

Charter for a democratic use of video-surveillance





This project has received the financial support of the European Commission within the framework of its Fundamental Rights and Citizenship Programme

European Forum for Urban Security

10, rue des Montiboefus, 75020 Paris

+ 33 1 40 64 49 00

www.efus.eu // contact@efus.eu

Printer the 20th of May

By STIPA

Design : Pete Jeffs // Translation : Tom Bayes

>>> Preamble

The video-surveillance systems of European cities are witnessing qualitative and quantitative evolutions which are subject to differences in local and national contexts, as well as political, economic, cultural and social factors.

This project, involving ten European partners – Cities of Genoa, Rotterdam, Liège, Le Havre, Ibiza, Saint-Herblain, Regions of Veneto and Emilia-Romagna, London Metropolitan Police, Sussex Police – and experts, aimed to reaffirm those points of convergence that exist in spite of these differences. These points of convergence are the foundation of this work; upon them can be constructed methods and strategies for the effective and appropriate use of video-surveillance.

The first point is the common necessity to include in the development and functioning of video-surveillance systems guarantees that protect citizens' privacy and fundamental liberties. This requirement is enshrined in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms which states that:

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

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 objective of this Charter is to provide citizens with guaranties regarding the use of CCTV, as these systems

- affect the expression of individual liberties in the area under surveillance;
- develop in such a way as to exceed their original objectives, through the ongoing and rapid technological developments that characterise this area of activity;
- have the potential to generate concerns and debate among citizens;

To put the citizen at the heart of the city’s judgements regarding video-surveillance systems has been the guiding light of the project ‘Citizens, Cities and Video-Surveillance’. To this aim can be added the respect for and the enshrining of the citizen’s right to privacy in public spaces.

The second point of convergence is the demand to translate the aim of citizen engagement into practice.

The principles contained in the Charter for the Democratic Use of Video-Surveillance aim to balance these two points. Through a set of self-imposed rules, it is an engagement to which its signatories commit themselves. These fundamental principles are set out alongside concrete measures to ensure that these same principles are acted upon. In this way, the Charter becomes more than an abstract statement and is in reality a working and practical document.

Some recommendations, contained in this Charter, represent the expression of several principles. These recommendations are summarised as the four ‘methodological tools’ identified by partners to the project. The four such tools are:

- The undertaking of prior audits to define objectively local needs. These audits should also allow an evaluation of the feasibility of a video-surveillance project in a given area. Ideally, this audit should be carried out by an external body;
- Periodical evaluations serving as an aid to decision making and allowing for a strengthening or repositioning of the video-surveillance system;
- Training of operators. The operators are the key-stone of the video-surveillance system. On them largely depends the sound functioning of the system. Their training should include the fundamental principles of this charter but equally the recommendations to be put into practice. The objectives of the system should also form a part of their training. Training ensures quality;
- A controlling authority should guarantee adherence to the Charter's principles. The creation of such a local structure could be set in motion either by national law or as a result of local initiative. This authority must be of the greatest possible independence;

The scope of application >>> of the charter

This Charter governs the design, operation and subsequent development of public video-surveillance systems, i.e. those operated by public authorities, be they national, regional or local. However, the rules set out in the Charter should also be applied to private video-surveillance systems, especially when their use and their data might be made available to public authorities.

The fundamental >>> principles

Seven principles have been outlined. These principles are complementary and thus should not be considered mutually exclusive. They are self-confirming in their relevance and in their permanence.

I. The principle of legality

The design and development of video-surveillance systems can only be undertaken in compliance with existing laws and regulations.

Respect of and compliance with European, national, regional and local laws. A video-surveillance system should also only be developed in compliance with norms regarding data-protection, the monitoring of communication and conversations, illicit interference with privacy, protection of dignity, image, home and other places. Norms concerning protection of workers should also be taken into account.

RECOMMENDATIONS AND FORMS OF ACTION

Video-surveillance systems should be developed in line with:

1) Major European and international texts:

- The Convention for the Protection of Human Rights and Fundamental Freedoms (CEDH) of the Council of Europe - 1950;
- The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - 1981;
- Charter of Fundamental Rights of the European Union;
- Directive 95/46/CE of the European Parliament and of the Council of 24th October 1995 relative to the protection of persons in regard to the handling of personal data and the free circulation of these data;

2) National and local rulings governing video-surveillance systems and protection of personal data:

- Assess whether the installation of a CCTV system is suitable or appropriate to achieve the objectives for which the Constitution allows a limitation of fundamental rights.

