIS) differs in that it provides an overview of the key trends of security projects, noticing a move towards recognising that security (protection against national/global threat) is a combination of technology and society: “There has been a gradual shift from traditional concerns and threats, centred on state security, to a stronger societal focus”\textsuperscript{14}.

<table>
<thead>
<tr>
<th>Project</th>
<th>Duration</th>
<th>Key focus</th>
<th>Approach/theme</th>
<th>EU programme</th>
</tr>
</thead>
<tbody>
<tr>
<td>DETECTOR</td>
<td>2008-2011</td>
<td>counter-terrorism</td>
<td>ethical standards</td>
<td>EU FP7 - Security</td>
</tr>
<tr>
<td>INDECT</td>
<td>2009-2014</td>
<td>detecting crime with surveillance technologies</td>
<td>Development of ethics processes through the project</td>
<td>EU FP7 - Security</td>
</tr>
<tr>
<td>ETTIS</td>
<td>2011-2014</td>
<td>European security trends and threats in society</td>
<td>Analysis of projects for trends – security and/or society focussed.</td>
<td>EU FP7 - Security</td>
</tr>
<tr>
<td>SurPRISE</td>
<td>2012-2015</td>
<td>surveillance/privacy/security</td>
<td>Balancing trade-offs, privacy by</td>
<td>EU FP7 -</td>
</tr>
</tbody>
</table>

\textsuperscript{13} In Ethics of Security and Surveillance Technologies. Opinion No. 28 of the European Group on Ethics in Science and New Technologies. 2014 (p.14)
A brief summary of aspects of these projects considered relevant to SAMi2 is given below\(^\text{15}\).

### 3.3.1 The DETECTOR Project

The DETECTOR project\(^\text{16}\) takes a risk-based approach to provide an ethical analysis, using a matrix as their method, to a range of ‘detection technologies’. One of the technologies they assess is data-mining, which could be relevant to this project. They conclude that intrusiveness is a risk for data-mining, but there are different levels of intrusiveness depending on the level of ‘mining’ and aggregation of data. High aggregation of data is likely to be more intrusive. There is also a risk of discrimination from social identity. Data mining by its nature results in stereotypes which can lead to a suspicion of communities which is disproportionate to the few targets that belong to those communities. The effect of stereotyping, of individuals and communities, could result in members of those communities adapting legitimate behaviour because of the

\(\text{15}\) All of the projects listed here have a wealth of information in their public Deliverables comprehensively detailing aspects of their work. For the purposes of this deliverable on ethics requirements for SAMi2, the extracts have been selected for relevance to ethics, human rights, and the types of technologies that impact these areas. All project deliverables referred to can be found from the relevant project website.

\(\text{16}\) http://www.detecter.eu/
perceived risk that their behaviour may be misinterpreted, and they could become suspects. The perception of an individual that they are at risk from false interpretations of behaviour, and change their normal behaviour to fit a social norm, has been labelled as the ‘chill factor’. These risks come from the characteristics of the technology, and public perceptions regarding a risk to them from using technology in this way. A slightly different type of risk identified is unauthorised access to the system (from an internal or external source is not specified) but this risk also has a ‘chill’ factor in that uncertainty over who has access to the data add to the ‘chill’ and could inhibit behaviour that is disapproved of in wider society.

DETECTOR Ethics Summary – keywords: Privacy issues, impacting on autonomy of the individual, (changing behaviour); dignity (in cases of high level of intrusiveness) possibly reputation damage; discrimination; misleading interpretations (leading to unwarranted suspicion and subsequent impact on person).

3.3.2 The INDECT Project

The focus of the INDECT project on combatting terrorism and ‘other criminal activities’ aimed at the development of algorithms to support human decision-making. Examples of the criminal activities as given on their website include child pornography, detection of dangerous situations such as robberies, and the use of dangerous objects such as knives or guns in public spaces. The project received adverse media coverage in terms of ‘big brother’ on the basis of the surveillance aspects of the project. The negative coverage prompted a response by the European Commission explaining about the project and that the media had reported “misleading information”. A statement on the project website addresses the concerns: “INDECT is not installing any cameras in the EU; nor is it filming people at random. It is not connected to any existing database or social network.” It is interesting to note the growing emphasis on matters of ethics as the project progressed given in the four public deliverables covering the period 2009-2012.

Deliverable D0.8 gives an overview of the ethical issues addressed within the project based on the technical aspects of the system and subsystem. Issues mentioned (INDECT D0.8, p.17) are privacy in relation to pattern mining, a Blog analyser, and a system managing information about organised criminal gangs (accessible only to police officers and analysts under their national regulations and using technical access control mechanisms).

On the behavioural profiling system (p.18) they note the risk of stereotyping and in the development of the system “have explicitly avoided any prejudicial stereotypes”. They also recognise that this type of technology could be misused, emphasising the need for “carefully designed security protocols” to be followed, and further that: “The use of the
software needs to be entrusted to a democratically supervised and accountable security authority." Deliverable D4.15 gives more detail, using security procedures such as encrypted storage, encryption of data, all human activities on the system logged, data anonymised and can be de-anonymised when necessary (logged); legally authorised access where necessary (also logged), human verification of output to avoid false positives (INDECT D4.15, pp.10-11).

Another system relied on algorithms for face recognition, which is out of scope for this SAMi2 project. Also out of scope of this project is the work on automatic detection of events, from audio/video involving people and moving vehicles in urban areas (Deliverable D7.2).

WP6 addresses issues related to the INDECT portal (giving access to the systems) and refers to police policies on access (not specifically addressed in the public deliverable due to sensitivity of information and the diversity of policies in different countries). The deliverable document does however state that the portal supports the enforcement of such policies.

**INDECT Ethics Summary – keywords:** Privacy, stereotyping, security mechanisms (anonymisation, encryption, logging of user actions), human intervention (false positives), legal warrants, technology support and enforcement of policies.

### 3.3.3 The ETTIS Project

The ETTIS\(^2^0\) project notes a shift from a focus on technology as separate from society as a security tool used to protect against national or global threats, to a view on that acknowledges security is a combination of technology and society, and a trend towards a more societal context as noted earlier.

**ETTIS Ethics Summary – keywords:** societal context

### 3.3.4 The SurPRISE project

The focus of the SurPRISE\(^2^1\) project is privacy related to security and surveillance technologies, drawing on the views of European citizens through ‘Citizens Summits’ held in different European countries. Views of Spanish citizens on aspects of privacy and impact from some technologies related to cyber-surveillance, biometrics, behavioural profiling, and others, are represented in Section 4.4 of Deliverable 7.1 (Report on Decision Support Testing). Interesting explorations of privacy are provided in Deliverable D2.2, as well as clear explanations as to what privacy actually means to individuals, and the impact of the loss of privacy on other fundamental rights. Mapping concepts of privacy as physical privacy to functions of privacy such as capability for intimacy, and the relationship with fundamental rights, in this example human dignity allows an articulation of the privacy function (confiding, expressing oneself freely,

---

\(^{2^0}\) [www.ettis-project.eu](http://www.ettis-project.eu)

\(^{2^1}\) [www.surprise-project.eu](http://www.surprise-project.eu)
protect from others’ judgments etc.) allows a deeper understanding of the importance of privacy to ordinary life. The human rights covered in this mapping exercise are: Human dignity; Freedom of thought, conscience and religion, Freedom of assembly and of association, Freedom of expression.

A key message in relation to SAMi2 project is the high impact from data retention (as enabled by some of the technologies given above) on all types of privacy “as the variety of data than can be retrieved and stored is potentially unlimited, from consumption behaviour to health data, political beliefs and social relations” (D2.3 p.39). Further, that the use of deep packet inspection, which is linked to data retention, has the capacity to impact on human rights in terms of freedom of expression through the enabling of censorship, and personal autonomy through coercion as a result of observing communications, and of course privacy from the capability of large-scale real-time surveillance.

**SurPRISE Ethics Summary – keywords:** Privacy, security, surveillance, fundamental human rights, censorship, autonomy.

### 3.3.5 The SURVEILLE Project

The SURVEILLE project undertakes a survey of the range of surveillance technology deployed in Europe with the intention to assess the benefits and costs, and to identify, elaborate and assess the whole range of legal and ethical issues raised by these technologies in the context of terrorism and other crime. The primary focus in Deliverable 4.2 is on the analysis of large volumes of data, specifically of ‘predictive analytics’ in the context of social media, referred to as ‘open source data’.

The SURVEILLE project undertakes a survey of the range of surveillance technology deployed in Europe with the intention to assess the benefits and costs, and to identify, elaborate and assess the whole range of legal and ethical issues raised by these technologies in the context of terrorism and other crime. According to the author of the deliverable “Predictive profiling of social media by law enforcement proves especially problematic where its efficacy is largely dependent upon a broad, sweeping analysis of communications” and further that “Conceptually, a crucial distinction is that by which public authorities may determine that the use of ‘open source intelligence’ obviates the requirement to duly consider the right to respect for private life, including private communications” (D4.2, p.42). It is not made clear by the author whether publicly available communication types, such as Twitter, falls within this category of private communications.

The author warns of the implications of predictive and behavioural profiling for the purposes of law enforcement from the perspectives of the technology (accuracy) and

---

22 Table 6: Relationships among privacy dimensions, functions and fundamental rights p.68 D2.2 Draft Report on Key Factors available from http://surprise-project.eu
23 www.surveille.eui.eu
impact on societal behaviour (changed behaviour as a result of perceptions of being constantly under observation). From the technology perspective there is concern about the capability of the technology to accurately interpret the relationships, associations and networks accurately. An example is given that suggests the changed behaviour would result in a changed set of norms that would become new norms and standards from which to make assumptions. Behavioural change, of individuals and consequently society, would be to conform, to keep a low profile, to try to be invisible. This example underlines the role of privacy as a human right, the diminishing of which has an impact on freedom of association, freedom of thought and conscience, and the prohibition of discrimination. In the words of the author: “The indivisibility, interdependence and interrelatedness of rights evoke the criticality of our recognizing the intrinsic value of protecting human dignity” (D4.2, pp.41-42).

From the technology perspective part of the problem are a number of risks identified regarding the quality of the decision-making that are embedded in systems. A significant risk can be raised from the premise that the algorithms used in the system (on which the decisions depend) are impartial, i.e. that they do not have any ‘predisposition or bias’. This impartiality, according to the author, is not present due to the value judgments necessarily included in the design. Users should be aware that discriminatory practices can become ‘embedded and perpetuated’ in the profiling process. Also emphasised is the risk of a system hiding practices that are discriminatory – whether through lack of thought, or by intention (Deliverable 4.2, pp.43-44).

Locational privacy also comes under scrutiny in D4.8\(^\text{25}\) which gives examples of different locational contexts and expectations of privacy both in the home and in public showing the different degrees of privacy that might be expected dependent on the situation. The discussion of different examples clearly shows why privacy is such an important concept for society, and significance of the societal impact (discussed above regarding behavioural change). Although the deliverable states at the beginning that a perspective will be taken later in the deliverable on law enforcement applications, this is not evident.

Finally, a summary of the fundamental rights that are at risk from surveillance are given as: freedom of movement, freedom of association, freedom of assembly, freedom of expression, freedom of thought, conscience and religion, the right not to be discriminated against, and the right to liberty of the person (Scheinin and Sorell, 2015)\(^\text{26}\).

