SEVENTH FRAMEWORK PROGRAMME

Networked Media

Specific Targeted Research Project

SMART

(FP7-287583)

Search engine for MultimediA environment generated contenT

D7.7 Data Protection Protocol

Due date of deliverable: 30-01-2012

Actual submission date: 21-05-2012

Start date of project: 01-11-2011 Duration: 36 months

Summary of the document

Code:	**D7.7 Data Protection Protocol**
Last modification: **State:**	18/05/2012 Final
Participant Partner(s): **Author(s):** **Fragment:**	ATOS, AIT Daniel Field, Irene Schmidt, John Soldatos, Paul Moore NO
Audience:	☒ public ☐ restricted ☐ internal
Abstract:	*This a document designed to (a) demonstrate to project management and chain of oversight that the project is aware of, and compliant with, the necessary laws and regulations covering data protection; and (b) to inform and educate project participants on their obligations and responsibilities when in contact with personal data. It therefore sets out the rules which the project must comply with.*
Keywords:	• *Data Protection*
References:	D7.8; DPA, DoW

Table of Contents

1 Executive Summary 4
2 Introduction....6
3 Ethical and Legal Implications of SMART Data Collection and Storage....6
3.1 Ethical issues 6
3.2 Applicable Law and Regulations....7
3.2.1 European Convention of Human Rights and Fundamental Freedoms....7
3.2.2 The Charter of Fundamental Rights of the EU 8
3.2.3 Data Protection Directive 95/46/EC 8
3.2.4 Privacy and Electronic Communications Directive 2002/58/EC 11
3.2.5 Spanish law.... 11
3.2.6 Applicable areas of European and Spanish Data protection laws regarding personal data 11
4 SMART Compliance.... 16
4.1 Permission from the Data Protection Agency 16
4.2 Measures for Secure Storage 16
4.3 Measures for Privacy Protection 17
4.4 Other measures 17
5 Conclusions.... 18
6 BIBLIOGRAPHY AND REFERENCES 19
7 ANNEXES 20
7.1 DPA (Spanish) 20

1 Executive Summary

Deliverable D7.7 (Data Protection Protocol) is a document designed to (a) demonstrate to project management and chain of oversight that the project is aware of, and compliant with, the necessary laws and regulations covering data protection; and (b) to inform and educate project participants on their obligations and responsibilities when in contact with personal data. It therefore sets out the rules which the project must comply with.

A number of ethical issues are raised within SMART by the nature of gathering personal and public data on volunteers and bystanders. Because the project involves the tracking the location and observation of people, fundamental rights and privacy are key ethical issues. In particular this is relevant for the two categories of data subjects: volunteers and bystanders. In the case of the former, a voluntary consent form is required and with this consent, a greater deal of data collection, storage and processing is permitted, including the use of these results in the project work. In the case of bystanders, the rules are more stringent and efforts must be taken to render anonymous the data collected, as well as reasonable efforts made to inform bystanders of the data collection in process. Note that children are not involved at any stage of SMART.

Furthermore the right to privacy, the fundamental rights to be safeguarded during the project are: Freedom of expression; Freedom of information; Freedom of assembly and Dignity. These rights are enshrined in the constitutions of some member states as well as the European Convention of Human Rights and Fundamental Freedoms and the Charter of Fundamental Rights of the EU. However it is in most cases through the Data Protection Directive 95/46/EC (extended through the Privacy and Electronic Communications Directive 2002/58/EC) which these rights are protected through legislation. More precisely these rights are protected by each member state through the legislation of that state which, as a minimum, must comply with the above directives.

The main thrust of the 95/46/EC directive is:

- The right of access to own personal data.
- The rights of erasure, blocking or rectification of the data, which do not comply with the provisions of the Directive, are incomplete or inaccurate.
- The right to be informed of all relevant details relating to the data processing and the rights granted to self.
- The right to a judicial remedy for any breach of the above mentioned rights

Three important definitions arise from the directive, hereafter also referred to as the data protection directive (DPD):

- Data subject: the individual who is the subject of the personal data.
- Data controller: a person (natural or legal) who alone or jointly with others “determines the purposes and means of the processing of personal data” (Art. 2(d) DPD).
- Data processor: a third party who simply processes personal data on behalf of the data controller without controlling the contents or making use of the data (Art. 2(e) DPD).

Within Spain, the member state of principle interest due to the location of the field trials, the issue of data protection is enshrined by Organic Law 5/1992 on the Regulation of the Automatic Processing of Personal Data. Law 5/1992 was subsequently amended by Organic Law 15/1999 on the Protection of Personal Data. Organic Law 15/1999 implemented Directive 95/46/EC into Spanish law.

In addition to the set of basic obligations of this directive, as mentioned above, either due to the nature of SMART or of specific Spanish law, there are further relevant issues. These are those relating to ‘sensitive’ data, the right of access to date, the obligation to inform data subjects, the right of obligation and ability to move data across national borders.

In SMART a series of measures will be taken to ensure that the regulations are followed: Data will be stored on secure systems where unauthorised access (electronically or physically) will be prevented. Copies will be made to ensure accurate and complete data records in the case of data destruction. The data will be stored for a specific purpose and stored only for that purpose. When that purpose has expired, for instance after the conclusion of the project, that data will be erased. All data will be stored in a data file format compatible with the law. No SMART application will be permitted to use real data until the required security level has been

achieved.

To ensure privacy volunteers participating in SMART will have provided informed consent prior to the trial and will be made aware of how their personal data will be used, the purpose of the data collection and their rights with respect to that personal data. SMART will notify bystanders of public and private spaces employed in all data collections and testing of the monitoring system. This will be implemented by posting a notice visible from all access points to the employed area. Data involving bystanders will be rendered anonymous and destroyed when the relevant research task is complete.

SMART will make a point of contact available for any volunteers who wish to withdraw from the tests, to access, correct or erase their data or to object to the data processing, and similar measures will be provided for bystanders.

In conclusion it has been shown that the SMART project has carried out due diligence in identifying the relevant laws and legislation applicable to the project. SMART has decided on a number of measures, relating to the way data is stored and processed, and in interacting with bystanders and volunteers which will be carried out to ensure no breach of the law.

2 Introduction

This document exists to describe the necessary activities and controls in place within the SMART project to comply with data protection at the European level and, as data is collected in Spain, Spanish data protection law.

As such it both serves to demonstrate that the project is aware of and compliant with applicable law, and serves as a set of guidelines by which all members of the project in contact with personal data must follow.

The document is set out in seven chapters. Sections 1 (executive summary) and 2 (introduction) introduce the document. Section three introduces the ethical issues relevant to the project (although this is covered in greater depth in companion deliverable D7.8 (Ethical Dimensions of SMART Technologies) and then proceeds to describe the necessary laws and regulations which apply to data protection. This section serves two purposes: it provides an overview of this regulation to orient the reader to further investigation on this matter, and secondly extracts from these sources the most salient points for the project SMART, without, of course, limiting the obligations of the project or its participants merely to these sections. Section five describes the specific measures which will be taken in the SMART project to comply with the current legislation, including DPA approval, and finally, section six concludes the report.

3 Ethical and Legal Implications of SMART Data Collection and Storage

3.1 Ethical issues

The principal ethical issues in SMART are the protection of fundamental rights and privacy. This is because the project involves the tracking the location and observation of people. These rights are covered by European and national laws and regulations which will be followed in SMART. Further details are provided in deliverable D7.8 (Ethical Dimensions of SMART Technologies) and are merely touched on here to provide context for the relevance of the laws and regulations covered in the following section.

The two categories of third parties whose rights and privacy must be protected in relation to field testing are i) volunteers and ii) bystanders.

i) Voluntary participants are people selected by the project (with assigned “token role” or a greater role in the unfolding of a scenario). They will have provided informed consent for their information to be used in the project prior to involvement. An ethical panel will approve their involvement during the selection process. Under no circumstances will vulnerable subjects be selected as a SMART actor; this includes persons under the age of 18 and any other person unable to give the informed consent.

ii) In the case of bystanders, they will be informed that data is being collected and monitored in any private or public space before entering into it and all data will be rendered anonymous (blurring of faces, etc.) before any public disclosure.

Children will not be involved at any stage.

The ethical issues surrounding these fundamental rights and privacy issues are:

- The right of access to own personal data.
- The rights of erasure, blocking or rectification of the data, which do not comply with the provisions of the Directive, are incomplete or inaccurate.
- The right to be informed of all relevant details relating to the data processing and the rights granted to self.
- The right to a judicial remedy for any breach of the above mentioned rights.
- Privacy
- Fundamental rights:

- Freedom of expression
- Freedom of information
- Freedom of assembly
- Dignity

And particularly within the context of the SMART project, specifically the following issues may arise:

- Personally identifiable data
- Crowd reaction
- Social conversations
- Location tracking
- Consent for pictures and videos
- Suspicious behaviour
- Stored modelling
- Acoustics, audio (interception)
- Elements in speech
- Biometrics
- False positives
- Unusual movements
- Activation of acoustic sensors
- Automated rating

3.2 Applicable Law and Regulations

3.2.1 European Convention of Human Rights and Fundamental Freedoms

The European Convention of Human Rights and Fundamental Freedoms sets out, among other issues, several basic freedoms including: the right to privacy and the right to freedom of expression.