3) Jurisprudence: consultation of previous rulings

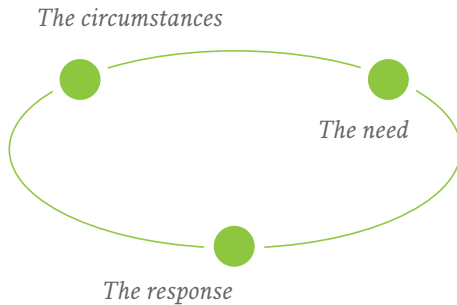
4) In regards to technological development and in the case of a lack of legal judgement on a specific question, the putting into operation of a video-surveillance system must be sure to obey the principles defined by the present charter.

II. The principle of necessity



The installation of a video-surveillance system must be justified

The decision to install a system should be based upon necessity. Necessity can be termed as the adequate balancing of circumstances and needs on one hand and, on the other, the appropriate response, in this case the use of video-surveillance. It is based on this need and these circumstances that the decision can be considered correct and the action necessary. The principle of necessity requires a clear demonstration of the reasoning behind an action, thereby justifying it. It is upon this principle of necessity that depends the decision to install a video-surveillance system. Necessity can be considered prescriptive, as it renders actions imperative, in the sense that there is no other measure that can attain the same goal as effectively.



The conjunction between the circumstances and the need necessitate the response.

RECOMMENDATIONS AND FORMS OF ACTION

A- THE CIRCUMSTANCES

- Precisely identify the security and crime prevention problems present in a defined area through an audit of the issues to be addressed;
- Establish the range of local resources available and existing systems capable of responding to the problems thrown up by the audit;

B- THE NEED

- Draw out the needs exposed by the audit and the analysis of local conditions. The needs should be as precise as possible as they form the basis of the objectives for the project;
- Consider less intrusive possibilities to respond to the problems to be addressed;

C- THE RESPONSE

- The system's objectives must be defined, including an identification of its expected benefits and intended outcomes. These objectives must be translated into operating methods. For example, it is necessary to outline the functional implications of a video-surveillance system whose objective is crime prevention.
- Establish what sort of system could realistically allow a city to achieve its objectives. This system should be set up in an appropriate manner to meet efficiently the identified needs;
- Video-surveillance should only be employed when other, less invasive, available measures are shown to be insufficient or inapplicable (following a considered evaluation) or where the problem to be solved is beyond the means of existing measures. In any event, video-surveillance must form part of a coordinated response to an identified problem.
- Allow the possibility of withdrawal. Cities should be able to decide, on the basis of evaluation, that video-surveillance is no longer necessary or that cameras could, on the basis of analysis, be relocated;

- Data protection

Images recorded through video-surveillance constitute personal data and as such should come under the same level of protection as is applied to all other forms of personal data. This means that strict rules should be adhered to, covering the recording, retention, disclosure and ultimate disposal of such images. It is important to ensure that the objectives are appropriate to:

- The decision to store or not to store images, thus to create or not to create personal data;
- The period for which data should be saved, which should always be temporary. The period of data conservation should be limited to that which is strictly necessary, outlined and defined in the system's setup;
- The physical and technical protection of data. Define the protocols governing access and transmission of images. It is important to include in these protocols the "Privacy by design" method, which encourages personal data protection to be considered at the early stages of the system design.

- Video-surveillance should strike a balance and take its place within an integrated public security and crime-prevention strategy. Video-surveillance is only one tool within a broad, global security policy and its use should be in collaboration with other responses. It is in this way that it can be applied most efficiently.

IV - The principle of transparency

Every authority employing a video-surveillance system must have a clear and coherent policy regarding the operation of their system

The notion of transparency is closely linked to communication. Transparency can be defined as visibility from the exterior. This principle is thus significantly based on the information made available. It is an essential principle as, if video-surveillance can be considered a technology that restricts liberties, it should be accompanied by thorough public information. All information displayed around the system, respecting legislation in vigour, would be in line with this principle of transparency.

