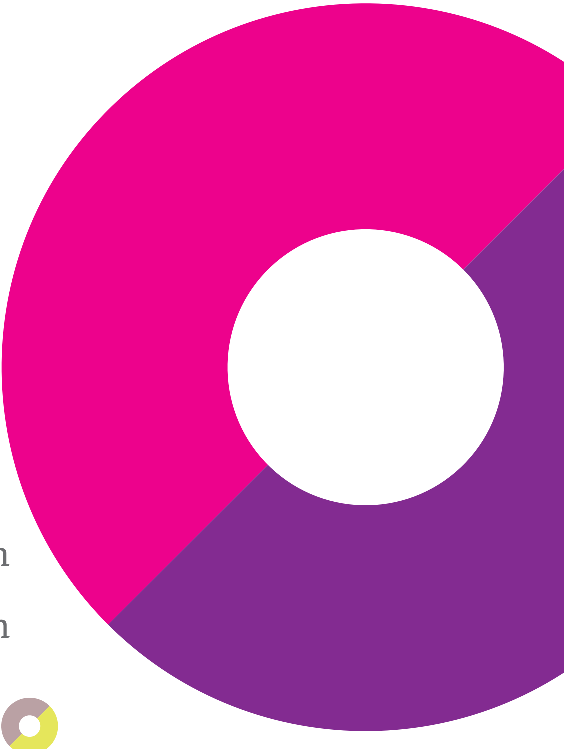


European
Forum *for*
Urban
Security

Citizens, Cities and Video Surveillance

What price are we willing to pay for a society that holds security as a fundamental value? The increasing use of CCTV to watch over all kinds of public areas infringes on our individual right to anonymity. The European Convention on Human Rights invites us to demand that public authorities justify such an infringement. Furthermore, it is necessary to clarify how cameras and images are used. ➤

Co-financed by the European Commission/
Fundamental Rights and Citizenship
Programme

European
Forum *for*
Urban
Security

Citizens, Cities and Video Surveillance

*Towards a democratic and
responsible use of CCTV*

This publication is the fruit of the collaboration of all the partners of the “Citizens, cities and video surveillance”-project. It was edited by the European Forum for Urban Security, Roxana Calfa, Sebastian Sperber and Nathalie Bourgeois.

Translation: Helga Birkle, Jara Campelo, Charlotte Combe, Kerstin Elsner, Nathalie Elson, Gianfranca Gabbai, John Tyler Tuttle.

Art direction: Pete Jeffs & Marie Aumont

Printed in June 2010
by STIPA - Montreuil
NºISBN : 2-913181-37-6
NºEAN : 9782913181373

European Forum for Urban Security
10 rue des Montibœufs, Paris 75020, France
Tél : + 33 (0) 1 40 64 49 00
fax : + 33 (0) 1 40 64 49 10
www.efus.eu
contact@efus.eu

The "Citizens, cities and video surveillance"-project including this publication was made possible through the financial support of the European Commission Directorate General Justice, Freedom and Security /Fundamental Rights and Citizenship Programme.

However it only reflects the views of the authors. The European Commission cannot be held responsible for either its content or for any use which might be made of the information contained therein.

Acknowledgments

This project and the publication would not have been possible without the dedication of the representatives of the project partners, the cities, regions and police authorities. We would like to thank them for having brought this project to life.
Special thanks go to the experts for their valuable contributions, to the hosts of the various meetings, study visits and the final conference as well as to all those who we had the pleasure to meet and hear during the project.

Project partners:
Catherine Schlitz, Christian Beaupere, Guy Geraerts, Serge Lodrini (Liège, Belgium), Bertrand Binctin, Christophe Bois (Le Havre, France), Charles Gautier, Dominique Talledec, Eric Fossembas (Saint-Herblain, France), Rossella Selmini, Gian Guido Nobili (Emilia Romagna region, Italy), Francesco Scidone, Mariapia Verdona, Marcelo Sasso, Marco Morelli (Genoa, Italy), Giorgio Vigo (Veneto region, Italy), Ahmed Aboutaleb, Ineke Nierstrazs, Afke Besselink, Niels Witterholt, Nienke Riemersma, Wilco Mastenbroek, Linda Ouwerling, Ciska Scheidel (Rotterdam, Netherlands), Manuel Ayala Garcia, Juan-Jose Ferrer Planells, Tomas Paris *(Ibiza, Spain),* Christopher Ambler, Roger Fox (Sussex Police, United Kingdom), Andrew Bayes, James Farrell (London Metropolitan Police Service, United Kingdom).