The fundamental right to privacy is recognized in Article 8, which stipulates that everyone has the right to respect for his or her private and family life, home and correspondence:

> *"Right to respect for private and family life*
>
> *1. Everyone has the right to respect for his or her private and family life, his or her home and his or her 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 well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

The European Union requires all member states to legislate to ensure that citizens have a right to privacy, through directives such as the 1995 Directive 95/46/EC on the protection of personal data.

With the advent of new technologies, however, the notion of correspondence has acquired a wider perspective and it has come to contain, in addition to its traditional meaning, any type of point-to-point communication realised through an electronic communications network.

Article 10 covers freedom of expression;

> *"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
>
> *2. The exercise of these freedoms, since it carries with it duties and responsibilities, may*

be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."[1]

3.2.2 The Charter of Fundamental Rights of the EU

The Charter of Fundamental Rights in the course of the respective legal trend dedicates a separate article to the protection of personal data. Article 8 sets out the right to the protection of personal data of an individual and thus the protection of personal data has now its own legal basis apart from the right to respect an individual's private life and the protection of human dignity. Article 8 of the Charter sets out the rules for the legitimate processing of personal data, notably that the processing shall be fair and for pre-specified purposes based on the consent of the data subject or other legitimate basis laid down by law. Reference is furthermore made to two rights of the data subject: the right of access to the data and the right to have it rectified. Finally, Article 8 sets out the need for an independent authority, which shall control the compliance with the data protection rules. Article 11 also protects the right of free expression:

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected."

Other fundamental rights covered in the charter and convention include the right to freedom of information, the right to free assembly and the right to dignity.

3.2.3 Data Protection Directive 95/46/EC

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data lays down a series of rights of the data subject. These are:

- The right of access to own personal data.
- The rights of erasure, blocking or rectification of the data, which do not comply with the provisions of the Directive, are incomplete or inaccurate.
- The right to be informed of all relevant details relating to the data processing and the rights granted to self.
- The right to a judicial remedy for any breach of the above mentioned rights.

All these are applicable to SMART. The first three aforementioned rights may be restricted if this is necessary for reasons relating to the protection of the data subject or the rights and freedoms of others or to prevent a criminal offence or for reasons relating to public security.

The Data Protection Directive (DPD) aims to lay down specific rights of the individual on his or her personal data, while ensuring that such data can move freely within the single market created between the Member States of the European Union. It further aims to harmonize the data protection rules within the European Union.

Article 2(a) of the Data Protection Directive (DPD) 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 or her physical, physiological, mental economic, cultural or social identity". Although the Data Protection Directive tried to harmonise the processing of personal data with the free movement of such data, there are still many differences between the Member States with regard to the term 'personal data', and especially when it refers to an 'identified of identifiable natural person'.

According to Article 2 (b) of the DPD, "data processing" is defined as "any operation or set of operations

[1] http://en.wikipedia.org/wiki/Article_10_of_the_European_Convention_on_Human_Rights, Retrieved 06/03/2012

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". It follows that the definition of processing is extraordinarily broad, which means that it is difficult to conceive any operation performed on personal data which would not be covered by it. It is important to note that mere storage of personal data by the providers of publicly available electronic communications services or of a public communications network constitutes 'data processing', so that simply storing data on a server or other media is deemed to be processing, even if nothing else is being done with it.

In the context of processing of personal data, three distinctive categories of parties are recognised:

- Data subject: the individual who is the subject of the personal data.
- Data controller: a person (natural or legal) who alone or jointly with others "determines the purposes and means of the processing of personal data" (Art. 2(d) DPD).
- Data processor: a third party who simply processes personal data on behalf of the data controller without controlling the contents or making use of the data (Art. 2(e) DPD).

Under the regime established by the Data Protection Directive, a key concept is that of the 'data subject's consent'. If the data controller obtains the data subject's consent, then he or she is broadly free to process the personal data. The Directive states that a 'data subjects' consent' must be freely given, specific and informed (Art. 2 (h) DPD).

Article 8 of the DPD describes special categories of data, i.e., "personal 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", commonly known as sensitive data. The processing of the aforementioned data is prohibited, unless one of the specific grounds described in the same Article is fulfilled.

There are a number of exceptions:

- The interested person has given his or her consent
- The processing is necessary for vital security interests of the other person who would be physically or legally incapable to give his or her consent
- The processing is effected with administrative purpose, under the responsibility of persons pursuing legal activities, with a political, philosophical, religious character as well as by trade unions. The files are constituted to collect information about their members. The information may not be communicated to third parties.
- The processing is used for journalistic purposes (freedom of expression), for the creation of literary or artistic works.
- In health issues, exceptions have been accepted in the interest of the patient or in the field of preventative medicine, the medical diagnostics, and medical treatment. The processing of data is being effected by a heath practitioner who is bound by his or her professional oath or by another person under the professional oath.
- The processing of data concerning criminal offences, sentences and measures of security (preventive retention) can only be effected under the control of public authority. Particularly, a collection of all penal condemnations can only be established under the control of a public organ.

The person concerned has to be granted an access right to his or her personal data. She can make changes or delete the data that are incomplete or incorrect. She has also a right to oppose to the storage of data for legitimate reasons with regard to his or her particular situation. The Directive uses the words "justified opposition". It leaves a margin of evaluation to national authorities as to the storage of data.

Moreover, all the actors recognise that security is a condition for freedom. The entity responsible for the processing uses technical measurers and adequate organisation to avoid destruction or accidental loss, alteration, diffusion or non-authorised access. The security level is chosen with respect to the risk incurred in the procedure of data processing. If a subcontractor is chosen by the persons or company responsible for the treatment, he has to bring sufficient guarantees: like all subcontractor, he can act only according to instruction by the persons or company responsible of the treatment.

With the international data exchange, a principle of reciprocity as to the protection of personal data is aimed at:

> *"The Member States shall provide that the transfer to a third country of personal data which are under-going processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection."*

3.2.3.1 Basic principles in data processing

The European legal framework on data protection contains some basic principles for the processing of personal data. These principles serve as good practices that data controllers should comply with in order to protect the data they hold. The first of these principles requires fair and lawful processing (Art. 6(a) DPD). In determining whether any processing of personal data is 'fair', particular regard must be paid to the method by which data were obtained. Under the second principle, data controllers must obtain data only for specified and legitimate purposes, and must not carry out any further processing which is incompatible with those purposes (Art. 6(b) DPD). This principle thus has two components: (1) the data controller must specifically inform the data subject of the purposes for which data has been collected; and (2) once data has been properly collected, it must not be used for further purposes incompatible with the original purposes. The third principle requires a data controller to hold only personal data that is "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (Art. 6(dc) DPD). Data controllers are therefore obliged to store only a bare minimum of data that will suffice for the running of their services.

The fourth principle stipulates that all personal data "shall be accurate and, where necessary, kept up to date" (Art. 6(d) DPD). The specific legislative provision creates an obligation for the data controllers to take every reasonable step to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected, are either erased or rectified. In practice, a data subject is likely to complain of a breach of this principle in cases where there has been some detriment to the individual as the result of the information being incorrect. It is therefore advised that the data controllers set up a mechanism whereby the data subjects are able to update their personal data or notify the data controller about the inaccuracies of the present information. This mechanism could be set up either within the network platform (by using the network's interface), or outside the platform (e.g. by the use of a 'hotline'). The fifth principle reads that personal data must not be kept for longer than what is necessary for the purposes for which this data were collected (Art. 6(e) DPD). This implies that data should be destroyed or rendered anonymous when the specified purpose for which they were collected has been achieved. The sixth principle requires processing to be carried out in accordance with the rights of the data subjects. More precisely, Article 12 of the DPD grants data subjects the right to obtain certain basic information from the data controller about the processing of their personal data.

The seventh principle addresses the issue of data security: it requires data controllers to take 'appropriate technical and organizational measures' (Art. 17.1 DPD) against unauthorized or unlawful processing, and accidental loss, destruction or damage to the data. This principle covers the security requirements and robustness of the network itself, taken as a whole this principle imposes a statutory obligation on data controllers to ensure that personal data are processed in a secure environment. This means that the data controllers must consider the state of technological development and the cost of the implementation of any security measures. Finally, the last principle is the notification to the supervisory authority in order to ensure the supervision of the data processing. The data controller must notify (Art. 18,19 DPD) the supervisory authority about the processing, an mention among other matters the name of the controller, the purpose of the processing, the categories of data subjects, the categories of data processed, as well as the recipients to whom the data might be disclosed.

The Data Protection Directive also contains a liability provision. Pursuant to Article 23, any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national data protection legislation is entitled to compensation from the controller for the damage suffered. The controller may be exempted from liability, in whole or in part, if he or she proves that he or she is not responsible for the event giving rise to the damage.