\(^{25}\) Guelke, J. D4.8 Ethical analysis of the right to privacy in different locations, 2014.
\(^{26}\) Scheinin, M. Sorell, T. D4.10 Synthesis report from WP4, merging the ethics and law analysis and discussing their outcomes, 2015.
3.3.6 The SAPIENT Project

The SAPIENT project had as its aim the identification and analysis of impacts posed by future smart surveillance technologies. The context of use of these technologies to be assessed, as given on their website, is to “identify potential evil-doers” in order to control crime in urban settings, border control and critical infrastructure protection. Specifically this means the smart surveillance systems will be used to profile citizens.

A risk assessment method is developed based on privacy impact assessments, which are already in general use in organisations, that is to say ‘tried and tested’. The output of the project is a surveillance impact assessment manual (D.4.4. SIA Manual, 2014). Using the step by step guide the organisation assesses the threats to primary and supporting assets, examples of which are given, such as privacy, dignity, reputation (as primary assets) and a supporting asset is an information system or organisational component (SAPIENT, D4.4, p.9). The threats to risk are identified as (i) feared events (e.g. false accusation) and (ii) threats caused by the exploitation of vulnerabilities. A sample list of threats and vulnerabilities is provided in Annex B of this deliverable, including a sample list of the source of threats (organisations developing or deploying the system) and include among others interception of communications and monitoring of web activities carried out by an individual (D4.4 p.43). One of the suggested vulnerabilities given, relevant to an organisation using a surveillance system, is the information system configuration (p.45). Assets to be protected are also identified in Annex B for a range of stakeholders (individuals, groups, society, an organisation), and those given as assets to individuals include: material or physical assets, personal data, privacy, dignity, autonomy or free choice, reputation or image, individuality, self-esteem, life-chances (opportunities) or one’s job and/or career (revenue-generating capacity) (p.42).

Annex D provides a short questionnaire that can help stakeholders identify privacy issues and ethical issues. The privacy issues section is based on the eight principles of data protection (EU Data Protection Directive 95/46/EC). For example, under the heading of data retention the question is asked: “is data retained without a set period of time for deletion?”. There are only two options for the answer, yes or no. In the table on p.49 of the manual, an answer of ‘yes’ to that question is a privacy issue. A similar table is supplied for identifying impacts of ethical issues, examples are given below (p.52):

<table>
<thead>
<tr>
<th>Impact</th>
<th>Question</th>
<th>Yes or No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethical</td>
<td>-Is the dignity of the individual protected under the surveillance system?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Have individuals freely given their explicit informed consent to being monitored, tracked and/or targeted?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Is trust between those surveilled and the organisation undertaking the surveillance or between individuals or groups and the government maintained and protected under the surveillance technology or system?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>-Are there clear lines of accountability? Who will be responsible if the surveillance system is found to be unduly intrusive?</td>
<td></td>
</tr>
</tbody>
</table>

NO = ethical issue
And for societal impact:

<table>
<thead>
<tr>
<th>Impact</th>
<th>Question</th>
<th>Yes or No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Societal</td>
<td>- Does the surveillance in question have a negative impact on social cohesion or trust?</td>
<td>Yes = Societal issue</td>
</tr>
<tr>
<td></td>
<td>- Does the project, technology, application or service increase or decrease social affiliation or isolation?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Are their other options available to achieve a given social objective (e.g. a reduction in violent crime or in benefits fraud)?</td>
<td></td>
</tr>
</tbody>
</table>

The rationale provided for such an assessment is provided in Deliverable D66 (Policy Brief) where attention is given to the different data types available in surveillance, one is metadata and the other is data from the content of communications. In terms of data protection, note is made that this:

“distinction between personal data and metadata becomes irrelevant when several sources of data about one individual are cross-referenced … thus a huge risk for the fundamental right to data protection is that operational data gathered and shared by law enforcement authorities in the EU without any safeguards for the individual might reveal personal information about him or her. Moreover, metadata might be more revealing than content” (p.15)

SAPIENT Ethics Summary – keywords: as privacy, dignity, reputation, personal data, dignity, autonomy or free choice, reputation, individuality, self-esteem, life-chances, informed consent, accountability.

3.3.7 The PRISMS Project

The PRISMS project investigated aspects of security and privacy against the backdrop of rhetoric on the ‘trade-off’ notion (the idea that to achieve security privacy must be compromised). The project undertook an EU wide survey to examine whether people evaluate the concept of trade-off between security and privacy when security technologies are introduced with the aim of identifying the factors influencing public assessment of security and privacy technologies.

Seven types of privacy are given (attributed to Zagazio, 2012) which are: Physical security, political security, socio-economic security, cultural security, environmental security, radical uncertainty security, information security. The questions in the survey are based on these types. Outcomes of the survey were that general security and personal security were highly correlated, and that there is no “significant correlation between people's valuation of privacy and their worries about security on the level of

28 www.prismsproject.eu
attitudes” (not actual behaviour), and that a “simple trade-off between citizens’ privacy and security perceptions does not exist”\(^{30}\).

The project also investigated the relationships between security and privacy to develop a decision support tool for supporting investors and stakeholders in “reconciling security and privacy, trust and concern”. In further understanding the trade-off model, and its context in European policy, the publication (output from the project) on this issue concludes that privacy and security are different values which cannot be compared or ‘weighed’ noting Zedner’s (2009)\(^ {31}\) two differences countering the notion of balancing:

“The first is that, as we have already observed, we are weighing collective interests against those of small minorities or individuals. The second is what might be called temporal dissonance, namely the fact that we seek to weigh known present interests (in liberty) against future uncertainties (in respect of security risks)” (in van Lieshout et. al. 2013, p.124).

The authors also point out the inconstancy in attempting any balance, on the argument that if privacy is a necessary factor for democracy then giving that up for security undermines democracy\(^ {32}\) (van Lieshout et. al. 2013, p.124).

**PRISMS Ethics Summary – keywords: Privacy, security, privacy/security trade-off.**

### 3.3.8 The PACT Project

The PACT\(^ {33}\) project investigated public perceptions on issues of security and privacy related to security/surveillance technologies by conducting a large scale pan-European survey of citizens (PACT, D3.3). The end mission of the project was to produce a Privacy Reference Framework for Security Technology and Decision Support System to assist end users in considering privacy and fundamental rights in evaluation of proposed security investments. The output of the project was a software tool that can be used to assess levels of privacy risk. From their investigations of types of privacy associated with a range of technologies they developed a taxonomy and mapping matrix which uses four aspects of privacy in relation to today’s technologies: Privacy of Personal Information; Privacy of the Person, Privacy of Personal Behaviour and Privacy of Personal Communications (PACT, D1.3). Under these headings a range of technology driven contexts are given, including communications surveillance and location determination (relevant to this SAMi2 project).

---


\(^ {33}\) www.projetpact.eu
The risk to personal privacy under these headings is assessed as likely or unlikely, with explanations for each of the four perspectives. In the Communications surveillance category it is likely that: privacy of personal information, privacy of the person, privacy of personal behaviour and privacy of personal communications are all affected. Their general interpretation of communications surveillance appears to focus on interception, either through wire-tapping or email.

In the location determination category, the first three types of privacy are also considered likely, with the Privacy of personal communications indicated as unlikely. The types of privacy infringements described are from e.g. sensor networks for smart homes, health monitoring systems, which transmit a variety of information. The transgression of privacy under the personal behaviour description notes that behavioural analysis can be performed from the collection of information from multiple sensors.

Of particular interest for this project is the report on functional specifications (PACT, D6.2), an extract is given below on the privacy risk for data surveillance, communications surveillance and location determination from the comments written into the program:

"dataveillance": "Consequences of this risk, which is real, can be very serious: identity fraud and/or theft, stalking, surveillance without consent, profiling and tracking, etc.

"Communications_surveillance": "The purpose in communications surveillance is not usually specified. Sometimes communication surveillance are performed for example for counter terrorism and are performed by policy or by the government, in these cases the data will be more controlled. But in most of the times this communication surveillance are performed for malicious purposes, so these privacy risks are very serious, intrusion, data theft, data retention, espionage, workplace control. Communications secrecy: Evaluations based on subjective information; Privacy of third parties."

"location_determination: "Redundant high accuracy location information can be exploited for out of (sic.) requested application requirements and objectives."

Other functions include context which is relevant to the risk factor. Extensive details are given in the report D6.2, as well as screen shots of the tool interface with responses on example scenarios. Finally, some key concerns identified regarding social media are given (PACT, D1.1, p.70):

"concerns about data protection, privacy, surveillance, inequality, consumer and advertising culture, inequality, and discrimination arise in the context of Facebook and other commercial social media."
3.3.9 The ASSERT Project

The ASSERT project aims to provide proposers of security projects the means to assess societal impact integrated into the proposal development and provides a societal impact assessment tool for security projects to meet the objectives of the project.

Interaction with stakeholders solicited views on impacts which have been categorised in themes: Way of life, fears, aspirations; culture and community; political systems; environment; health and well-being; personal and property rights. These categories provide the core of the societal assessment tool. The steps to be followed for each of the dimensions are:

1. Examine whether the security research project meets the needs of society;
2. Integrating a second time through the same six aspects, review the potential externalities or costs to society, enumerating risks and identifying ways to mitigate them;
3. Finally, pass through the six societal impact aspects a third time to identify potential benefits to society.

A set of questions are offered to help the consideration of the above elements. Included in the list of questions are several related to human rights, such as "How could the research have a negative impact on human dignity?" with similar phrasing on the right to life, equality, freedom of thought, among others. Another question addresses the potential for discrimination on specific groups, and/or vulnerable groups. Also included are questions on the benefits to society of the proposed development. (ASSERT Deliverable 3.1 Societal Impact Assessment Manual and Toolkit, 2014.).

3.4 Summary of EU security projects and ethics

The projects above can be categorised into different themes, DETECTER and INDECT were developing technologies and considering the ethical aspects of the technologies under development. ETTIS, SURPRISE and SURVEILLE were investigating the links between technology and society (ETTIS) and assessing surveillance technologies in Europe from the perspective of impact and views of European Citizens (SURPRISE) and assessments of the value (in terms of efficiency) against benefits and costs (SURVEILLE). SAPIENT also took an impact assessment approach with future...
surveillance technologies in mind and provided a framework for future development against which impact could be considered and assessed. PRISMS looked at the notion of trade-off, often put forward in defence of surveillance technologies in that to provide security citizens may need to accept some loss of privacy, and both PRISMS and PACT sought the views of citizens across Europe on these matters, the latter (PACT) providing a risk assessment tool to help developers to assess the privacy/security risks. Another assessment tool was provided by the ASSERT project, this time for societal impacts with the negatives weighed against the benefits to society.