RECOMMENDATIONS AND FORMS OF ACTION

- The authority installing video-surveillance cameras should give citizens clear information on:
 - the project to install a video-surveillance system
 - the objectives of the system;
 - the costs of the system;
 - the zones being surveyed. In order to achieve this, it is necessary to use visible and recognisable signage, with symbols;
 - the contact details of the department that can be contacted for more information. This information should feature on the sign displayed in surveyed zones;
 - the specific measures in place to protect images recorded;
 - access to data created by a video-surveillance system should be restricted through password-protection. This data should only be used for the ends set out, by authorised persons and saved only for the necessary time. All use of these images should be recorded in a register to be kept up to date;
 - the authorities that can make use of the images recorded;
 - their rights concerning images of their own person, specifically:
 - The right to access one's own image (without prejudicing another's rights). This right can be refused in the case of judicial process or when linked to risks to national security or defence;
 - The right to confirm the deletion of one's own personal images once the deadline for deletion has been reached;

The information mentioned above must be provided in an intelligible way, using clear and easily comprehensible language.

- The authority responsible for the system should regularly inform citizens of results and the achieving of objectives, through the normal means by which such an Authority reports on its public security and crime strategy. This approach encourages the clear definition of objectives, and ongoing evaluation of performance against previously defined indicators;
- It is discouraged to make use of false cameras. This misinformation is liable to discredit the system and bring its managers into question.

V - The principle of accountability

The right to surveillance of public areas is reserved to carefully limited authorities. These authorities are responsible for the systems installed in their name.

The authorities in charge of video-surveillance systems are the guarantors of a use that is legal and respects privacy and fundamental liberties. They would therefore be responsible for any breaches or violations reported. The administrative authorities with the competence to deal with these problems should be clearly identified. Video-surveillance systems owned and operated by private companies which cover public areas must operate to the same standard as systems operated by public authorities.

RECOMMENDATIONS AND FORMS OF ACTION

- Communicate the contact details of those responsible for the system. Each sign indicating a surveyed zone could also display this information;
- Affirm the system managers' obligation to ensure confidentiality. This obligation could be enshrined in an internal code or in a code addressed to the system managers. Their responsibility could be challenged in the event of breaches of this obligation;
- Employment of suitable security measures to protect access to the system's control room and stored images. Technical measures to control access should be put in place;
- Make known the means for judicial pursuit of suspected abuses;
- Establish an appropriate mechanism to publish information required by citizens to understand properly the use of video-surveillance.

VI - The principle of independent oversight

Checks and measures should be put in place to maintain the correct functioning of the video-surveillance systems through a process of independent oversight.

The notion of control presupposes the definition of established norms and standards. The principle of independent oversight guarantees the continued application of those standards set out by the Charter. The process of independent oversight can take numerous forms and be applied at various points in the development of the systems. The independent scrutiny might be carried out by a qualified individual or a specific body, including citizen participation.

RECOMMENDATIONS AND FORMS OF ACTION

- It is recommended that this independent authority provide, following consideration, the authorisation to install a video-surveillance system;
- This independent authority should also be charged with ensuring that the installation and use of the system complies with the defined rules and standards.

VII - The principle of citizen participation

All must be done to encourage citizen involvement at every stage in the video-surveillance system's life.

The principle of citizen participation consists of giving citizens a voice, through various forms of consultation, involvement, deliberation and joint decision-making. Every new installation or extension of existing systems should envisage the active participation of the area's inhabitants. Wherever possible, discussion groups or other forms of citizen participation should be organised. Citizen participation improves the chances of success.

RECOMMENDATIONS AND FORMS OF ACTION

- Support citizen participation in the identification of needs in the context of the prior auditing, for example through victimisation studies;
- Encourage initial citizen involvement in the installation of cameras when responding to a specific need. This might take the form of environmental visual audits;
- Seek citizen acceptance of global security projects. It is recommended to organise public information meetings to encourage citizen support for the local authority's holistic public security and crime strategy;
- Encourage citizen involvement in the control and evaluation of the system through satisfaction questionnaires;
- Provide a managed and formal system to give citizens the opportunity to visit the video-surveillance system's control room. These visits should be unannounced. Refusal to allow access must be properly documented and explained (i.e. confidential security operation underway) The rights of third parties should not be compromised by this opportunity ;
- Reinforce the local authority's engagement to set up a system allowing regular citizen involvement. The creation of a local control and oversight structure should include active citizen participation in the system's life and development.

>>> Future plans

The cities having signed this charter shall make every effort to ensure its application and the dissemination of its principles in their local or national contexts.

They are committed to continued exchanges regarding developments in the field and technological evolutions.

They wish for a European label and certification to be put in place.

They support the idea of creating a common language of video-surveillance for European citizens that would translate into the creation of a European sign to indicate surveyed zones.



Panel type *Dome*



Panel type *Camera*



Key:

A : Zone *picto*

B : Zone text "*Videosurveillance*"

C : Zone text "*Legal and ethical information*"

D : Zone text "*Public space*"