Since 1995 the Data Protection Directive has been complemented by other Directives such as in the ePrivacy Directive from 2002. This Directive translates the data protection principles of the general Data Protection Directive into specific rules for the electronic communications sector, regardless of the medium used. This directive regulates issues such as the confidentiality of communications, the status of traffic and location data, itemised billing, and unsolicited communications. It is applicable for example to electronic communication services providers; mobile communication services providers, etc.

3.2.4 Privacy and Electronic Communications Directive 2002/58/EC

The Privacy and Electronic Communications Directive (2002/58/EC) translates the data protection principles of the general Data Protection Directive into specific rules for the electronic communications sector, regardless of the medium used. This directive regulates issues such as the confidentiality of communications, the status of traffic and location data, itemized billing, and unsolicited communications. It is applicable for example to electronic communication services providers; mobile communication services providers, etc.

3.2.5 Spanish law

As the field trials and data collection will occur in Spain, SMART must also comply with these national laws.

In Spain, article 18 of the Spanish constitution (1978) establishes that:

> *"(1) The right of honour, personal, and family privacy and identity is guaranteed.*
>
> *(2) The home is inviolable. No entry or search may be made without legal authority except with the express consent of the owners or in the case of a flagrante delicto.*
>
> *(3) Secrecy of communications, particularly regarding postal, telegraphic, and telephone communication, is guaranteed, except for infractions by judicial order.*
>
> *(4) The law shall limit the use of information, to guarantee personal and family honour, the privacy of citizens, and the full exercise of their rights."*[2]

Provision 4, which enshrines the issue of data protection, was further developed by Organic Law 5/1992 on the Regulation of the Automatic Processing of Personal Data. The Spanish Data Protection Agency was formally created by Royal Decree 428/1993 of 26 March.

Law 5/1992 was subsequently amended by Organic Law 15/1999 on the Protection of Personal Data. Organic Law 15/1999 implemented Directive 95/46/EC into Spanish law.

3.2.6 Applicable areas of European and Spanish Data protection laws regarding personal data

The above paragraphs discuss the specific laws and regulations which apply to the project. The conscientious reader is referred to these documents for the complete text. However, for the benefit of the reader, the key points which apply in the SMART project is hereby given, in part abridged from an excellent analysis Douwe Korff (consultant to the European Commission)[3]

As has been discussed elsewhere, Member States shall provide that personal data may be processed only if the data subject has unambiguously given his consent. There exist exceptions; however these are not applicable to SMART.

Furthermore:

3.2.6.1 'Special' or 'sensitive' data

In addition to personal data, there is also a series of categories considered to be "special".

[2] http://www.servat.unibe.ch/icl/sp00000_.html, Retrieved 06/03/2012

[3] Korff, D., Comparative Summary Of National Laws: EC STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE (Study Contract ETD/2001/B5-3001/A/49). September 2002

Art. 8(1) of the Directive 95/46/EC refers to 'Special categories of data': "personal 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."

Most of the laws of the Member States regard the same categories of data as "special" or "sensitive" as are listed in Art. 8(1) of the Directive, quoted above and the Spanish law too is very close to the Directive by applying "special protection" to data which "reveal" "ideology, trade-union membership, religion or belief", or which "refer to" racial origin, health or sex life.

However there are some exceptions:

"1. Member States shall prohibit the processing of personal 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.

2. Paragraph 1 shall not apply where:

*(a) **the data subject has given his explicit consent** to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or*

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that' the data are not disclosed to a third party without the consent of the data subjects; or

*(e) **the processing relates to data which are manifestly made public by the data subject** or is necessary for the establishment, exercise or defence of legal claims."*

(Art. 8(2) of the Directive)

"The Spanish law re-affirms a constitutional stipulation that no-one may be forced to reveal his religion or beliefs (and adds that individuals must be advised of this if they are asked for such information); and stipulates (also because of constitutional imperatives) that the creation of files solely for the purpose of listing the "ideology, trade-union membership, religion, beliefs, racial or ethnic origin or sex life" of individuals "remains prohibited."

In the case of SMART this means that the any data entering into either definition of 'sensitive' or 'special' cannot be collected from bystanders, that the volunteer consent form must explicitly state which, if any, of these types of data will be collected, and that SMART must not create any files solely for the purpose of collecting this data.

The SMART sensor based technologies to not reveal any of the characteristics above. However, third party contributors (i.e. the OS community) must be made aware of this. Any video or sound recordings must be kept away from places of worship or trade union offices and no record of conversation discussing these matters kept.

However, the case of Twitter and other social media, the privacy of the individual is covered by the social

network, although we can make the distinction of filter that raise no-privacy issues and filters where such privacy issues can emerge. It is additionally arguable that Twitter and the public pages of social media are covered under exception (e), as the participant will be considered to have manifestly made this data public.

Besides it is not the intention of SMART to collect such data per se, any collection of this data will be through a side effect of wider data collection (for example recording a conversation which happens to cover these subjects as part of a wider recording remit). This means that it is improbable that specific Spanish constraint is breached.

3.2.6.2 Informing of data subjects

> *"Article 10:*
>
> *Information in cases of collection of data from the data subject Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:*
>
> *(a) the identity of the controller and of his representative, if any;*
>
> *(b) the purposes of the processing for which the data are intended;*
>
> *(c) any further information such as*
>
> *• the recipients or categories of recipients of the data,*
>
> *• whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,*
>
> *• the existence of the right of access to and the right to rectify the data concerning him –*
>
> *in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.*
>
> *The Member States have implemented the above provision (and its companion one, Art. 11, discussed in the next sub-section) quite differently. Some stay quite close to the Directive, while others divert considerably from it.*
>
> *The Spanish law too requires that all the additional information must always be given, unless this is obvious - which is stricter than the Directive - and in addition stipulates that the data subjects must be informed of the actual recipients of the data (rather than just the categories of recipients) and of the fact that the data are to be held in a (structured) filing system or automatically processed.*
>
> *As far as the timing of the information is concerned, there are similar divergences. Spain demands that the information be provided "when the data are collected", or "before the data are provided [by the data subject to the controller]", or "beforehand" or "at the latest when the data are obtained""*

Thus in the case of SMART it is clear that the volunteer consent form must contain the information in (a), (b) and (c), above. Going further the recipients of the data must be explicitly mentioned. We will do this with very clear and narrow descriptions of the groups of actors (project officer, reviewers and so on).Similarly the notice to bystanders must make provision for this information to be available before or during data collection.

3.2.6.3 Informing when data are collected otherwise

> *"Article 11:*
>
> *Information where the data have not been obtained from the data subject*
>
> *1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of per-*

sonal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as

- *the categories of data concerned,*
- *the recipients or categories of recipients,*
- *the existence of the right of access to and the right to rectify the data concerning him –*

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

*2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or **scientific research**, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.*

The laws of the Member States also differ in respect of the information that must be provided to data subjects when data on them are obtained other than from the data subjects themselves. Again, some stay quite close to the Directive, some qualify the requirements of the Directive in terms seemingly at odds with the Directive, and yet others go beyond the requirements of that instrument.

Spain [is]: again more demanding, in the same way as discussed in the previous subsection, by requiring that all the information be always provided"

In the case of SMART this may apply to bystanders and is related to the comment made in the previous subsection.

3.2.6.4 Right of Access

"Article 12: Right of access

Member States shall guarantee every data right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- *confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,*
- *communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,*
- *knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred .to in Article 15 (1);*

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

The laws in all the Member States provide for the right of data subjects to receive confirmation, on request, of whether data on them are processed by a particular controller

The most important formal difference in the laws is that some countries - Greece, Spain and Sweden - require controllers always to inform data subjects, on request, of the sources of the data - and not just of "any available information" as to these source[s].

All the Member States except Spain in principle give data subjects the right to obtain a copy of the data The Spanish law provides for this alternative too, but without stipulating that if the data subject wants he can demand a hard copy rather than mere access"

In the context of SMART this means that the project must be able to give any data subject requesting this information on the terms described above, as well as the sources of this data and a copy of the data itself.

3.2.6.5 The general right to object

"Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f),72 to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.

By contrast, the laws in Finland, Spain and Sweden do NOT contain provide for a general right to object - or at least not explicitly

As far as Spain is concerned, the absence of the general right to object can be explained by the fact that the two criteria to which it must relate according to the Directive are severely restricted in the law in the first place."

In SMART this means that a data subject has the right to withdraw from the scheme and/or object to any further processing of their data.

3.2.6.6 Rules and procedures relating to intra-EU transfers

"Member States shall neither restrict nor prohibit the free flow of personal data between

Member States for reasons connected with [data protection]." (Art. 1(2) of the Directive)"

"One of the main aims (indeed, perhaps, strictly speaking the main aim) of the Directive is to remove obstacles to the Single Market arising out of restrictions imposed by data protection laws on cross-border data transfers. The Directive seeks to ensure a high level of data protection so that those obstacles can be removed. Having done so, it can therefore lay down the principle of a "free zone" for data transfers throughout the European Community, as is done in the above-quoted provision. However, like all the other provisions in the Directive, this stipulation too of course only applies to matters within its own scope (that is, broadly speaking, to matters within the scope of Community law). Indeed, a similar freedom cannot be stipulated in such an unconditional way for matters outside the scope of the Directive, because there is no guarantee that in such matters the same high level of protection is guaranteed. The two things hang together: freedom to transfer data where there is protection; no such freedom where this is not guaranteed."