### 3.5 Discussion

The projects briefly described in the previous section are addressing the dilemma of the use of technology in providing security to citizens on behalf of state, and specifically in projects –co-funded by the European Commission, applied in Europe for protection (security) of European citizens. The difficulty the projects address is how to exploit the capabilities of the technologies available, and the technologies in use by citizens, to meet security needs, while at the same time keeping a commitment to the core values and fundamental rights of citizens. According to the Institute for the Protection and Security of the Citizen (European Commission, Joint Research Centre, 2014) publication consolidating the Opinions 26-28 of the European Group on Ethics (EGE):

“In the EU vision, security, including cyber- and ICT security, is grounded, to be legitimate, in the European fundamental rights and values”. Further, “Access for all, democratic and efficient multi-stakeholder governance, and shared responsibility to ensure security are further elements of this normative landscape.” (pp 6-7)

However, as noted in the Ethics Summaries for those projects, some core fundamental values are potentially at risk from the technologies developed to protect citizens. When considering surveillance technologies, as a means to provide security, the political perspective of technology use comes to the fore, and it is often this side that concerns citizens. Surveillance, according to the publication of 2014 above “even more than security, is traditionally linked to the images of power and control.” (Ibid.p.8)

Understanding the technology and its capabilities is key to understanding the ethical and societal risks of employing it, additionally understanding the context in which it is used helps to determine whether boundaries of privacy are crossed, or need to be crossed, and what forms of governance provide the boundaries of use:

“Together with sovereign States, corporations, groups, and individuals can now intrude in all aspects of life. All these unleashed powers need to be rethought on order to assess and balance them, to harmonize them with...”

fundamental rights, and to ground them in more robust forms of democratic legitimacy.” (Ibid. p.8)

The scope of use is also relevant to these discussions, and it is important therefore to be clear at the outset of a development project what the objectives of the use of these technologies are. For example, there were concerns in some of the projects above (e.g. SURVEILLE) about using technology for ‘predictive’ policing, and in particular when used for profiling citizens’ behaviours in order to try and circumvent threats to society. While SAMi2 is not intending to profile behaviours or predict in the above sense, one of the scenarios proposed is to alert police of an illegal event that is being planned. The difficulty then arises, and poses the question, “knowing that an event is planned, is it beneficial to the police, and society, to know who are involved in the planning” and further, if identified, would the SAMi2 system – through its learning capabilities – start to focus on, or be alert to, these individuals. In this way, profiling of a sort is taking place.

According to the SURVEILLE project (D4.2, p.5):

“The distinction between descriptive and predictive profiling has to date evolved in accordance with established differentiations made between anticipatory or preparatory acts and, contrastively, criminal actions having already been committed”.

In this regard ‘preparatory acts’ in e.g. event planning would be classed as ‘predictive profiling’, as the descriptive profiling is based on events having happened. However, there is a more narrow interpretation given that applies to the context of SAMi2, an explanation of predictive profiling according to the deliverable 4.2 (referring to Harris37, 2003) is given as:

“predictive profiling resolves to identify, in advance of a specific criminal act occurring, those who may be predisposed toward engaging in unlawful activities for the purposes of prevention.”

Why is profiling an issue here? Again, according to the discussions in the SURVEILLE project, and findings in the literature, where monitoring of behaviour is understood by ‘the monitored’ to be taking place, those included in the surveillance system are likely to change their behaviour so as not to ‘stand out of the crowd’. The ethical implications of this are that all citizens, including honest and law abiding citizens, are in some way coerced by technology (and the use to which is it put, or perceived to be put) to hide what they would like to do, or what they would like to discuss with friends or others. This undermines individual autonomy – an ethical principle that is the foundation of what it is, or should be, to be human – that is, an individual’s right to ‘be themselves’, self-determining in life choices and actions.

If this changing behaviour were to happen, the first impact is that explained above (the loss of personal autonomy), there is however another impact, also discussed in the D4.2, which has to do with the way the technology works. If the system that is being used to anticipate illegal events is based on algorithms that learn from the data that is provided (by the citizen), which in most cases is likely, and in the case of the SAMi2 system is how the system will work, then as the behaviour of the citizens gradually change in order to avoid being highlighted as 'citizens of interest', the system will itself adapt to the changed data, and those changed behaviours would become the new norm. This is problematic in that the interpretations of the data by the system, although accurate (based on way the system has been developed), do not accurately reflect the people involved in this data collection in terms of their intent, or their relationships. Taking this a step further, and potentially even more problematic, is that this ‘adapted behaviour’ of the users (i.e. society) is recognised by the system as a new norm. If some of these people are planning events, and adopting behaviour that is recognised by the system as potentially risky (i.e. that this new norm is likely to result in an illegal event), then again, other innocent people will be caught up in this, and find themselves implicated in criminal activities.

In the case of SAMi2, is the intention in to identify the individuals planning an unlawful event, or just the event? If individuals are to be identified from the data then according to the above, predictive profiling is taking place. If the information collected (data) comes from tweets is it possible to profile? If the profiling is not undertaken by the system, but is instead undertaken by police analysts, does this make a difference? In as much as experienced analysts and police officers develop profiles from prior experience, and may demonstrate bias, it should be recognised as such by the analyst. That is, it seems not possible to bring previous experience, and consequent bias, into the picture. The difference between the system and the human analyst is that the analyst and/or colleagues can recognise bias and take remedial action. If the system is developing bias (through its previous experiences) it is hard to see how the bias might be recognised, and addressed due to the algorithms and learning operations.

In respect of the above, Article 49 of the European Code of Police Ethics\(^{38}\) (p.11) stipulates that investigations made by law enforcement officials prove impartial and be suitably sensitive to citizens’ requirements, stating:

> Police investigations shall be objective and fair. They shall be sensitive and adaptable to the special needs of persons, such as children, juveniles, women, minorities including ethnic minorities and vulnerable persons.”

Noted in SURVEILLE D4.2 "the use of the investigatory technique in respect of predictive modeling for preemptive purposes may require exceptional review so as to discern whether it meets this standard" (see Appendix to the Recommendation Rec (2001) 10 of the Committee of Ministers to member states on the European Code of Police Ethics, adopted by the Committee of Ministers 19 September 2001)

3.6 Ethics of research on Social media

Undertaking research using social media presents a dilemma to researchers in that it presents a rich resource of social data but at the same time it is not clear whether the information put on social media is in a private or public space, this is particularly true of Facebook for example, perhaps less so for Twitter. More importantly perhaps is whether the users of social media believe themselves to be acting in a private or public sphere. It is the level of privacy expected by the user that is central, regardless that information put on social may be deliberately shared with many, it is ‘who’ the many are, and whether the user intends to share with them that is key. The temptation put in front of researchers to access such a rich source of research material is high, particularly if there is a clear social benefit from the research.

Principles of research ethics agreed by many, are “obtaining informed consent, maintaining confidentiality and anonymity, and minimizing risk of harm to participants and researchers” (Beninger et.al. 2014 p.6). The implications of doing otherwise are: covert collection of data about people; sharing the content of the information with others and identifying from whom it came (most likely publicly); and not being at all concerned about the people involved in the research and whether they may be harmed, but more concerned about the research result. Respect for others is a foundation for ethics, “the dignity and worth of the human person and in the equal rights of men and women” forms part of the Preamble to the Universal Declaration of Human Rights.39

Social media presents challenges to researchers firstly from the principle of informed consent, in that a researcher announcing their intention of studying a group discussion, for example, is at risk of influencing the discussion by their presence. Another problem related to consent is whether the person has the capability of (a) understanding (being informed) and (b) an adult and able to give consent. Depending on the social media used, and how it is used, it can be easy for people to create a fake identity. This fake identity potentially creates an additional problem for researchers, aside from the capability to consent, which is whether the results of the research are affected by ‘fake’ participants in terms of representing a sample population that have been specifically selected. Maintaining confidentiality can also be problematic, as even anonymizing information (data) may not be enough to keep the identity of a person confidential. In such a rich social setting where large amounts of information are exchanged between people it could be easy to identify a person or persons from contextual information.

Moreno et al. (2013) take a different perspective on the ethics of social media research. They look at the different methods of research that involve the study of people, and identify three categories of research “observational research, interactive research, and survey/interview research.” In the case of observational research, which is the most relevant of the three categories for the SAMi2 project, this is classed as “exempt” from Institutional (ethics) Review Boards (IRB’s) “if the following conditions are met, access to the SMW [Social Media Website] is public; information is identifiable, but not private; and information gathering requires no interaction with the person who posted it online”. This is because of the public nature of the research, which equates in non-digital life to, for example, observing people on the street:

“Exempt research includes research involving the observation of public behavior, except when information obtained is (a) recorded in such a manner that subjects can be identified either directly or through the identifiers linked to the subjects, or (b) any disclosure of subjects' responses outside the published research that could reasonably place the subjects at risk of criminal or civic liability, or be damaging to the subjects' financial standing, employability, or reputation.” (p.709)

The authors note that social network sites such as Facebook and LinkedIn would come into this category, as long as only publicly available material (they refer to profiles) were used – that is, there would be no interaction with the people observed. They also note that in addition to protecting the privacy of the website user the privacy guidelines of the social network provider and legal considerations must be taken into account. In reporting a case from one university studied by the authors, Facebook policy (at the time of writing the article) is given, which clearly separates Facebook from the research:

“If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.”

If privacy settings are in place then it is assumed the research is longer exempt from ethics review. The exemption from ethics review also does not apply where children (minors) are involved – as they might be in the case of Facebook and Twitter. For Facebook the minimum age is 13 years old. Twitter does not set a minimum age, but it does offer the opportunity for users to provide their date of birth so that they can be protected from inappropriate advertising. With regard to privacy options, Twitter states:

“our Services are primarily designed to help you share information with the world .... Our default is almost always to make the information you provide public but we generally give you settings to make the information more

40 https://support.twitter.com/articles/20169945-age-screening-on-twitter#
What can be drawn from the above for SAMi2? The ethical significance of the public versus private nature of the context in which the information (data) is provided, and that publicly available data is ethically acceptable to study with certain conditions. People should not be publicly identified (for example, in publishing results of the research), or be put at risk. In the context of this project the risks given in the quotation above, “criminal or civic liability, or be damaging to the subjects' financial standing, employability, or reputation” would only apply to people not engaging in criminal activity (i.e. people who are innocent) as crime – and therefore ‘criminal liability’ and its consequences for the person who has broken the law – are the specific focus and objective of the product developed from the research. From the technical point of view, it is necessary to take all possible measures to filter our persons not perceived to be engaging in criminal activity from the system. There could also be serious issues if children are using Twitter and included in the SAMi2 system results – police procedures should be put in place to address this issue. Finally, the terms of use of the social network must always be taken into account.

3.7 Ethical use of Twitter data

The use of social media data for police intelligence purposes can have negative consequences, as pointed out by Fuchs and Trottier in their discussions on surveillance of social media, in that a culture of suspicion – as has been seen post 9/11 - could result in “constant monitoring of social media” which carries the implication that all users of social media “are actual or potential criminals” unless proved otherwise (2013, p.21). This, as noted earlier in this document (p.22) from the DETECTOR project, can result in the ‘chill factor” whereby people adapt their behaviour to conform.

This adaptation of behavior has implications for free speech and free expression, it is related to social media users’ perceived capability to freely, and without coercion, exercise their right to free speech and free expression – the coercion arising from the potential consequences of speaking freely.

Another concern expressed by Fuchs and Trottier is that of stereotyping, and the risk of “suspicion of communities which is disproportionate to the few targets that belong to those communities”. The stereotyping of communities could also include “groups that already face discrimination in Western societies, like immigrants, people of colour, people of Arabic or African background, the poor, the unemployed, political activists and that thereby stereotypes and discrimination are deepened and reified” (Ibid. p.19). Again, such stereotyping and discrimination is likely to lead to the “chill factor”. It has also been noted earlier, in the commentary on the DETECTOR project, that unauthorised access, or not knowing who has access to data, can contribute to the “chill factor”.

private if you want. Your public information is broadly and instantly disseminated." (p.710)
The INDECT project (this document, p.22) have recognized some of these problems, on the issue of stereotyping the project states in the development of the systems they “have explicitly avoided any prejudicial stereotypes”. On the subject of misuse they emphasise the need for “carefully designed security protocols” need to be in place (such as logging activities, anonymising data, legally authorised access where necessary). Similarly the SAPIENT project identifies risks, and threats to risks which are (i) feared events (e.g. false accusation) and (ii) threats caused by the exploitation of vulnerabilities.