In the context of SMART this means that there should not be any problem in principle for the consortium partners in different nation states from receiving and processing the data in accordance with the description of work and the ethical and data protection norms of the project.

4 SMART Compliance

4.1 Permission from the Data Protection Agency

Due to the public nature of the A/V SMART sensors (cameras and microphones) and privacy issues, it was necessary to apply to the Spanish Data Protection Agency for permission (original response from the DPA is added to the Annexes). The first submission was rejected because it was not sufficiently clear that persons would not be identifiable in the video streams. Therefore a resubmission is being prepared where it will state more clearly (and show with video examples) that individuals will not be identifiable in the SMART system.

Note: it is not sufficient that individuals are not being identified or that techniques are employed to render data anonymous. The system must be set up in such a manner that identification is impossible due to image quality, camera distance and/or camera angle and that the cameras are at their maximum zoom.

This will be updated as the situation developments.

4.2 Measures for Secure Storage

Data will be stored on secure systems. There will be controlled access and only authorised persons will be able to access the information. This authorisation will be managed by both the person in charge of the security of the servers system (i.e. software security systems to avoid hacking or other attempted ways to access the data other than through the controlled means), and by the ethics panel of the project who will control who can access the data and on what grounds.

Furthermore;

- Prevention of access by any unauthorised person to installations used for processing the SMART personal data. This control of entrance to installations is not directly a responsibility of SMART applications, but must be borne in mind before the implantation of SMART applications in a real environment. All services which store images and/or audio must to have permission of the ethics committee of the project.
- To prevent data media from being read, copied, altered or removed by unauthorised persons. SMART applications must include mechanism to authenticate and identify authorised persons.
- To safeguard data security copies will be made and a mechanism established in advance to restore data in case of data destruction/loss, partial or total. These backup/restore mechanisms must be checked periodically in order to verify the correct operation. This requirement not only implies to SMART applications, it involves the entire SMART system. Furthermore, the backup/recovery copy shall be stored outside the place where the information systems are located, and such copy will be protected by implementing all the above security measures
- According to the Principle of Conservation and Principle of Finality/Purpose Limitation the data is stored for the duration of the SMART project and for the purposes of the project, and will not be made available to parties outside the consortium, other than in processed form in the context of the project. The SMART system will ensure the secure storage and transmission of personal data (Principle of Security). All images and/or audio stored must be deleted one month later if it doesn't have security utilities. All security utilities must be ordered by a judge.
- All images and/or audio signals when are converted in files format must to accomplish regulations of LOPD (Data protection Law) as a Data file.
- Any tests to be conducted prior to the implementation or modification of SMART applications that manage personal data shall be done with no real data (only fictitious data may be used in such tests), unless if it assures the required security level.

As an additional measure, the project is considering the following:

- A record of Incidences: The record should indicate the procedures followed to recover the data, the name of the person who recovered such data, and the data manually re-introduced.
- Periodic audits: The personal data database shall be audited periodically by an employee or a third independent party. The audit report shall indicate the adequacy of the security measures adopted, deficiencies of the security measures and alternative or additional measures that shall be implemented. It must also include the data, facts or comments on which such report is based.

4.3 Measures for Privacy Protection

- Volunteers participating in the field trials will have provided informed consent prior to the trial and will be made aware of how their personal data will be used, the purpose of the data collection and their rights with respect to that personal data.
- SMART will notify bystanders of public and private spaces employed in all data collections and testing of the monitoring system. This will be implemented by posting a notice visible from all access points to the employed area.
- Information about data collection locations and images/videos potentially capturing the identity of captured bystanders will be stored anonymously in a secure database and will be destroyed as soon as the study/research task is completed and in any case will be automatically destroyed at the end of the project. Access to the database will be permitted only to authorized personnel, whose access is controlled through secure authentication techniques (see also the Annex 2- Indication of how any data storage and handling processes will ensure data protection and confidentiality).
- Any accidental or incidental collection of video data that might be related to personal information of bystanders, captured by SMART monitoring system, “such as the capture of a person’s vehicle number plate or any other personal data that might be used to identify the person, will be blurred before being made public.
- In the case of bystanders, they will be informed that data is being collected and monitored in any private or public space before entering into it and all data will be rendered anonymous (blurring of faces, etc.) before any public disclosure.

4.4 Other measures

Control of ‘sensitive’ or ‘special’ data: (See section 3.2.6.1).

- It is forbidden to generate any file with the sole reason collecting sensitive data
- The consent form must include explicitly include consent for collection of sensitive data.

Informing of data subjects (See section 3.2.6.2).

- The consent form and public notice to bystanders must include the identity of the data controller, the purpose of data collection, any recipients of the data, the voluntary nature of data provision and the existence of the right to access.

The right of access (See section 3.2.6.4).

- SMART must make available and known to data subjects the mechanism for the right to access personal data stored on them, as well as the remainder of rights related to this (right to object, right to rectification, erasure and so on).

5 Conclusions

In conclusion it has been shown that the SMART project has carried out due diligence in identifying the relevant laws and legislation applicable to the project.

Analysis of the regulations has exposed a number of obligations which the project must comply with and a number of rights which the data subjects have. Without negating the remainder of the clauses on the named documentation, or indeed any other laws applicable in any project participant state, the principal issues have been discussed, along with the implications on the project.

The project has decided on a number of measures, relating to the way data is stored and processed, and in interacting with bystanders and volunteers which will be carried out to ensure no breach of the law. One area of compliance, permission from the DPA has proved more complicated in practice. The initial solicitude was rejected. The project is taking action to redress this issue.

6 BIBLIOGRAPHY AND REFERENCES

D7.8 Ethical Dimensions of SMART Technologies

Korff, D., Comparative Summary Of National Laws: EC STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE (Study Contract ETD/2001/B5-3001/A/49). September 2002

The Charter of Fundamental Rights of the EU

The Data Protection Directive 95/46/EC

The European Convention of Human Rights and Fundamental Freedoms

The Privacy and Electronic Communications Directive 2002/58/EC

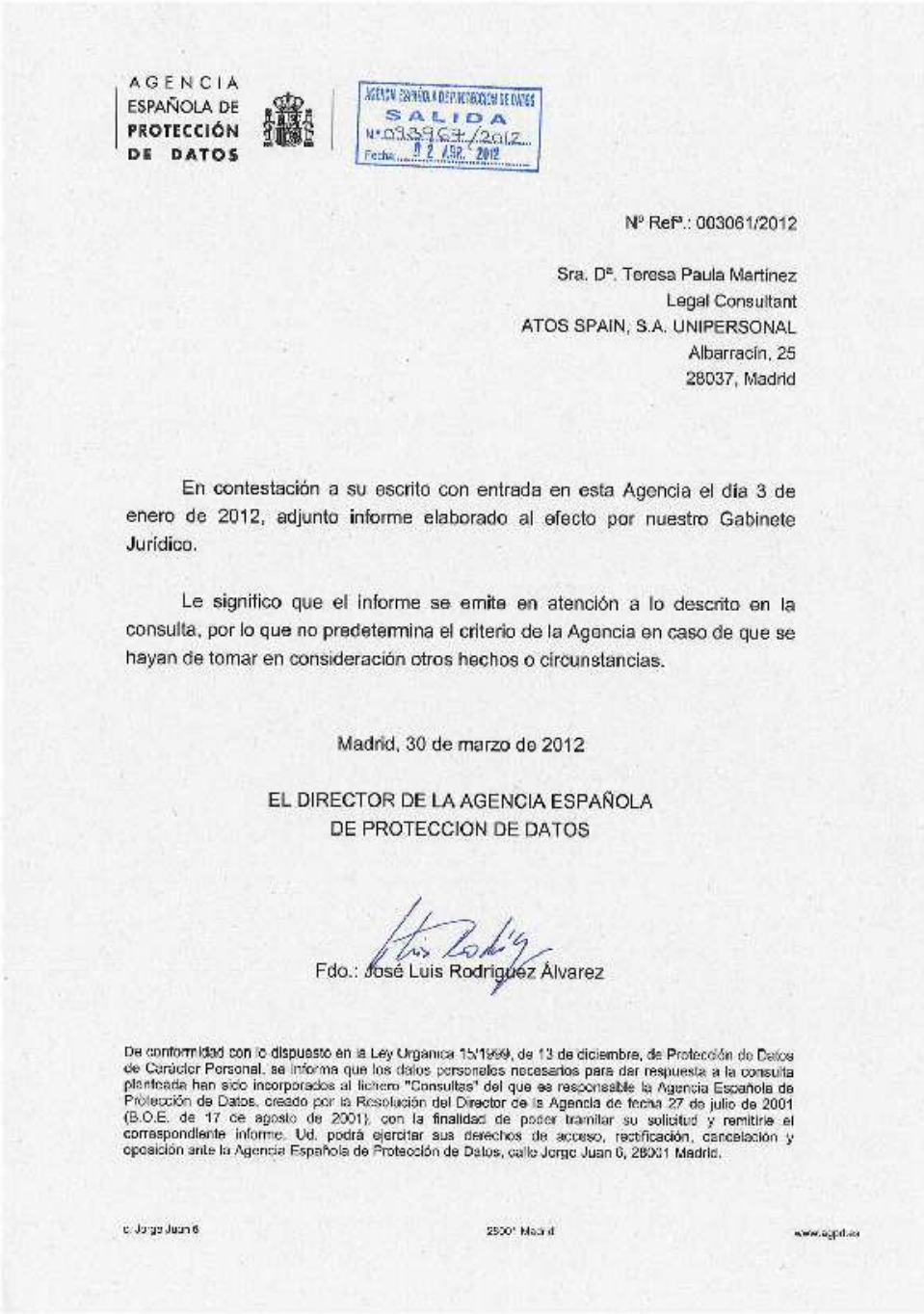
Translation of the Spanish Constitution:

http://www.servat.unibe.ch/icl/sp00000_.html

Retrieved 06/03/2012

7 ANNEXES

7.1 DPA (Spanish)



AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
SALIDA
Nº 013964/2012
Fecha 02 ABR. 2012

Nº Refª.: 003061/2012

Sra. Dª. Teresa Paula Martínez
Legal Consultant
ATOS SPAIN, S.A. UNIPERSONAL
Albarracín, 25
28037, Madrid

En contestación a su escrito con entrada en esta Agencia el día 3 de enero de 2012, adjunto informe elaborado al efecto por nuestro Gabinete Jurídico.

Le significo que el informe se emite en atención a lo descrito en la consulta, por lo que no predetermina el criterio de la Agencia en caso de que se hayan de tomar en consideración otros hechos o circunstancias.

Madrid, 30 de marzo de 2012

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCION DE DATOS

Fdo.: José Luis Rodríguez Álvarez

De conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa que los datos personales necesarios para dar respuesta a la consulta planteada han sido incorporados al fichero "Consultas" del que es responsable la Agencia Española de Protección de Datos, creado por la Resolución del Director de la Agencia de fecha 27 de julio de 2001 (B.O.E. de 17 de agosto de 2001), con la finalidad de poder tramitar su solicitud y remitirle el correspondiente informe. Ud. podrá ejercitar sus derechos de acceso, rectificación, cancelación y oposición ante la Agencia Española de Protección de Datos, calle Jorge Juan 6, 28001 Madrid.

c/ Jorge Juan 6 28001 Madrid www.agpd.es

lunes, 02 de abril de 2012.max

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

Ref. de entrada 003061/2012

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente a la consulta planteada por ATOS SPAIN, S.A. UNIPERSONAL, cúmpleme informarle lo siguiente:

Se consulta si resulta conforme a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la captación de imágenes y sonidos en las calles de una población con dos finalidades: la vigilancia o seguridad pública y la divulgación o difusión de noticias. Dicha divulgación se pretende llevar a cabo a través de internet mediante el uso de las redes sociales o de otras plataformas públicas.

Según señala la consulta se pretende la instalación en una determinada población de 4 cámaras, que estarán a la altura de las luminarias con micrófonos integrados en las mismas, en lugares muy concurridos y que estén cercanos a los dispositivos de otras redes de sensores de modo que se pueda utilizar la información adicional de esos sensores. Según indica las imágenes y los sonidos son filmados en vivo y la búsqueda es en tiempo real, pero también se graban las imágenes y posteriormente, en caso de ser necesaria la divulgación de imágenes o identificación de personas se realizaría una labor de difuminado de rostros, matrículas, etc.

I

Con carácter previo, debe recordarse que el derecho a la protección de datos personales ha sido configurado por el Tribunal Constitucional en su Sentencia 292/2000 como un derecho fundamental distinto al derecho a la intimidad, cuyo contenido esencial según expone dicha sentencia consiste en *"un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos."*

c. Jorge Juan 6
28001 Madrid
www.agpd.es

1

lunes, 02 de abril de 2012.max

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

Asimismo, y dado que la presente consulta hace referencia a la posibilidad de captar imágenes de las personas que circulan por lugares públicos deben tenerse en cuenta las consideraciones efectuadas a este respecto por el Grupo de Trabajo del artículo 29, órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en el Dictamen 4/2004, relativo al tratamiento de datos personales mediante vigilancia por videocámara.

El citado Dictamen señala que *"una parte considerable de la información recogida mediante la vigilancia por videocámara se refiere a personas identificadas o identificables, que han sido filmadas mientras se encontraban en un lugar público o abierto al público. Es muy posible que la persona que se encuentra de paso se espere disfrutar de un menor grado de intimidad, pero lo que no se espera es verse totalmente desprovisto de sus derechos y libertades en lo que se refiere a su propia esfera e imagen"*, al tiempo que pone de manifiesto la aplicabilidad de la citada Directiva que garantiza a la protección del derecho a la intimidad y la vida privada, así como la gama más amplia de protección de datos personales en lo que respecta a las libertades y los derechos fundamentales de las personas físicas.

Asimismo, recuerda el Dictamen que *"también cabe tener en cuenta aquí el derecho a la libre circulación de las personas que se encuentran en el territorio de un Estado de manera legal, lo que se contempla en el artículo 2 del Protocolo Adicional nº 4 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.*

Dicha libertad de circulación sólo puede estar sujeta a restricciones necesarias en una sociedad democrática y proporcionales a la consecución de fines específicos. Los interesados tienen derecho a ejercer su derecho a la libre circulación sin verse sometidos a un condicionamiento psicológico excesivo en cuanto a sus movimientos y su conducta y sin ser objeto de un control detallado, como la posibilidad de que se sigan sus movimientos o se disparen «alarmas» basadas en programas informáticos que «interpretan» de manera automática la conducta supuestamente sospechosa de un individuo, sin ningún tipo de intervención humana, a causa de la utilización desproporcionada de la vigilancia por videocámara por parte de varias entidades en diversos lugares públicos o abiertos al público."

II

Con carácter general debe indicarse que los artículos 1 y 2 de la Ley Orgánica 15/1999, extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento de sus datos de carácter personal, siendo definidos éstos en el

c. Jorge Juan 6
28001 Madrid
www.agpd.es

lunes, 02 de abril de 2012.max

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

artículo 3.a) de la citada Ley como "*cualquier información concerniente a personas físicas identificadas o identificables.*"

El artículo 5.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, precisa que constituye un dato de carácter personal "*Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.*"

En consecuencia, tanto la imagen como la voz de una persona identificada o identificable constituyen datos de carácter personal, por lo que su tratamiento está sujeto a lo previsto en la normativa de protección de datos. Asimismo, conforme a la definición del artículo 5 arriba transcrito, esa calificación se extiende a otras informaciones, como las matrículas de los vehículos que circulen por la calle, que igualmente serían captadas con las cámaras. En este sentido, el informe de esta Agencia de 8 de febrero de 2007 recordaba el carácter de dato personal que las matrículas de vehículos pueden tener y, en consecuencia, la sumisión a la Ley Orgánica 15/1999 del tratamiento de dicho dato. Se señalaba en el mismo que, siguiendo el criterio sustentado por las distintas Recomendaciones emitidas por el Comité de Ministros del Consejo de Europa, en las que se indica que la persona deberá considerarse identificable cuando su identificación no requiere plazos o actividades desproporcionados, debe concluirse que las placas de matrícula constituyen un dato personal por reunir dichas características, ya que la identificación del titular de los vehículos cuya matrícula sea conocida, únicamente exigirá la consulta del Registro de Vehículos, al que se refiere el Reglamento General de Vehículos, aprobado por Real Decreto 2822/1998, de 23 de diciembre, cuya finalidad esencial es la identificación del titular, para lo cual únicamente será necesaria la invocación del interés legítimo del solicitante.

Debe así tenerse en cuenta que tanto la captación en vivo como la grabación de dichos datos o cualquier otro concemiento a personas identificadas o identificables constituyen un tratamiento de datos de carácter personal, tal y como dispone el artículo 3 de la Ley Orgánica 15/1999 al definir éste como "*las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.*"

En aplicación de la normativa de protección de datos, para que la captación de dichos datos sea lícita será preciso que se encuentre legitimada en la forma prevista en el artículo 6 de la Ley Orgánica 15/1999 conforme al cual "*el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.*"

c/ Jorge Juan 6
28001 Madrid
www.agpd.es

3

lunes, 02 de abril de 2012.max

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

Debe señalarse que dada la imposibilidad en la práctica de obtener el consentimiento de las personas que transitan por las calles cuyos datos son captados por las cámaras al pasar, esta Agencia ha venido considerando que la legitimación para dicho tratamiento debe encontrarse en una norma con rango de Ley, de manera que no existiendo una Ley habilitadora dicho tratamiento constituirá una vulneración de lo previsto en la citada Ley Orgánica.

En lo que se refiere a la visualización y grabación con videocámaras de datos de personas físicas identificadas o identificables en las vías públicas, dicha legitimación viene restringida al supuesto de videovigilancia, debiendo tenerse en cuenta que la instalación de cámaras en las vías públicas con fines de videovigilancia solo está permitida cuando es realizada por las Fuerzas y Cuerpos de Seguridad, en los términos establecidos en la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos y su Reglamento de desarrollo, aprobado por Real Decreto 596/1999, de 16 de abril.