The concept of privacy has received a lot of attention in the EU projects described above and in the media. The loss of privacy can result in the ‘chill factor’ for the reasons explained above, and articulated by the SurPRISE project in terms of what privacy enables (i.e. the functions of privacy) such as “capability for intimacy, and the relationship with fundamental rights, in this example human dignity allows an articulation of the privacy function (confiding, expressing oneself freely, protect from others’ judgments etc.)” (this document, pp.22-23).

Also of note to this SAMi2 project is the possibly misleading distinction between metadata and personal data identified in the SAPIENT project (this document, p.27) which is that the first (metadata) has less risk in identifying people, and thus less risk as far as data protection principles are concerned. They make the point that combining several sources of data can carry a risk to individuals, and that meta-data can provide more revealing information about an individual than might be supposed.

The issue of trust has come up in several of the EU projects, with outcomes such as the “chill factor” already mentioned, but also in the context of citizens concerns identified by the PACT project with regard to social media:

"concerns about data protection, privacy, surveillance, inequality, consumer and advertising culture, inequality, and discrimination arise in the context of Facebook and other commercial social media." (this document, p.30).

In light of the issues summarized above, and expressed in the INDECT project (this document, p.22) “The use of the software needs to be entrusted to a democratically supervised and accountable security authority.”

The view above has been emphasized in one of the Newsletters produced by the PACT project on deep packet inspection (DPI) in connection with surveillance technologies. It reviews the export of surveillance technologies incorporating DPI by European companies to countries outside the EU that could impinge on fundamental human rights, and notes that a resolution was passed in 2011 banning the “export of IT systems that can be used "in connection with a violation of human rights, democratic principles or freedom of speech [...] by using interception technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of Internet use (e.g. via Monitoring Centres and Lawful Interception Gateways). The countries to which exports of this nature are banned are: “Argentina,
There is no doubt that social media plays a significant role in society in organizing events and mobilizing activists, whether judged to be for the good in acts of liberation against oppressive states, or protests against other groups or communities. The evidence provided by the media over the last few years gives testament to this. What is of interest to note for this project in those situations is the convergence of different types of social media. For example, it has been noted in Eaton (2013, p.13) that with regard to the Egyptian uprising "Facebook was most important in the build-up to the protests, Twitter was a far more effective tool for activists once on the ground, as they were often able to use the Twitter interface through their mobile phones" and ‘cascade information through networks at high speed. This is relevant to the SAMi2 system in distinguishing between social media types, such as Facebook, which is considered to be private by many users, and therefore not in the scope of this project– as opposed to Twitter which is for the most part public, and has data provided by Twitter for development use.

In summary, there are societal consequences to be borne in mind when monitoring social media, even when protecting citizens. There is a danger of loss of trust through an overuse of technologically inspired monitoring systems. Therefore this is the first of the ethical requirements and followed by requirements drawn from this and the preceding sections:

*Ethics RQ1: Identify scope of system use, particularly the limits and boundaries of use.*

*Ethics RQ2: The system must support fundamental human rights within the boundaries given in the context of use (policing and legitimate aims of protecting citizens and preventing crime), and avoid stereotyping and discrimination on the grounds of ethnic origin, political opinion, and religious beliefs.*

*Ethics RQ3: To protect innocent people the system must have the ability to anonymise data, and de-anonymise if necessary (with a rational for de-anonymisation provided).*

*Ethics RQ4: All actions on the system taken by users must be logged, and individual users’ identified (through authentication mechanisms).*

*Ethics RQ5: Development decisions relating to the AI components should be logged and be available for verification if asked for.*

The requirements above can be supported by guidelines suggested in the context of research and the ethical use of Twitter data. Although the use of Twitter data in the context of police investigations is different from researchers in, for example, universities, using this data for social or other research, the following guidance
provided by Rivers and Lewis (2014) could in part be relevant to SAMi2. The authors have devised a list of keywords, produced to give the overall acronym of TACTICs, as follows:

*Tactics for the Ethical Use of Twitter Data* (Rivers and Lewis, 2014)

T  **Transparent** - make objectives, methodologies, and data handling practices transparent and easily accessible
A  **Anonymity** - protect the anonymity of tweet authors by not publishing identifiable information without consent.
C  **Control** - Honor Twitter users’ efforts to control their personal data by omitting private and deleted tweets.
T  **Tracking** - No tracking users across multiple sites without consent unless IRB approves.
I  **IRP** - Work collaboratively with IRB for study designs that may compromise privacy and anonymity.
C  **Context** - Respect the context in which a tweet was sent.

In particular, the notion of transparency could be transferred to the SAMi2 system, especially in regard to data handling practices. The system should be able to log actions taken by users, and on the developers side key decisions should be explained and logged – for example, for the selection of algorithms and reasons behind the choice of algorithms used. Anonymity is also relevant to the SAMi2 system, as has been discussed earlier, and is closely related to the “Control” bullet point which follows. Tracking is relevant, especially in terms of cross referencing between social media sites. For the IRP section, which is about “Institutional Review Boards” the guidance provided by the European Commission on ethics, and also local guidelines (for example police guidelines, or Codes of Conduct if they exist) are relevant here. Last but not least is the “Context” in which the Tweet was sent – context is highly relevant when making any analysis of data by technological means, and needs to be considered by the human operators (intelligence analysts) when the results of the analysis are presented to them.

Some of the requirements listed also constitute good practice, as expressed for example in the “Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System” (2011) produced in the UK by the Forensic Science Regulator. For example under Section 20.18 Control of data:

20.18.1.1. The provider shall have procedures within its management system to ensure that all necessary information is recorded accurately, maintained so that its authenticity and integrity is not compromised, and is retained and destroyed in accordance with the provider’s retention and destruction policy.

Under Section 20.18.2. Electronic information capture, storage, transfer, retrieval and disposal:
20.18.2.4. Where information in the form of a compound document is stored (e.g. embedded files, hyperlinks), the linkage of all elements of the compound document shall be stored in line with the provider’s retention policy along with their content.

On the subject of databases (Section 20.18):

20.18.4.2. Providers shall maintain a list of all databases used to make inferences and interpretation; this includes, but is not limited to, those internally developed, commercially developed or remotely accessed.

20.18.4.3. Information included in all databases used to make inferences and interpretations shall be capable of authentication through documentation to its original source, meet a minimum quality standard specified by the owner of the database, be validated for accuracy of transcription on entry to the database, and be auditable for corruption.

20.18.4.4. Any programs or script for data manipulation employed within databases to make inferences and interpretations shall be validated, either separately or as part of the process or method they are used in as laid out in these Codes, e.g. with reference to the impact of any uncertainty of measurement and the risk of false positives/negatives.

Developers working on systems that provide for law enforcement agencies should look at the requirements for this domain. The complete Codes of Practice document is available online, together with a separate Appendix document focussing on digital forensic services (Codes of Practice and Conduct. Appendix: Digital Forensic Services. 2014).
4 Legal Issues

4.1 Online Social Networks

Online Social Networks (OSN) enable activities such as information creation, sharing, exchange and interactions between people across geographic, cultural and socio-economic boundaries. The information created, shared or exchanged using OSN can be either public or private (restricted to one or more persons) based on the privacy settings of a particular user. Currently the popular OSN include Facebook, Twitter, Flickr and YouTube.

SAMi2 will primarily focus on gathering and analyzing data from Twitter, therefore, the focus of this deliverable will be on discussing relevant legal issues related to use data from Twitter.

4.2 Twitter and Legal Aspects

Twitter is an online social network platform that allows users to share various kinds of information including facts, thoughts and jokes using 140 characters or less. Each 140-character message is called a tweet. A tweet can also contain an image, however, for this project only textual tweets will be collected and processed. An individual registered with Twitter can either post a tweet or read using a website or an application on a mobile device. Posted tweets can be private or public depending on the level of privacy that the user selects. An unregistered user can only read a tweet.

4.2.1 Terms of service for Twitter users

Twitter's Terms of Service governs users' access to and use of Twitter services. They also inform users of the respective legal rights of both parties (i.e. users and Twitter).

Under it's Terms of Service in Term 1 Twitter informs users that:

"The Content you submit, post, or display will be able to be viewed by other users of the Services and through third party services and websites."

In Term 2, Twitter informs users that any information collected from them is subject to use according to Twitter’s privacy policy. Further that the use of Twitter services implies that users consent to their information being collected and used (in accordance with Twitter’s privacy policy) including the transfer of information to the United states and other countries for storage, processing and use by Twitter.

41 https://twitter.com/
42 https://twitter.com/tos
Twitter accepts that users retain rights in their content, however, users also grant Twitter a license to use that content in various ways including redistribution (Term 5):

“By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed).”

Further any content can be made available to third parties (Term 5):

“You agree that this license includes the right for Twitter to provide, promote, and improve the Services and to make Content submitted to or through the Services available to other companies, organizations or individuals who partner with Twitter for the syndication, broadcast, distribution or publication of such Content on other media and services, subject to our terms and conditions for such Content use.”

In Term 8 Twitter states that it will not disclose identifying information to third parties except in accordance with their privacy policy. They however provide instances in which disclosure will be made to third parties:

“We also reserve the right to access, read, preserve, and disclose any information as we reasonably believe is necessary to (i) satisfy any applicable law, regulation, legal process or governmental request, (ii) enforce the Terms, including investigation of potential violations hereof, (iii) detect, prevent, or otherwise address fraud, security or technical issues, (iv) respond to user support requests, or (v) protect the rights, property or safety of Twitter, its users and the public.”

Twitter explicitly allows interaction with its data (consisting of tweets and accompanying attributes) using its API. Third parties are allowed to access and encouraged to re-use Twitter content (Term 8):

“We encourage and permit broad re-use of Content. The Twitter API exists to enable this.”

As noted earlier SAMi2 will collect data from the Twitter API for analysis.
4.2.2 Twitter Privacy Policy

Twitter’s Privacy Policy informs users about the collection, use and sharing of their information.

Users are informed that all tweets are public by default and can be viewed all around the world instantly. They are also informed that their name and username used to create or reconfigure a Twitter account are listed publicly on their Services including on a user’s profile page and in search results. Via privacy settings users can decide whether others (the public) can find them using an email address or cell phone number.

Users are informed that the provision of information to Twitter implies making that information public:

“Most of the information you provide us is information you are asking us to make public. This includes not only the messages you Tweet and the metadata provided with Tweets, such as when you Tweeted, but also the lists you create, the people you follow, the Tweets you mark as favorites or Retweet, and many other bits of information that result from your use of the Services.”

Users, however, can opt for more privacy:

“Our default is almost always to make the information you provide public for as long as you do not delete it from Twitter, but we generally give you settings to make the information more private if you want.”

Users are warned that public information is widely disseminated and used by third party developers and organization for a variety of reasons, including to analyse trends and insights:

“Our Services broadly and instantly disseminate your public information to a wide range of users, customers, and services. For instance, your public user profile information and public Tweets are immediately delivered via SMS and our APIs to our partners and other third parties, including search engines, developers, and publishers that integrate Twitter content into their services, and institutions such as universities and public health agencies that analyze the information for trends and insights. When you share information or content like photos, videos, and links via the Services, you should think carefully about what you are making public.”

https://twitter.com/privacy?lang=en
4.2.3 Twitter Developer Policy and Agreement

The Twitter API gives developers access to Twitter’s global stream of Tweet data. Various streams can be captured from the API namely: public streams, user streams and site streams.

Twitter’s Developer Policy and Developer Agreement govern the use of Twitter information. They provide rules and guidelines for developers who interact with Twitter’s ecosystem of applications, services and content.

The Developer Policy contains the following:

I. **Guiding principles**: to maintain the integrity of Twitter’s products; to respect users’ control and privacy; to clearly identify a developer’s service; to keep Twitter spam free; to be a good partner to Twitter; to avoid replicating the Twitter experience, to engage in appropriate commercial use.

   With regard to the activities in SAMi2, the principle guidelines regarding respect for user’s control and privacy are very important. Examples include the following requirements: not to share or publish protected Content, private or confidential information; delete Content that Twitter reports as deleted or expired; modify Content that Twitter reports has been modified.

II. **Rules for specific products or features**: for example Twitter login and Social updates among others.

The Development Agreement contains the following:

I. **Twitter API and Twitter content**: Definitions, grant of license from Twitter and incorporation of terms into the agreement.

II. **Restrictions on Use of Licensed material**: important among some of the restrictions are that location data can only be aggregated, cached or stored in conjunction with the Tweet to which it is attached.

III. **Updates**: That Twitter may update or modify their APIs from time to time and at their sole discretion.

IV. **Ownership and Feedback**: Twitter asserts that Licensed Materials are licensed and not sold and that Twitter, its licensors and end users retain all worldwide rights to the Licensed Materials and Content.

V. **Termination**: Twitter reserves the right to immediately terminate or suspend the agreement at its sole discretion.

---

44 https://dev.twitter.com/overview/terms/policy
45 https://dev.twitter.com/overview/terms/agreement
VI. **Confidentiality**: Where access to confidential information is given by Twitter, such information cannot be disclosed without Twitter’s prior written consent. Further, the information must be protected from unauthorized use, access or disclosure.

VII. **Other important Terms**: e.g. User protection, Government use Compliance with Laws: Export and Import, among others.

Under it’s User Protector section the agreement asserts that API content should not be used: to assist law enforcement to conduct surveillance on content where a court order is required; and to violate the human rights of any person.

“A. User Protection. You will not knowingly: 1) allow or assist any government entities, law enforcement, or other organizations to conduct surveillance on Content or obtain information on Twitter’s users or their Tweets that would require a subpoena, court order, or other valid legal process, or that would otherwise have the potential to be inconsistent with our users’ reasonable expectations of privacy; and 2) display, distribute or otherwise make available Content to any person or entity that you reasonably believe will use such data to violate the Universal Declaration of Human Rights.”

The collection and processing and tweets in SAMi2 will not violate any of the terms quoted above. No actions carried out in SAMi2 are actions that require a court order, or violate the human rights of any person.

4.2.4 Legal rights in tweets

An essential question is whether users have any legal rights in tweets that they post to the public, and whether these tweets attract any legal protection that would to prevent use of such public tweets in the SAMi2 project.

4.2.4.1 Tweets and Privacy Rights

The right to privacy is a fundamental human right enshrined in Article 8 of the European Convention of Human Rights (ECHR).

Solove (2002) identifies at least six conceptions of privacy namely: (i) the right to be let alone; (ii) the ability to limit access to oneself; (iii) the ability to conceal certain matters from others; (iv) the ability to control information about oneself; (v) the protection of one’s personality and (vi) the ability to control access to intimate aspects of one’s life.

An interesting legal question is whether one can claim privacy rights in tweets that are posted in the public domain.

---

In *Rotaru v Romania (2000)*, European Court of Human Rights (ECtHR), in a judgment concerning an action under Article 8 of the ECHR, noted at paragraph 56 that “...public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities.”

This principle was further reiterated in the later ECtHR judgment in *P.G. and J.H. v. the United Kingdom (2002)*, where the Court stated at paragraph 56: “There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of “private life”.”

These ECtHR judgments imply that authors of tweets made public may have privacy rights in these tweets under some circumstances. These circumstances would include where tweets from identified users are systematically collected by law enforcement and stored in files (with their identifying information), without the necessary legal or judicial authority.

In SAMi2 use of an anonymiser component will result in the removal of any identifying information in structured data collected. Further tweets will not be stored based on any identifiable individual. Privacy rights and associated legislation will be discussed further below.

### 4.2.4.2 Tweets and Data Protection

Data protection law is concerned with the processing of personal information, defined under the EU Directive 95/46/EC (on data protection) as:

“...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,”

From the definition above, it is clear that a tweet or API tweet data can contain personal information. Such personal information may exist, for example, in structured data, e.g. a Twitter identifier/field (e.g. use ID or name), or in unstructured data (e.g. the contents of a tweet). Where personal data is identified in structured data then this will be anonymised, however, personal data in the text of tweets may not be easily identified. The processing of some tweets will therefore be protected under data protection law and data subjects will have accompanying data protection rights. For this reason, data protection legislation is discussed in greater detail below.

---

47 Rotaru V. Romania: (application No. 28341/95); Judgment; Strasbourg, 4 May 2000, European Court of Human Rights [ECtHR].

4.2.4.3 Tweets and Intellectual Property Rights

This section examines whether the 140 character tweet text is protected by intellectual property law, specifically copyright law and trade mark law, and the implications for SAMi2.

Copyright is an intellectual property right given to an author of a work. Copyright law gives the author various rights with regard to the commercial exploitation and reproduction of his/her work. Copyright also exists in sound recordings, films and typographical arrangement of published editions. The requirement for a work to be original is essential for the work to be protected by copyright. Such a requirement is common copyright law in general. This is confirmed in Chapter II (Article 10) of Spanish Law 22/11 of 11 November of 1987, on Intellectual Property, and other similar legislation such as Section (1) of the UK Copyright, Designs and Patents Act 1988 and §102 of The U.S. Copyright Act, 17 U.S.C. In the UK, originality requires that the author has exerted sufficient ‘effort, skill and time’ or ‘skill, labour or judgment’ to create the work. Under US copyright law, originality includes skill and labour but for a work to be copyrightable there must be “at least some minimal degree of creativity”. Various judicial rulings across multiple jurisdictions have concluded that copyright protection does not extend to short texts such as single words, titles, slogans, and short phrases, since they do not meet the level of originality (and/or creativity) required for copyright protection. Similarly where a tweet consists of only text, the 140 character limit of a tweet will not give rise to copyright protection primarily because it is difficult to establish sufficient creativity and originality with such a small character limit.

If the text of a tweet contains a trade mark, then another intellectual property protection regime (i.e. Trade mark law) can be used to protect the contents of a tweet. A trade mark is “Any sign capable of being represented graphically which is capable of distinguishing goods or services of one undertaking from another.” Infringement of a trademark occurs when someone who is not the trade mark owner uses the trade mark in connection with the sale of his/her goods or services (i.e. the trade mark is used in a commercial sense). In SAMi2, the contents of tweets will only be collected and...
analysed, and will not be used in a commercial sense. Therefore, even where tweets contain trade marks, use in SAMi2 will not infringe any rights.

4.3 Privacy and Data Protection Rights

4.3.1 Introduction

The right to privacy and the right to data protection are two rights enshrined in EU treaties, legislation and case law.

The right to privacy (respect for private life) is guaranteed under Article 8 of the European Convention on Human Rights (ECHR)\(^{60}\), and in Article F(2) of the Maastricht Treaty\(^{61}\) (which established the EU) the Union committed to respect all fundamental rights under the ECHR. The right to privacy is also guaranteed under Article 7 of the Charter of the Fundamental Rights of the European Union\(^{62}\) and is protected as an important principle in EU Law\(^{63}\).

The right to data protection in Europe was established by the Council of Europe’s “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”, (also known as Convention 108)\(^{64}\) which came into force on 1st October 1985. This led to many signatory countries enacting different legislation regulating the automatic processing of personal data. In an effort to harmonise data protection laws across the EU and hence facilitate the free flow of data within the EU, the European Commission proposed the Data Protection Directive (Directive 95/46/EC)\(^{65}\) in 1995. Data protection is also guaranteed under Article 8 of the Charter of the Fundamental Rights of the European Union.

The terms ‘Privacy’ and ‘data protection’ are sometimes used interchangeably however, the two rights are not completely the same, as seen by the distinction given to them in the Charter of the Fundamental Rights of the European Union. Kokott and Sobotta (2013)\(^{66}\) argued that in the context of EU law and jurisprudence, there are two major distinctions between the two rights namely: (i) the scope of (or information covered under) the two rights. The scope of Data protection is broader than the scope of privacy - data protection regulates all information relating to an identified or identifiable individual, however, privacy can be restricted to certain types of information. Also legal persons (e.g. companies) are excluded from data protection but have a right

---


\(^{63}\) For example see: CJEU, Case 136/79 National Panasonic v Commission [1980] ECR 2033, paras 17 et seq

\(^{64}\) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CL=ENG


to privacy; (ii) differences with regard to permissible interferences with the two rights. Under certain conditions (e.g. consent, legitimate basis, fair processing) there is no interference with data protection rights, however, there may still be interference with privacy rights, needing justification as required by law for such interference.

The following section focuses on relevant EU legislation to further discuss privacy and data protection.

4.3.2 European Convention on Human Rights

The European Convention of Human Rights (ECHR) established various fundamental rights and freedoms for all individuals in Europe, as well as the European Court of Human Rights (ECtHR). It was drafted in 1950 by the Council of Europe and came into force in September 1953. All 47 member states of the Council of Europe are signatories to the ECHR and the EU, under Article F(2) of Maastricht Treaty, affirmed that it would respect the rights guaranteed in the ECHR. The fundamental rights and freedoms under the ECHR must be complied with by public bodies (authorities) including courts and law enforcement, subject to some exemptions. Of particular importance in the context of the objectives of the SAMi2 project is Article 8 (ECHR): The right to respect for private and family life.

Article 8 states that:

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.”

2. 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 wellbeing 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.”

4.3.2.1 Public information and Privacy rights

Rulings by the ECtHR appear to indicate that an individual can have privacy rights in information that is public.

In Rotaru v. Romania (ECtHR, 2000), the Court stated that:

“45….public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities.”

67 The ECtHR hears complaints by individuals on alleged breaches of human rights by states who are signatories to the ECHR.
This was further noted in the later case of *P.G. and J.H. v. the United Kingdom* (ECtHR, 2002):

“56…..There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of “private life”.”

### 4.3.2.2 Interference under Article 8 (ECHR)

In *Leander v. Sweden* (ECtHR, 1987)\(^{68}\), The Court stated that three conditions had to be satisfied before there could be said to be interference with the right to respect for private life under Article 8 ECHR: (i). information had to have been stored about the person concerned; (ii) use had to have been made of it; and (iii) it had to be impossible for the person concerned to refute it.

The court further noted the need to examine whether the interference was: (a) in accordance with the law and (b) necessary in a democratic society.

The court explained that “*in accordance with the law*, mean that:

“50…..*the interference must have some basis in domestic law. Compliance with domestic law, however, does not suffice: the law in question must be accessible to the individual concerned and its consequences for him must also be foreseeable …*”

This was further explained in the later case of *Rotaru v. Romania* (ECtHR, 2000):

“52.....*the expression “in accordance with the law” not only requires that the impugned measure should have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects”

With regard to what is “*necessary in a democratic society*, The Court in *Leander v. Sweden* (ECtHR, 1987), explained that:

“58....*The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued*…”

Proportionate means that there is a balance between the severity of the interference with the individual right and the importance to the public interest.