Dicha instalación de cámaras con fines de videovigilancia se encuentra sujeta a muy estrictos requisitos de los que aquí cabe mencionar los relativos a su autorización, regulados en el artículo 3 de la Ley 4/19997 que dispone lo siguiente:

"1. La instalación de videocámaras o de cualquier medio técnico análogo en los términos del artículo 1.2 de la presente Ley está sujeta al régimen de autorización, que se otorgará, en su caso, previo informe de un órgano colegiado presidido por un Magistrado y en cuya composición no serán mayoría los miembros dependientes de la Administración autorizante.

2. Las instalaciones fijas de videocámaras por las Fuerzas y Cuerpos de Seguridad del Estado y de las Corporaciones Locales serán autorizadas por el Delegado del Gobierno en la Comunidad Autónoma de que se trate, previo informe de una Comisión cuya presidencia corresponderá al Presidente del Tribunal Superior de Justicia de la misma Comunidad. La composición y funcionamiento de la Comisión, así como la participación de los municipios en ella, se determinarán reglamentariamente.

3. No podrá autorizarse la instalación fija de videocámaras cuando el informe de la Comisión prevista en el apartado 2 de este artículo estime que dicha instalación supondría una vulneración de los criterios establecidos en el artículo 4 de la presente Ley Orgánica.

4. La resolución por la que acuerde la autorización deberá ser motivada y referida en cada caso al lugar público concreto que ha de ser objeto de observación por las videocámaras. Dicha resolución contendrá también todas las limitaciones o condiciones de uso necesarias, en particular la prohibición de tomar sonidos, excepto cuando concurra un riesgo concreto y preciso, así como las referentes a la

c. Jorge Juan 6
28001 Madrid
www.agpd.es

4

lunes, 02 de abril de 2012.max

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

cualificación de las personas encargadas de la explotación del sistema de tratamiento de imágenes y sonidos y las medidas a adoptar para garantizar el respeto de las disposiciones legales vigentes. Asimismo deberá precisar genéricamente el ámbito físico susceptible de ser grabado, el tipo de cámara, sus especificaciones técnicas y la duración de la autorización, que tendrá una vigencia máxima de un año, a cuyo término habrá de solicitarse su renovación."

Los criterios de autorización se encuentran en el artículo 4 de la norma según el cual *"Para autorizar la instalación de videocámaras se tendrán en cuenta, conforme al principio de proporcionalidad, los siguientes criterios: asegurar la protección de los edificios e instalaciones públicas y de sus accesos; salvaguardar las instalaciones útiles para la defensa nacional; constatar infracciones a la seguridad ciudadana, y prevenir la causación de daños a las personas y bienes."*

- Exige además dicha normativa que se adopte un criterio de proporcionalidad en su utilización, disponiendo en su artículo 6 que:

"1. La utilización de videocámaras estará presidida por el principio de proporcionalidad, en su doble versión de idoneidad y de intervención mínima.

2. La idoneidad determina que sólo podrá emplearse la videocámara cuando resulte adecuado, en una situación concreta, para el mantenimiento de la seguridad ciudadana, de conformidad con lo dispuesto en esta Ley.

3. La intervención mínima exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho al honor, a la propia imagen y a la intimidad de las personas.

4. La utilización de videocámaras exigirá la existencia de un razonable riesgo para la seguridad ciudadana, en el caso de las fijas, o de un peligro concreto, en el caso de las móviles.

5. No se podrán utilizar videocámaras para tomar imágenes ni sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial, ni de los lugares incluidos en el artículo 1 de esta Ley cuando se afecte de forma directa y grave a la intimidad de las personas, así como tampoco para grabar conversaciones de naturaleza estrictamente privada. Las imágenes y sonidos obtenidos accidentalmente en estos casos deberán ser destruidas inmediatamente, por quien tenga la responsabilidad de su custodia."

Uno de los de los aspectos esenciales del tratamiento de datos captados por las cámaras por parte de las Fuerzas y Cuerpos de Seguridad es el de la finalidad de las grabaciones, determinada en el artículo 7 de la Ley 4/1997, según el cual

c. Jorge Juan 6
28001 Madrid
www.agpd.es

5

lunes, 02 de abril de 2012.max

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

"1. Realizada la filmación de acuerdo con los requisitos establecidos en la Ley, si la grabación captara la comisión de hechos que pudieran ser constitutivos de ilícitos penales, las Fuerzas y Cuerpos de Seguridad pondrán la cinta o soporte original de las imágenes y sonidos en su integridad a disposición judicial con la mayor inmediatez posible y, en todo caso, en el plazo máximo de setenta y dos horas desde su grabación. De no poder redactarse el atestado en tal plazo, se relatarán verbalmente los hechos a la autoridad judicial, o al Ministerio Fiscal, junto con la entrega de la grabación.

2. Si la grabación captara hechos que pudieran ser constitutivos de infracciones administrativas relacionadas con la seguridad ciudadana, se remitirán al órgano competente, igualmente de inmediato, para el inicio del oportuno procedimiento sancionador."

Si las imágenes grabadas no captan hechos constitutivos de ilícitos penales o infracciones administrativas deberán ser destruidas, tal y como dispone el artículo 8 de la Ley, a cuyo tenor *"1. Las grabaciones serán destruidas en el plazo máximo de un mes desde su captación, salvo que estén relacionadas con infracciones penales o administrativas graves o muy graves en materia de seguridad pública, con una investigación policial en curso o con un procedimiento judicial o administrativo abierto."*

Por último, cabe reseñar que el número 2 de dicho artículo 8 recoge un deber de secreto en relación con las mismas al disponer que *"Cualquier persona que por razón del ejercicio de sus funciones tenga acceso a las grabaciones deberá observar la debida reserva, confidencialidad y sigilo en relación con las mismas, siéndole de aplicación, en caso contrario, lo dispuesto en el artículo 10 de la presente Ley."*

Por su parte el artículo 10 señala que *"Cuando no haya lugar a exigir responsabilidades penales, las infracciones a lo dispuesto en la presente Ley serán sancionadas con arreglo al régimen disciplinario correspondiente a los infractores y, en su defecto, con sujeción al régimen general de sanciones en materia de tratamiento automatizado de datos de carácter personal."*

De este modo, la instalación de cámaras en los espacios públicos que visualicen o graben a las personas que por ella transitan, con fines de videovigilancia solo se encuentra legitimada por lo previsto en la Ley Orgánica 4/1997, que encomienda exclusivamente a las Fuerzas y Cuerpos de Seguridad, con los requisitos y limitaciones recogidos en dicha Ley Orgánica y su normativa de desarrollo y con la única finalidad de puesta a disposición de la autoridad judicial o administrativa de las imágenes captadas cuando constituyan un ilícito penal o administrativo, debiendo destruirse las restantes.

En consecuencia, el consultante carece de legitimación alguna para proceder

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

a la captación de datos de personas físicas identificadas o identificables en espacios públicos con fines de videovigilancia.

III

La consulta indica que otra posible finalidad de la captación de los datos en las vías públicas sería la de la difusión de noticias. A este respecto debe tenerse en cuenta que el catálogo de supuestos legitimadores del tratamiento se ha visto ampliado por la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, por la que se resuelven las cuestiones prejudiciales planteadas por el Tribunal Supremo en los recursos interpuestos contra el Reglamento de desarrollo de la Ley Orgánica 15/1999. A su vez, el marco se ve igualmente afectado por las Sentencias dictadas por el Tribunal Supremo en fecha 8 de febrero de 2012, por las que se resuelven los mencionados recursos.

La Sentencia del Tribunal de Justicia ha declarado expresamente el efecto directo del artículo 7 f) de la Directiva 95/46/CE, según el cual *"Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si (...) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva"*. Por ello, dicho precepto deberá ser tomado directamente en cuenta en la aplicación de la normativa de protección de datos de carácter personal por los Estados Miembros, y en consecuencia por esta Agencia Española de Protección de Datos, dado que como señala el Tribunal Supremo en su sentencia de 8 de febrero de 2012 *"produce efectos jurídicos inmediatos sin necesidad de normas nacionales para su aplicación, y que por ello puede hacerse valer ante las autoridades administrativas y judiciales cuando se observe su trasgresión"*.

Tal y como recuerda la Sentencia del Tribunal de Justicia de la Unión Europea en su apartado 38, el artículo 7 f) de la Directiva *"establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado"* y, en relación con la citada ponderación, el apartado 40 recuerda que la misma *"dependerá, en principio, de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea confieren al interesado"*.

c/ Jorge Juan 6
28001 Madrid
www.agpd.es

7

lunes, 02 de abril de 2012.max

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

Por este motivo, la sentencia señala en su apartado 46 que los Estados miembros, a la hora de adaptar su ordenamiento jurídico a la Directiva 95/46, deberán "procurar basarse en una interpretación de ésta que les permita garantizar un justo equilibrio entre los distintos derechos y libertades fundamentales protegidos por el ordenamiento jurídico de la Unión", por lo que, conforme a su apartado 47 "nada se opone a que, en ejercicio del margen de apreciación que les confiere el artículo 5 de la Directiva 95/46, los Estados miembros establezcan los principios que deben regir dicha ponderación".