---

4.3.3 Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union became legally binding on EU institutions and national governments on 1st December 2009 (when the Lisbon Treaty came into force). The Charter declares all rights of the inhabitants of the EU – including civil, political, social, and cultural rights. It is consistent with the European Convention of Human Rights but broader in scope. Two important aspects of the Charter in the context of the SAMi2 project are Article 7 and Article 8.

Article 7 guarantees the right to respect of private and family life:

“Everyone has the right for his or her private and family life, home and communications”.

Article 8 guarantees the right to protection of personal data:

“1. Everyone has the right to the protection of personal data concerning him or her.
2. 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.
3. Compliance with these rules shall be subject to control by an independent authority.”

4.4 EU Data Protection Legal Framework

4.4.1 Introduction

The current EU legal framework regulating the processing of personal data in the police sector primarily consists of:

- Council of Europe Recommendation R(87)15 regulating the use of personal data in the police sector;
- (EU) Council Framework Decision 2008/977/JH on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters; and

---

69 The Council of Europe is a human rights organization consisting of 47 member states, 28 of which are members of the European Union. See: http://www.coe.int/aboutCoe/

• (EU) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.\(^1\)

At the time of writing this deliverable (2015), The EU data protection legal framework is undergoing a review with the proposal for a new legal framework consisting of two legislative proposals\(^2\) namely:

- 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). This Regulation will replace the current Directive 95/46/EC and will 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 (i.e. law enforcement).

- 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 Directive will apply to law enforcement and will therefore be relevant to the activities of the SAMi2 project.

Currently these proposals are undergoing revisions and amendments. They are expected to be in force by 2017. This deliverable will therefore focus on the current legal framework, however, the major principles of the latest version of the new Directive for law enforcement (which is still undergoing revisions) will be discussed.

4.4.2 Recommendation R(87)15

On 17\(^{th}\) September 1987, the Council of Europe’s Recommendation R(87)15 Regulating the use of Personal data in the Police Sector was adopted. This was the first proposal in Europe to specifically address data protection in the police sector. It reflected the provisions of Article 8 of the ECHR (right to privacy), and attempted to balance individual privacy rights with the interest of society in preventing crime and maintaining public order. It is non-binding on Member States, and therefore has been implemented to varying degrees. While this is not a recommendation from the EU, 28 member states of the EU are members of the Council of Europe, therefore, this recommendation is discussed under the EU legal framework.

---


\(^{72}\) EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Recommendation R(87)15 applies to the collection, storage, use and communication of personal data used for police purposes. Personal data is defined as any data relating to an identified or identifiable individual. The Recommendation sets out a number of principles that are briefly summarized below.

4.4.2.1 Control and Notification

Each member state must have an independent supervisory authority outside the police sector to ensure compliance with the principles of Recommendation R(87)15. Various notification requirements to this supervisory authority are given under this principle.

4.4.2.2 Collection of data

Data collection should be limited to what is necessary for police purposes (prevention of real danger or to suppress a specific criminal offence), except where specific national legislation provides otherwise.

A data subject must be informed of data collected and stored about him/her without his/her knowledge if not deleted, as soon as there will be no prejudice to police activities.

Data collection by technical surveillance or automated means should be regulated by special provisions.

The collection of sensitive personal data (e.g. racial origin, religious beliefs, sexual life, political opinions) is not permitted unless absolutely necessary for a particular investigation.

4.4.2.3 Storage of data

Data stored for police purposes should be limited to data that is accurate and necessary for the police to perform their functions.

Categories of data stored should be distinguished: according to their degree of accuracy or reliability; and according to whether data is based on facts versus opinions or personal assessments.

Data collected for administrative purposes which needs to be stored permanently should be a separate file from police data, and not subject to rules applicable to police data.

4.4.2.4 Use of data by police

Data collected and stored for police purposes should only be used for these purposes.
4.4.2.5 Communication of data

This section sets out the criteria for the communication of data: within the police sector; to other public bodies; to private bodies; via international communication; and where requests are made to the police.

Of interest to the SAMi2 project is the communication of data within the police sector for police purposes. This is only permissible where there is a legitimate interest for the particular communication as provided for by an existing legal framework detailing the powers of the two bodies involved in the communication.

4.4.2.6 Publicity and rights of data subjects

Data subjects have various rights (subject to exemptions) such as: the right of access to their police file; the right to rectify inaccurate data held in a police file; and the right of erasure of data that is excessive or irrelevant.

Any refusal or restriction of these rights needs to be made in writing to the data subject who can appeal to the national data protection supervisory authority.

4.4.2.7 Length of storage and updating of data

Data should only be kept for as long as necessary for the purposes for which they were collected.

4.4.2.8 Data Security

Appropriate physical and logical security measures must be taken to secure data and to prevent any unauthorized access, communication or alteration.

4.4.3 Council Framework Decision 2008/977/JH

The Council Framework Decision 2008/977/JH on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, was adopted by the EU in November 2008. This Framework Decision is aimed at establishing common data protection measures for cross-border exchanges of personal data between law enforcement in the context of police and judicial cooperation in criminal matters. It seeks to ensure the fundamental rights of individuals, especially the right to privacy with respect to the processing of their data by police authorities. It contains various principles applicable where personal data processed by police authorities (for the prevention, investigation detection of criminal offences or the execution of criminal penalties) are or have been transmitted or made available: (a) between Member States; (b) by Member States to authorities or information systems established on the bases of Title VI of the Treaty of the EU; and (c) by authorities or information systems established on the basis of Treaty of the EU or the Treaty establishing the European Community, to competent authorities in Member States.
Since the SAMi2 system will only be used by the Madrid Police and the scope of the project does not include cross-border exchanges then the details of Council Framework Decision 2008/977/JH will not be fully discussed. In addition, the Madrid Police are already subject to the provisions of Council Framework Decision 2008/977/JH where any cross-border data exchanges are carried out between police authorities. Nonetheless a brief summary of some of the main provisions of the Framework Decision will be given below.

Council Framework Decision 2008/977/JH reiterates principles requiring the lawfulness of processing, proportionality and necessity when collecting data (Article 3).

Data should be kept accurate and erased when no longer required (Article 4).

Time limits must be kept for the erasure and review of data (Article 5).

Sensitive personal data (e.g. racial and ethnic origin, sexual orientation, political opinions, religious beliefs, health information and trade union membership) should only be collected if strictly necessary (Article 6).

Automated decision can only be made if authorized by law (Article 7).

The quality (accuracy, completeness) of data transmitted or made available for transmission must be verified and if incorrect data has been transmitted or data has been unlawfully transmitted then the recipient of the data must be notified (Article 8).

Time limits on the retention (by the recipient) of data sent can be set by the transmitting authority, however they shall not apply if the data are required by the recipient for ongoing policing purposes at the time of expiry of the time limits set (Article 9).

All transmissions must be logged and documented (Article 10).

Council Framework Decision 2008/977/JH contains a total of 28 Article addressing various other aspects regarding cross-border exchanges including: compliance with national processing restrictions; transfers to competent authorities in third States and international bodies; transmission to private parties in Member States; Information for data subjects; Rights of data subjects; Confidentially; Security; and penalties.

4.4.4 EU Data Protection Directive (Directive 95/46/EC)

The EU Data protection Directive (Directive 95/46/EC) came into law, 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). It encompasses the key elements from Article 8 of the European Convention on Human Rights (ECHR), i.e. the right to privacy in personal and family life, as well as in the home and personal correspondence. The Directive has been implemented into the national laws of all EU member states. Although the details of national laws regarding data protection vary in
some areas, the Directive 95/46/EC outlines the basic parameters within which these laws operate. Directive 95/46/EC is concerned with some very important individuals including: data subjects – individuals who are the subject of personal data and are given certain rights under the Directive; data controllers – individuals who determine the purposes for and manner in which personal data processed. The Directive places various obligations on them; the Information Commissioner – An individual who has various powers to make sure that data protection law is properly implemented in a each Member State.

4.4.4.1 Definitions

Article 2(a) of Directive 95/46/EC defines ‘personal data’ as:

“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;”

Article 2(b) broadly defines the ‘processing of data’ as:

“any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;”

4.4.4.2 Principles related to data quality

Directive 95/46/EC details five principles related to data quality (Article 6).

(a) Fair and Legal - Personal data must be “processed fairly and lawfully”

(b) Purpose-Limited - Personal data must be “collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes....”

(c) Relevant - Personal data must be “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed”

(d) Accurate - Personal data must be “accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data that are inaccurate or incomplete, having regard for the purposes for which they were collected or for which they are further processed, are erased or rectified.”
(e) **Time-Limited** - Personal data must be "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."

### 4.4.4.3 Criteria for legitimate data processing

Directive 95/46/EC also details criteria for making data processing legitimate (Article 7).

(a) **Consent** - Personal data may be processed when "the data subject has unambiguously given his consent." The Directive further specifies that consent must be both informed and voluntary.

(b) **Contract** - Personal data may be processed when "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."

(c) **Legal Obligations** - Personal data may be processed when "necessary for compliance with a legal obligation to which the controller is subject."

(d) **Vital Interests** - Personal data may be processed when "necessary in order to protect the vital interests of the data subject."

(e) **Public Interest** - Personal data may be processed when "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."

(f) **Legitimate Interests** - Personal data may be processed when "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(1)."

Directive 95/46/EC (Article 8) adds an additional layer of protection to personal data considered uniquely sensitive. Sensitive personal data includes "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."

The processing of sensitive personal data is prohibited except in a limited set of circumstances set out in Article 8 (2). Those circumstances exist where:

(a) a data subject has given explicit consent,
(b) processing is necessary for controller to meet legal obligations with respect to employment law,

(c) processing is necessary to protect the vital interests of a data subject (or another person), and the data subject is physically or legally incapable of giving consent

(d) processing is carried out by a non-profit organization whose aim is to advance an agenda related to one of the categories of sensitive data,

(e) the data are manifestly made public by the data subject,

(f) processing is necessary to establish or defend legal claims, and

(g) the processing is required by a health professional in the course of providing treatment or managing health-care services.

4.4.4.4 Rights of data subject

Directive 95/46/EC establishes that data subjects are to enjoy certain rights subject to some exemptions (e.g. given in Article 13). Some of these rights include:

Right of Access (Article 12a)

Data subjects have the right to obtain information regarding:

(a) whether their personal data is being processed,
(b) the content and source of any personal data undergoing processing, and
(c) the purpose of any such processing.

Right to Correct (Article 12b)

Data subjects have the right to correct, erase, or block the transfer of inaccurate or incomplete data.

Right to Object (Art 14)

Data subjects have the right to “object at any time on compelling legitimate grounds relating to [their] particular situation to the processing of data relating to [them], save where otherwise provided by national legislation.” Data subjects also have the right to object “to the processing of personal data relating to [them] which the controller anticipates being processed for the purposes of direct marketing.”

Right not to be subjected to solely automated decisions (Art 15)
Data subjects have a right not to be subjected to solely automated decisions to evaluate certain personal aspects such as his performance at work, creditworthiness, reliability and conduct.

**4.4.4.5 Obligations on Data Controllers**

**Notice to Data Subjects (Art 10)**

Except where a data subject already has such information, controllers must provide the data subject with the following information:

(a) the identity of the controller;
(b) the purpose of the processing;
(c) the recipients or “categories of recipients” of the data;
(d) whether providing information is obligatory or voluntary (including an explanation of the consequences of failure to provide the information); and
(e) the existence of the right to access and correct personal data.

**Notice to Data Protect Authorities (Arts 18 & 19)**

Except where national law provides an exemption, controllers must provide the relevant data protection authorities with the following information prior to performing any automatic processing operation:

(a) the name & address of the controller & any relevant representative
(b) the purpose(s) of the processing;
(c) a description of the category or categories of persons affected, and of the data relating to them;
(d) the recipients to whom the data may be disclosed;
(e) any proposed transfers to third countries; and
(f) a general description of measures taken to ensure the security of processing

**4.4.4.6 Transfers of personal data to third countries**

The Directive expressly prohibits the transfer of personal data to third (non-EU) countries except under limited circumstances. (Arts 25 & 26)

The exceptions to the general prohibition against transferring personal data outside of the EU fall into the following categories: country-specific, business-specific or circumstance-specific.
Country-specific exceptions: Art 25 of the Directive provides that the transfer of personal data may take place where “the third country in question ensures an adequate level of protection.” e.g. EEA countries. Also The EU and the US Department of Commerce reached an agreement in 2000 (The Safe Harbor agreement) that permits the transfer of personal data from the EU to organizations in the U.S. that publicly certify themselves to be a Safe Harbor.

Business Specific exceptions: (a) standard contractual clauses and (b) binding corporate rules.

Circumstance-Specific Exceptions: These include: Consent, Contract, Public Interest, to establish or defend legal claims, and to preserve vital interests of data subject.

4.4.1 Proposed EU Data Protection Directive for the Police

In 2012 a new legal framework for the processing of data in the police sector was proposed by the EU Commission’s proposal 25.1.2012 COM(2012) 10 final 2012/0010 (COD) 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”.

Since the original draft of the proposal there have been many amendments to the text, and at the time of writing the proposal is still undergoing changes. The version dated 2nd October 2015 is the most recent to date with an amendment to the title as follows: “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 or the safeguarding against and the prevention of threats to public security, and the free movement of such data.”

The proposed Directive is based on the principles of Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty of the Functioning of the European Union regarding the right of everyone to the protection of his/her personal data. Some of the main aspects are briefly discussed below.

4.4.1.1 Subject matter and Definitions

Article (1)(1) states that the Directive contains rules for the processing of personal data by competent authorities for the purposes of “the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security. “

The usual definitions of ‘personal data’ and ‘processing’ are the same as in other data protection laws and are given in Article 3.
4.4.1.2 Principles for data processing

The principles related to data processing are outlined in Article 4 namely: processing of data must be fair and lawful; collection/processing of data should be for a specific purpose (or compatible purposes); collected data should be adequate, relevant and non-excessive; data should be kept accurate and up to date; data should not be kept for longer than necessary; adequate data security should be present.

4.4.1.3 Transmission of personal data

Personal data that is inaccurate, incomplete or no longer up to date must not be transmitted or made available (Article 6).

If personal data is unlawfully transmitted or the data is incorrect then the recipient must be notified immediately. This data must then be rectified, erased or restricted (in accordance with Article 15).

4.4.1.4 Lawfulness of processing

Article 7 describes what constitutes lawful processing, namely: processing carried out under EU law or national law for the purposes set out in Article 1(1) i.e. “the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or the safeguarding against and the prevention of threats to public security.”

4.4.1.5 Processing of special categories of personal data

The processing of special categories of personal data (e.g. racial/ethnic origin, religion, political opinions, trade-union membership, genetic data, health data, sex life) is prohibited unless: it is necessary, subject to safeguards to protect the rights and freedoms of the data subject and only if (a) authorized by Union law or national law, or (b) done to protect the vital interests of the data subject or another person or (c) the data being processed has already been made public by the data subject, (Article 8).

4.4.1.6 Automated decision making including profiling

Decisions based solely on automated processing including profiling that either results in an adverse legal effect for the data subject or significantly affects the data subjects is prohibited unless authorized by union law or national law which provides appropriate safeguards regarding the rights and freedoms of the data subject (including at least the right for the data subject to have human intervention on the controller), (Article 9).

4.4.1.7 Rights of data subjects

Various subject rights, exemptions and provisions related to these rights are outlined in Articles 10 to 17. The extent of these rights is currently the subject of discussions among Member States. Article 10, sets out the communication and modalities for exercising the rights of the data subject. Controllers must take all reasonable steps to facilitate the exercise of data subject rights under Articles 12 and 15. Under Article
10(a) the following must be made available to a data subject: the identity and contact
details of the data controller; the purposes of the processing for which personal data is
intended; and the right to make a complaint to the supervisory authority.

The 2nd October 2015 version of the proposed Directive contains the following data
subject rights:

- Right of a data subject of access to data being processed about him/her and to
  obtain further information including: the purposes of such processing, to whom
  the data has been disclosed, and length of data storage among others (Article
  12). There are various limitations to the right to access. These are given in
  Article 13 and include:

  “(a) to avoid obstructing official or legal inquiries, investigations or
  procedures;
  (b) to avoid prejudicing the prevention, detection, investigation or prosecution
  of criminal offences or the execution of criminal penalties;
  (c) to safeguard public security;
  (d) to safeguard national security;
  (e) to safeguard the rights and freedoms of others.”

- Right to rectification, erasure and restriction of processing (Article 15);
- Right to be notified of any personal data breach (Article 29).

4.4.1.8 Data Protection by design and default

Appropriate technical and organisational measures based on current technology and
cost of implemented, should be implemented (appropriate to the processing activity
being carried out and its objectives) to meet the provisions of the Directive and protect
the rights of data subjects, (Article 19).

4.4.1.9 Records of personal data processing activities

Each data controller must maintain a record of all categories of personal data
processing activities under its responsibility, (Article 23).

4.4.1.10 Logging

In automated processing systems logs must be kept of the following processing
operations (unless impossible to do so or it involves a disproportionate effort):
collection, alteration, consultation disclosure, combination or erasure, (Article 24).

4.4.1.11 Security of data processing

Data controllers and processors must implement appropriate technical and
organizational measures to ensure a level of security appropriate to the risk (Article
27).
4.4.1.12 Notification of personal data protection breach to the supervisory authority

When a personal data breach occurs and it is likely to be of high risk to the rights and freedoms of data subjects, the controller must notify the supervisory authority not later than 72 hours after becoming aware of it. Where the notification is given later than 27 hours, reasons for doing so must be given, (Article 28).

4.4.1.13 Communication of personal data protection breach to the data subject

The controller must also inform the data subject (without undue delay) of any data breach that is likely to result in a high risk for his/her personal rights and freedoms, (Article 29).

4.5 Spain: Data Protection Legal Framework

4.5.1 Introduction

In Spain, data protection is a constitutional right, guaranteed by Article 18.4 of The Spanish Constitution of 1978 which states that:

"the law shall restrict the use of informatics in order to protect the honour and the personal and family privacy of Spanish citizens, as well as the full exercise of their rights"

In addition to Article 18.4 of The Spanish Constitution, the legal framework for data protection in Spain consists of:

- Organic Law 15/1999 on Personal Data Protection (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal)\(^{74}\). It repealed the existing data protection legislation (Constitutional Act 5/1992\(^{75}\)) and formally implemented the provisions of EU Directive 95/46/EC although Constitutional Act 5/1992 was largely consistent with the provisions of Directive 95/46/EC.

- Royal Decree 1720/2007 relating to Organic Law 15/1999 on Personal Data Protection\(^{76}\) which contains additional data protection regulations and security measures for data protection.

- Supplementary legal instruments (e.g. sectoral laws such as Law 34/2002\(^{77}\) and Law 9/2014\(^{78}\), orders and legal memorandums from the Spanish Data Protection Agency).

---

\(^{74}\) Organic Law 15/1999 on Personal Data Protection (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal or LOPD), http://www.legislationline.org/documents/id/9044

\(^{75}\) Constitutional Act 5/1992 of 29 October on the Regulation of the Automatic Processing of Personal Data.

D7.1 – Ethical and Legal Requirements


4.5.2 Organic Law 15/1999 and Royal Decree 1720/2007

Since SAMi2 will collect and process personal data in Spain, relevant aspects of Organic Law 15/1999 (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, thereafter referred to as LOPD) and Royal Decree 1720/2007 relating to Organic Law 15/1999 (thereafter referred to as DLOPD) will be discussed to give an understanding of the Spanish legal framework.

4.5.2.1 Scope

Spanish Data protection law regulates the processing of personal data in the public or private sector (LOPD Art 2(1)). This includes law enforcement. The law is aimed at:

- data controllers who process personal data in the context of activities of an establishment located in Spain:
- data controllers who are not established on Spanish soil but Spanish law is applicable under international public law; and
- data controllers who are not established in the EU but processes data with hardware located on Spanish soil (and not simply employed in transit).

According to LOPD Article 2(2) and DLOPD (Article 4), the law is not applicable to the following: personal databases; classified databases; terrorism and organized crime databases.

Where files are created for the purposes of terrorism and organized crime, the Spanish Data Protection Agency should be notified about the existence of these files and their characteristics and purpose.

The scope defined above means that the Spanish data protection law is not applicable where SAMi2 is used in the investigation of terrorism and organized crime.

4.5.2.2 Definitions

The following selected definitions are important in the context of this deliverable.

Personal data is defined under LOPD Article 3(a) as:

“any information relating to identified or identifiable natural persons”.

Further DLOPD Article 5(1)(f) states that “personal data shall mean any
numerical, alphabetical, photographic, acoustic or any other type of information relating to identified or identifiable natural persons".

Processing of personal data means (DLOPD Article 5(1)(t)):

“Any operation or technical process, whether automated or not, that allows the collection, recording, storage, creation, amendment, consultation, use, rectification, erasure, blocking or deletion, as well as the disclosure of data arising from communications, consultations, interconnections and transfers.”

A data controller is any (DLOPD Article 5.1(q)):

“natural person or legal entity, public or private, or administrative body, that alone or jointly with others decides on the purpose, content and use of the processing, although he does not effectively do it.”

A data subject is any (RLOPD Article 5(1)(a)):

“natural person to whom the data undergoing processing pertains.”

Consent from a data subject means (LOPD Article 3(h)):

“any freely given, specific, unequivocal and informed indication whereby the data subject signifies his agreement to the processing of his personal data.”

4.5.2.3 Data Protection Principles

Data controllers are required to comply with several general principles. Some relevant principles are discussed below.

- Data Quality
  - **Lawful basis for processing data**

    There must be a lawful basis for processing data.

    LOPD Article 4(1): “Personal data may be collected for processing, and undergo such processing, only if they are adequate, relevant and not excessive in relation to the scope and the specified, explicit and legitimate purposes for which they were obtained.”

    DLOPD Article 8(1): “Personal data must be processed fairly and lawfully. The collection of data by fraudulent, unfair or illicit means is hereby prohibited.”

  - **Purpose limitation**

    Data should be processed for specific (or compatible) purpose(s) for which it was collected.
LOPD Article 4(2): “Personal data subjected to processing may not be used for purposes incompatible with those for which they were collected. Further processing of the data for historical, statistical or scientific purposes shall not be considered incompatible.”

DLOPD Article 8(2): “Personal data may only be collected for specified, explicit and legitimate purposes of the data controller.”

DLOPD Article 8(3): “Personal data subjected to processing may not be used for purposes incompatible with those for which they were collected.”