Teniendo en cuenta lo anterior, cabria examinar si la captación de imágenes y sonidos en la forma señalada en la consulta con la finalidad de difusión de noticias podria encontrarse amparada en la libertad de información recogida en el artículo 20 de la Constitución que dispone en su epígrafe 1, apartados a) y d):

"1. Se reconocen y protegen los derechos:
a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.
(...)
d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades."

En este sentido la propia Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, dispone en su artículo 9 que *"en lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión".*

El legislador español no ha establecido una previsión similar a la establecida por el artículo 9 de la Directiva 95/46/CE. No obstante, la resolución del conflicto entre los derechos reconocidos en los artículos 18 y 20 de la Constitución ha sido objeto de reiterado análisis por la jurisprudencia del Tribunal Constitucional, sentando como regla general la doctrina emanada del citado tribunal que el segundo de los derechos citados prevalecerá en aquéllos supuestos en los que la información objeto de publicación sea, por una parte, veraz, y por otra resulte de relevancia pública, siendo de interés general las materias a las que la misma se refiere y la relevancia de las personas a las que la misma se refiere.

En particular y en lo que al derecho a la propia imagen se refiere, resulta de especial interés la doctrina sentada por el Tribunal Constitucional en el marco de

lunes, 02 de abril de 2012.max

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

protección establecido por la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

Así la Sentencia 81/2001, de 26 de marzo de 2001, pone de manifiesto el contenido esencial de dicho derecho declarando que *"En su dimensión constitucional, el derecho a la propia imagen consagrado en el art. 18.1 CE se configura como un derecho de la personalidad, derivado de la dignidad humana y dirigido a proteger la dimensión moral de las personas, que atribuye a su titular un derecho a determinar la información gráfica generada por sus rasgos físicos personales que puede tener difusión pública.*

(...)La facultad otorgada por este derecho, en tanto que derecho fundamental, consiste en esencia en impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad -informativa, comercial, científica, cultural, etc.- perseguida por quien la capta o difunde. Así, pues, lo que se pretende con este derecho, en su dimensión constitucional, es que los individuos puedan decidir qué aspectos de su persona desean preservar de la difusión pública, a fin de garantizar un ámbito privativo para el desarrollo de la propia personalidad ajeno a injerencias externas.

Por supuesto, al igual que sucede con los demás derechos, el derecho a la propia imagen no es absoluto. Como todos los derechos encuentra límites en otros derechos y bienes constitucionales y en este caso, muy particularmente, en el derecho a la comunicación de información y en las libertades de expresión y de creación artística."

En cuanto a la concreción de esos límites cabe recordar en primer término los fijados por la propia Ley Orgánica 1/1982 en su artículo 8.2, según el cual *"En particular, el derecho a la propia imagen no impedirá:*

a) *Su captación, reproducción o publicación por cualquier medio cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público.*
b) *La utilización de la caricatura de dichas personas, de acuerdo con el uso social.*
c) *La información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesoria.*

Las excepciones contempladas en los párrafos a) y b) no serán de aplicación respecto de las autoridades o personas que desempeñen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza." (El subrayado es de la Agencia de Protección de Datos)

C. Jorge Juan 6
28001 Madrid
www.agpd.es

lunes, 02 de abril de 2012.max

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

Igualmente, el Tribunal Constitucional se ha pronunciado en diversas ocasiones sobre dichos límites, razonaba así la Sentencia 156/2001 *"La determinación de estos límites debe efectuarse tomando en consideración la dimensión teleológica del derecho, y por esta razón hemos considerado que debe salvaguardarse el interés de la persona en evitar la captación o difusión de su imagen sin su autorización o sin que existan circunstancias que legitimen esa intromisión. De ahí que hayamos sostenido que "la captación y difusión de la imagen del sujeto sólo será admisible cuando la propia -y previa- conducta de aquél o las circunstancias en las que se encuentre inmerso, justifiquen el descenso de las barreras de reserva para que prevalezca el interés ajeno o el público que puedan colisionar con aquél" (STC 99/1994, FJ 5).*

Resulta, por tanto, que el derecho a la imagen se encuentra delimitado por la propia voluntad del titular del derecho que es, en principio, a quien corresponde decidir si permite o no la captación o difusión de su imagen por un tercero. No obstante, como ya se ha señalado, existen circunstancias que pueden conllevar que la regla enunciada ceda, lo que ocurrirá en los casos en los que exista un interés público en la captación o difusión de la imagen y este interés público se considere constitucionalmente prevalente al interés de la persona en evitar la captación o difusión de su imagen. Por ello, cuando este derecho fundamental entre en colisión con otros bienes o derechos constitucionalmente protegidos, deberán ponderarse los distintos intereses enfrentados y, atendiendo a las circunstancias concretas de cada caso, decidir qué interés merece mayor protección, si el interés del titular del derecho a la imagen en que sus rasgos físicos no se capten o difundan sin su consentimiento o el interés público en la captación o difusión de su imagen."

De este modo, el alcance de los requisitos exigidos por la jurisprudencia constitucional para entender prevalente el derecho a la libertad de información sobre el derecho a la protección de datos deben interpretarse coherentemente con lo dispuesto en el artículo 9 de la Directiva 95/46/CE, que ya se ha reproducido; es decir, esta prevalencia se debe fundar en excepciones a la aplicación de las normas de protección de datos *"sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión"*.

En este sentido, y expresándonos en la terminología establecida en la Ley Orgánica 15/1999, las excepciones a la aplicación de dicha norma deben entenderse como manifestaciones del principio de proporcionalidad, consagrado por el artículo 4.1 de la Ley Orgánica, a cuyo tenor *"Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido"*.

De todo lo señalado cabe concluir que para captar y posteriormente difundir la voz o imágenes de personas identificadas o identificables en cualquier medio, incluidas las redes sociales, sin recabar el consentimiento de los ciudadanos

c. Jorge Juan 6
28001 Madrid
www.agpd.es

lunes, 02 de abril de 2012.max

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

afectados, es preciso que la información publicada tenga relevancia pública, esto es, que se den las circunstancias constitucionalmente previstas para que la libertad de información prevalezca sobre el derecho a la protección de datos.

En el presente supuesto no nos encontramos ante la captación de voz o imagen en el ejercicio de la libertad de información cuando se produce una noticia, sino que se pretende proceder a una visualización y grabación continuada de un determinado espacio público por el que transitan los ciudadanos, con la finalidad de captar, en el hipotético caso de que se produjera, un hecho noticiable, por lo que dicho tratamiento no puede encontrar amparo en lo previsto en el artículo 7.f) de la Directiva 95/46/CE al resultar, de una parte, desproporcionado para la finalidad legítima de ejercicio de la libertad de información y, de otra, vulnerador de otros derechos fundamentales como los relativos a la intimidad y propia imagen e incluso al de la libertad de circulación de los ciudadanos, afectando especialmente a quienes residen o trabajan en el área en que se produce la captación de imágenes o acuden a ella habitualmente al procederse a un control injustificado de sus movimientos.

IV

Se consulta, asimismo, si el difuminado de los elementos identificativos de la personalidad tras la grabación de las imágenes determina que éstas no resulten datos de carácter personal y en consecuencia queda excluido su tratamiento de las prescripciones de la Ley Orgánica 15/1999.

Cabe recordar a este respecto, que el artículo 3 de la Ley Orgánica 15/1999 define el tratamiento de datos como *"las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."*

De este modo no solamente la difusión de los datos sino la visualización o grabación de los mismos constituyen un tratamiento de datos personales, que exige igualmente el consentimiento de los interesados o, en su defecto, encontrarse amparado en alguno de los supuestos de legitimación contemplados en la normativa de protección de datos y que, como ya se han analizado, no resultan de aplicación al presente caso.

No obstante, no resultaría de aplicación la Ley Orgánica 15/1999 en el supuesto de que los datos captados con las cámaras no permitieran la identificación de las personas. De este modo, solo sería posible la visualización o grabación de espacios públicos por los que circulan las personas o vehículos pretendida por el consultante cuando no se graben sonidos y no resulte posible la lectura de las matrículas o la identificación de las personas, ya sea por la distancia con la que se toman las imágenes o utilizando parámetros digitales que impidan discernir rasgos

c. Jorge Juan 6
28001 Madrid
www.agpd.es

lunes, 02 de abril de 2012.max

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

faciales y números de matrícula. En este sentido, esta Agencia ha venido señalando la posibilidad de toma de imágenes panorámicas, así indicaba el Plan Sectorial de Oficio sobre videocámaras en Internet que "*La captación de imágenes de paisajes o panorámicas, en la medida en que no permitan identificar a las personas cuya imagen pueda ser captada quedaría fuera del ámbito de aplicación de la normativa de protección de datos.*

En definitiva, en tanto el consultante carece de legitimación para la captación en las vías públicas de sonidos e imágenes de personas identificadas o identificables, no podrá proceder a captar voces de las personas que por ellas transitan y solamente podrá visualizar o grabar imágenes de las mismas si ya en la propia captación, y no en un proceso posterior, dichas personas no resultan identificables.