- **Data minimization**

  The minimum necessary data required should be collected and kept.

  LOPD Article 4(4): “Personal data shall be accurate and updated in such a way as to give a true picture of the current situation of the data subject.”

  LOPD Article 4(5): “Personal data shall be erased when they have ceased to be necessary or relevant for the purpose for which they were obtained or recorded. They shall not be kept in a form which permits identification of the data subject for longer than necessary for the purposes for which they were obtained or recorded.”

  DLOPD Article 8(4): “Personal data may only be processed if they are adequate, relevant and not excessive in relation to the specific, explicit and legitimate purposes for which they were obtained.”

- **Proportionality**

  Data processed must be adequate, relevant and non-excessive in relation to the purposes for which they are collected.

  LOPD Article 4(5): as above

  DLOPD Article 8(4) as above.

- **Exercise of rights by data subjects**

  LOPD Article 4(6): “Personal data shall be stored in a way which permits the right of access to be exercised, unless lawfully erased.”

- **Transparency**

  - **Right for data subject to be informed when collecting data**
LOPD Article (5)(1): “Data subjects from who personal data are requested must previously be informed explicitly, precisely and unequivocally of the following:

a) The existence of a file or personal data processing operation, the purpose of collecting the data, and the recipients of the information.
b) The obligatory or voluntary nature of the reply to the questions put to them.
c) The consequences of obtaining the data or of refusing to provide them.
d) The possibility of exercising rights of access, rectification, erasure and objection.”

If data is not collected directly from a data subject then there is a requirement for the data subject to be informed, subject to certain circumstances as noted in LOPD Articles 5(4) and 5(5).

LOPD Article 5(4): “Where the personal data have not been obtained from the data subject, he must be informed explicitly, precisely and unequivocally by the controller or his representative within three months from the recording of the data – unless he has been informed previously – of the content of the processing, the origin of the data, and the information set out in (a), (d) and (e) of paragraph 1 of this Article.”

LOPD Article 5(5): “The provisions of the preceding paragraph shall not apply where explicitly provided for by law, when the processing is for historical, statistical or scientific purposes, or when it is not possible to inform the data subject, or where this would involve a disproportionate effort in the view of the Data Protection Agency or the corresponding regional body, in view of the number of data subjects, the age of the data and the possible compensatory measures.”

With regarding to the processing of personal data carried out in SAMi2, LOPD Article 5(5) above provided an exemption for subject notification since generally it may not be possible to contact people whose personal data may be included in the text of tweets. SAMi2 will automatically collect thousands of tweets and it will be impossible to distinguish personal data from non-personal data in unstructured texts. Also Data subjects' right to information during data collection (LOPD Article 5), is not applicable if informing data subjects will hinder or impair public authorities in their duties, or where the following is involved: national defence, public safety, the prosecution of criminal offences or misdemeanors (LOPD Article 24).

- **Consent of data subject**

LOPD Article (6)(1): “Processing of personal data shall require the unambiguous consent of the data subject, unless laid down otherwise by law.”
LOPD Article 6(1): “Consent shall not be required where the personal data are collected for the exercise of the functions proper to public administrations within the scope of their responsibilities.”

- **Exercise of rights by data subjects**

  LOPD Article 4(6): “Personal data shall be stored in a way which permits the right of access to be exercised, unless lawfully erased.”

- **Data with special protection**

  LOPD Article 7 details certain categories of data that need to be processed only with the explicit consent of the data subject. They include data relating to: ideology, political philosophy, trade union membership, religion, racial or ethnic origin, sex life and beliefs.

- **Security**

  LOPD Article 9(1) states that the controller (and processor) must take all necessary measures (technical and organizational) to: make sure that data is secure; prevent the alteration or loss of data; and the unauthorized processing or access to data. This must be done in the context of the state of the art of the technology, the nature of the data stored, and the risks (whether human action or physical or natural causes) to which the data is exposed.

  LOPD Title VIII addresses several provisions regarding security measures in the processing of personal data.

- **Secrecy**

  LOPD Article 10: “The controller and any persons involved in any stage of processing personal data shall be subject to professional secrecy as regards such data and to the duty to keep them. These obligations shall continue even after the end of the relations with the owner of the file or, where applicable, the person responsible for it.”

- **Data disclosure**

  LOPD Article 11(1): “Personal data subjected to processing may be communicated to third persons only for purposes directly related to the legitimate functions of the transferor and transferee with the prior consent of the data subject.”

  LOPD Article 11(2) gives several exemptions to the consent required in LOPD Article (1) including “when the data were collected from publicly accessible sources.”

---

79 LOPD Article 6(1) gives several conditions where consent of a data subject is not required.
• **Access to data by third parties**

  LOPD Article 12: details the requirements for third party access to data.

### 4.5.2.4 Rights of data subjects

Data subjects have certain rights under law related to the processing of their personal data including the following:

- Right to object to assessments or acts/decisions, made based solely on data protection procedures, intended to evaluate personality or behavioural aspects (LOPD Article 13).

- Right to consult the General Data Protection Register to verify that records of their personal data, purpose for their collection and identity of controller (LOPD Article 14).

- Right of access to information about personal data – how it was obtained, has been or is being used and/or communicated to third parties (LOPD Article 15, DLOPD Article 27).

- Right of rectification and erasure of personal data that is inaccurate, incomplete or processed in violation of data protection law (LOPD Article 16, DLOPD Article 31).

- Right to object to certain kinds of processing: where consent is not required but there are legitimate grounds relating to personal circumstances; for advertising and direct marketing; to make decisions based solely on automatic processing of personal data. (DLOPD Article 34, Article 36).

- Right to Indemnity/compensation for loss suffered due to violations of data protection law (LOPD Article 19).

Public authorities (including law enforcement) can deny subject rights to access, rectification and erasure based on the following reasons (LOPD Article 23): risks to state security, protection of third party rights/freedoms, and the protection of an ongoing investigation. Any denial of subject rights must be reported to the Data Protection Agency or competent regional body to make sure that the denial is justified.

### 4.5.2.5 Public Sector Files

The law (under Title IV, Sectoral Provisions) contains special provisions for data processing in the public sector which will include law enforcement and the activities of SAMi2. Some important aspects of the provisions relevant to SAMi2 are discussed below.

**Registration**
Public authorities are required to undergo registration of their files (databases) in the Official State Journal or analogous regional publication, before processing data (LOPD Article 20). A registration must contain a description of: the purpose of the database and its intended use; persons or groups whose personal data will be gathered; how personal data will be gathered; the structure of the database; any surrender of personal data and planned transfer of personal data to third countries; public bodies responsible for the database; how subjects’ rights will be addressed; and security specification (low, medium or high level).

**Data disclosure between public authorities**

LOPD (Article 21) prohibits disclosure of personal between public authorities to perform duties of a different nature or relating to different matters, except this is allowed by other legislation, or whether data are discloses for processing related to historical, statistical or scientific purposes.

**Files kept by law enforcement**

LOPD Article 22(2) limits the scope of personal data collection by the law enforcement where there is no consent from the data subject. This scope is limited to data required to safeguard public safety and prevent crime. Further the data must be stored in specific files established for this purpose and classified according to the degree of their reliability.

Specially protected data described under LOPD Article 7 (i.e. data relating to ideology, political philosophy, trade union membership, religion and beliefs) can be collected and processed by law enforcement only when absolutely necessary for investigations, (LOPD Article 22(2)).

LOPD Article 22(4) mandates that personal data collected for law enforcement purposes should only be kept for as long as necessary and then erased.

**Exceptions to the rights to access, rectification and erasure.**

Law enforcement can deny subject rights to access, rectification and erasure based on the following reasons LOPD Article 23: risks to state security, protection of third party rights/freedoms, and the protection of an ongoing investigation. Any denial of subject rights must be reported to the Direct of the Data Protection Agency or competent regional body.

**Other exception to subjects’ rights**

Data subjects’ right to information during data collection (LOPD Article 5), is not applicable if informing data subjects will hinder or impair public authorities in their duties, or where the following is involved: national defense, public safety, the prosecution of criminal offences or misdemeanors (LOPD Article 24).
4.5.2.6 Private Sector files

LOPD Articles 25 to 32 detail special provisions for data processing in the private sector. Since SAMi2 will be used by law enforcement and other public authorities (e.g. security services) these articles will not be discussed in detail in this deliverable.

4.5.2.7 Infringements and penalties

Infringement of data protection laws will involved various penalties. LOPD Articles 46 to 48 outline types of infringement, procedures and penalties related to public authorities.

4.6 Spain: Investigating Terrorism

One of the use cases of SAMi2 focuses on the detection of terrorism related activities on Twitter. It is therefore necessary to briefly examine some aspects of the legal framework for terrorism in Spain, especially with regard to law enforcement powers when investigating terrorism since the Spanish Data Protection legal framework does not apply to the investigation of terrorism related activities (LOPD, Article 2(2) and DLOPD, Article 4).

Spanish authorities have had a long history of combating terrorism in Spain. Since the 1960s until a ceasefire in October 2011, *Euskadi Ta Askatasuna* (ETA - Basque Fatherland and Liberty) have waged a violent campaign (including terrorist acts) in Spain intended to establish a separate Basque state. Spanish authorities have used a number of measures including anti-terrorism legislation and the criminal law to combat terrorism. Spain has also actively supported two important UN Security Council resolutions aimed at combating terrorism adopted after the 9/11 US attacks. Security Council Resolution 1373 on September 2001 mandated all UN member states to adopt specific measures to combat terrorism and created the Counter Terrorism Committee (CTC) which monitor states’ compliance. A later Security Council Resolution 1456 in January 2003 mandated that UN member states comply with their obligations under international law (including human rights, refugee and humanitarian law) when undertaking any measure to combat terrorism. In an interview with Human

---


Rights Watch on July 12 2004, Spanish Attorney Cándido Conde-Pumpido affirmed Spain’s commitment to an antiterrorism approach based on the rule of law.84

When terrorist groups are being investigated, the Spanish Constitution85 (Article 55(2)) allows for the suspension of certain individual rights namely: Article 17 (the restriction on time limits for detention); and Article 18 subsection 2 (sanctity/privacy of the home) and subsection 3 (secrecy/privacy of communications). These suspensions are not automatically applied but are implemented via various legal instruments, for example, the suspension of the right to privacy of communications must be authorised via a court order or in emergency circumstances by the Minister of the Interior or if not available, the Secretary of State (see Article 579, Code of Criminal Procedure86). Terrorist groups are defined in the Spanish Criminal Code (Código Penal87) and the powers of law enforcement and judicial authorities with regard to investigating terrorism, and the right of terrorist are detailed in the Code of Criminal Procedure (Ley de Enjuiciamiento Criminal, LEC).

The scope of this deliverable does not include discussing the Spanish legal framework for terrorism in detail. This deliverable, however, seeks to inform end users of the SAMI2 system that the Spanish data protection legal framework does not apply when investigating terrorist activities although the Data Protection Authority needs to be informed of the presence of any files created related to terrorism investigations.

85 Spanish Constitution http://www.congreso.es/portal/page/portal/Congreso/Congreso/Hist_Normas/Norm/const_espa_texto_ingles_0.pdf
86 Criminal Procedure Act (Spain) - Ley de Enjuiciamiento Criminal http://www.ela.eu/wp-content/uploads/file/Civil_Procedure_Act_%28Ley_de_Enjuiciamiento_Civil%29%5B1%5D.pdf