V

Se consulta también si es posible la captación de voz e imágenes en lugares cerrados y privados, entendiendo esta Agencia que con ello se trata de referirse el consultante a espacios privados de uso público, tales como locales de ocio, centros comerciales, etc.

De conformidad con lo establecido en el artículo 6 antes transcrito de la Ley Orgánica 15/1999, la legitimación para captar imágenes de personas identificadas e identificables que se encuentren en dichos espacios exige el consentimiento de las personas que se encuentran en dichos espacios, que, igualmente, resultará prácticamente imposible de obtener o la existencia de una Ley que habilite dicha captación, teniendo en cuenta que la legitimación para el tratamiento fundada en lo previsto en el artículo 7.f) de la Directiva 95/46/CE resulta inaplicable también en este caso por las mismas razones antes expuestas.

En el marco de los espacios privados de uso público, sus propietarios o, en su caso, sus poseedores por cualquier título legítimo tienen la facultad de captar imágenes con fines de videovigilancia, encontrándose dicha habilitación en la Ley 23/1992, de 30 de julio, de Seguridad Privada, en particular en su artículo 5, cuya reforma, operada por la Ley 25/2009 de 27 de diciembre, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios, elimina la exigencia, anteriormente resultante de la interpretación conjunta de dicho precepto con el Reglamento de Seguridad Privada, aprobado por Real Decreto 2364/1994, de 9 de diciembre, de que la instalación de las cámaras fuese realizada por una empresa de seguridad que previamente hubiese cumplido con todos los requisitos legalmente establecidos, salvo en el supuesto en que las cámaras se encuentren conectadas a una central de alarmas.

La captación de imágenes con cámaras de videovigilancia en éste ámbito se encuentra sujeta a lo previsto en la Ley Orgánica 15/1999, a su Reglamento de

c. Jorge Juan 6
28001 Madrid
www.agpd.es

lunes, 02 de abril de 2012.max

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

desarrollo aprobado por Real Decreto 1720/2007, de 21 de diciembre, y a la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de videovigilancia a través de sistemas de cámaras o videocámaras.

Sin perjuicio de la exigencia de otros requisitos, debe destacarse en el presente informe respecto de la captación de imágenes con fines de videovigilancia el principio de proporcionalidad en dicha captación.

Dicho principio se recoge en el artículo 4 de la Ley Orgánica 15/1999 a cuyo tenor *"Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido."*

La Instrucción 1/2006 de la Agencia Española de Protección de Datos, hace especial referencia a dicho principio al señalar *"El marco en que se mueve la presente Instrucción es claro. La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático.*

En relación con la instalación de sistemas de videocámaras, será necesario ponderar los bienes jurídicos protegidos. Por tanto, toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.

En consecuencia, el uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo funciones de vigilancia por lo que, desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo."

En la concreción de ese principio de proporcionalidad se encontrará en todo caso el derecho a la intimidad, honor y propia imagen de las personas de forma que resultará *desproporcionada la captación de imágenes que puedan afectar a dichos derechos o la escucha o grabación de conversaciones*. Cabe así recordar que la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, dispone en su artículo 7 que *"Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo segundo de esta Ley:*

c. Jorge Juan 6
28001 Madrid
www.agpd.es

lunes, 02 de abril de 2012.max

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

Uno. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.

Dos. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción."

Debe recordarse que otro de sus límites viene dado por la prohibición de captar imágenes de las vías públicas, que como se ha señalado con anterioridad solamente puede llevarse a cabo por las Fuerzas y Cuerpos de Seguridad en el marco de lo establecido en la Ley Orgánica 4/1997.

Asimismo, las imágenes captadas con fines de videovigilancia, están sujetas al principio de finalidad recogido en el artículo 4.2 de la Ley Orgánica 15/1999 según el cual *"Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos"*. Debe aclararse aquí que la Audiencia Nacional partiendo de una interpretación sistemática de este precepto viene considerando la expresión "finalidades incompatibles" como sinónimo de "finalidades distintas".

Siendo la finalidad de la videovigilancia en lugares privados de uso público la misma que para los espacios públicos, esto es la puesta a disposición de la policía o de la autoridad judicial de las imágenes que hayan captado la comisión de un delito o de la correspondiente autoridad administrativa si se trata de una infracción administrativa, la utilización con cualquier otro fin de las imágenes por parte del responsable resultará contraria a lo previsto en la Ley Orgánica 15/1999, salvo que dicha utilización venga legitimada en lo previsto en otra norma con rango de ley o en el consentimiento de los afectados por el tratamiento de su imagen.

Por otra parte, la comunicación de las imágenes por parte del responsable del fichero a persona distinta constituye una cesión de datos de carácter personal, definida en el artículo 3 i) de la Ley Orgánica 15/1999 como *"Toda revelación de datos realizada a una persona distinta del interesado"*. La misma calificación tendrá la difusión de las imágenes sea por internet o cualquier otro medio.

Tal cesión debe sujetarse al régimen general de comunicación de datos de carácter personal establecido en el artículo 11 de la misma Ley, donde se establece que la misma solo puede verificarse para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y cesionario y exige para que pueda tener lugar, el previo consentimiento del interesado (artículo 11.1), otorgado con carácter previo a la cesión y suficientemente informado de la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar (artículo 11.3), y que debe recabar el cedente como responsable del fichero que contiene los datos que se pretenden ceder.

c. Jorge Juan 6
28001 Madrid
www.agpd.es

lunes, 02 de abril de 2012.max

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

La cesión de datos sin consentimiento de los afectados constituirá una vulneración de lo previsto en la Ley Orgánica 15/1999, salvo que pudiera ampararse en alguna de las excepciones a la necesidad de consentimiento recogidas en el número segundo del artículo 11 de la misma Ley. De este modo, solo queda amparada en lo previsto en el citado artículo 11 la comunicación a las autoridades policiales, judiciales o administrativas correspondientes.

VI

Resumiendo lo hasta aquí expuesto cabe señalar los siguientes principios en esta materia que han venido exponiéndose en los diversos informes de esta Agencia:

La ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal extiende su protección a los datos de las personas físicas identificadas o identificables, ello incluye tanto la voz como la imagen de las personas y las matrículas de los vehículos, así como cualquier otro dato que pueda resultar identificativo de éstas. En este sentido, esta Agencia ha señalado que no resulta contraria a la misma la instalación de cámaras que se limiten a la toma de imágenes panorámicas, en cuanto éstas no capten datos de personas identificadas o identificables en los términos vistos.

La Ley orgánica 15/1999 se aplica no solamente a la difusión o cesión de las imágenes, cualquiera que sea el medio por el que se lleve a cabo, sino igualmente a su captación, siendo preciso que dicho tratamiento cuente con la correspondiente legitimación que en el presente supuesto, por la propia naturaleza del tratamiento, no puede fundarse en el consentimiento, ni en el interés legítimo a que hace referencia el artículo 7.f de la Directiva, por lo que solamente será posible en el caso de que exista una Ley habilitante

La habilitación para captar imágenes de personas identificadas o identificables en espacios públicos, queda restringida a la función de videovigilancia efectuada exclusivamente por las Fuerzas y Cuerpos de Seguridad en el marco de la Ley Orgánica 4/1997.

En los lugares privados de uso público sus propietarios o poseedores se encuentran legitimados por la ley 23/1992, de Seguridad Privada para captar imágenes de personas identificadas o identificables con fines de videovigilancia, con los requisitos y límites fijados en la normativa de protección de datos. La captación de dichas imágenes tiene como finalidad su puesta a disposición de las autoridades policiales, judiciales o administrativas cuando en las mismas se compruebe la comisión de un delito o infracción. Dicha captación de imágenes está sujeta al principio de finalidad recogido en el artículo 4.2 de la Ley Orgánica 15/1999 por lo que resulta contrario a lo previsto en la misma Ley su utilización para otros fines.

c. Jorge Juan 6
28001 Madrid
www.agpd.es

15

lunes, 02 de abril de 2012.max

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Gabinete Jurídico

Asimismo, la comunicación de dichas imágenes a terceros distintos de la autoridades encargadas de la prevención de los delitos o infracciones o su difusión por cualquier medio, constituyen una cesión de datos personales y, en consecuencia, una vulneración de lo previsto en la Ley Orgánica 15/1999, salvo que se disponga del consentimiento de los afectados por el tratamiento.

Es cuanto tiene el honor de informar.

Madrid, 7 de marzo de 2012.

LA CONSEJERA TECNICA
DE LA UNIDAD DE APOYO A LA DIRECCIÓN

Fdo.- Marta Fernández López

Visto y conforme,
EL ABOGADO DEL ESTADO
JEFE DEL GABINETE JURÍDICO

Fdo. Agustín Puente Escobar

SR. DIRECTOR DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

c. Jorge Juan 6
28001 Madrid
www.agpd.es

16

lunes, 02 de abril de 2012.max