Associated partners:
Stanislav Jaburek, Lenka Stepankova (Brno, Czech Republic), Béla Danielisz, Gabor Gulyas, Zoltan Nemeth, Krisztina Szego (Budapest, Hungary).

Experts:
Benjamin Goold (University of British Columbia, Canada/Oxford University, United Kingdom), Jeroen Van Den Hoven (Technical University of Delft, Netherlands), Laurent Lim (CNIL, France), Maye Seck (French Forum for Urban Security, France), Peter Squires (University of Brighton, United Kingdom), Eric Töpfer (Technical University of Berlin, Germany).

Other speakers/personalities met:
Alessandra Risso, Gianluca Saba, Yuri Piccione, Rinaldo Sironi, Valerio Piazzi, Piero Anchini, Amerigo Alunno, Dario Messina, Furio Truzz (Genoa, Italy), Graeme Gerrad, Brian Watkinson, Dave Hinton, Ken Crawley, Mick Neville, Isabella Sankey, (London/Brighton, United Kingdom), Isabelle Mercier, Didier Delorme, Emmanuel Magne, Georges Pasini, Louis-Jean Despres, Mr. Pareja, Jacques Signourel, Patrick Aujogue, Thierry Dussauze, Jacques Comby (Lyon, France), József Schmidt, Attila Cserép, Richárd Schranz, Péter Rózsas, Endre Szabo, Tivadar Hüttl, Tomáš Koníček, Klára Svobodová (Budapest, Hungary), R.V. de Mulder, Laurie Bush, Zsuzsanna Belényessy, Sylvie Murengerantwari, Caroline Atas (Rotterdam, Netherlands).

Contents

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

Part I – The challenge: Reconciling the use of CCTV and individual liberties

Part II– Towards a Charter for the democratic use of CCTV in European cities

Part III– Zoom on the cities: How they use CCTV and how they protect fundamental rights and liberties

Foreword

➤ Cities are becoming more crowded, offering ever more opportunities for mobility, culture and education, which in turn require a vast range of increasingly complex and costly facilities. Traffic flows overlap. A relentless commercial show-off excites the public's desires. Round-the-clock human surveillance is no longer possible due to the high costs, but the development of electronics in the capitalisation of information and their crossover, with the provision of tools that can be either preventive or dissuasive, is leading to a general increase of the number of cameras watching over spaces dedicated to transport, public gatherings, and shopping centres. The prevention of technical incidents is the predominant reason for the installation of cameras, the images from which are both looked at directly and also, increasingly often, analysed using software. Preserving the integrity of these facilities is the second priority of these installations; misuse and intentional damage require rapid interventions for certain equipment, the functioning of which might affect thousands of people. The third motivation behind these installations is compensating for the reduction in the human workforce responsible for operating the equipment. It is for all of these reasons that our cities have become consumers of video surveillance images. The users of these images belong to both the private and public spheres. But a fourth motive has become apparent, and it brings a political twist to the debate. Thanks to CCTV cameras we can stop criminals from operating in the streets, in public spaces. This motive is borne out of a negative acknowledgement concerning the efficiency of the police services. Thus, increasing the number of cases solved would deter would-be criminals to commit a crime. This maxim for a liberal-leaning criminology asserts the principle that if criminals feel certain they will be caught, then they will abstain from commiting a crime. Hence, the twofold argument used in official texts: video cameras contribute to prevention and help to arrest criminals. Perhaps, perhaps... But is it worth it? Studies do not show a clear reduction in crime: they show arrests in some criminal cases, justifying in-depth studies, but the desired mass effect has not materialised. And this is a worry. To achieve at least the second objective, and perhaps even the first, cameras need to be placed throughout the entire city because crimes are evenly spread out in urban areas. If we cross this threshold by saturating public space with cameras, we are on a slippery road towards a society of mistrust, of restrictions of liberties. These questions are being debated throughout Europe.What price do we want to pay for a society that holds security as a fundamental value? A French parliamentary report has recently been published following a series of natural disasters. Its main conclusion is that perhaps we should think about re-introducing a “culture of risk” among citizens. The triumphalism of technology has eliminated the notion of risk from the consciences of citizens. What about letting them know that despite the wonders of technology, they must continue to live in a situation of risk? Is this not the same question that could be asked with regard to crime? There is no such thing as a safe, crimeless society, and any methods that purport to eliminate all risk should be rejected by responsible citizens. The increasing number of cameras watching over public spaces infringes on our individual right to anonymity. Public authorities have a duty to justify this infringement. The European Convention on Human Rights invites us to demand such a justification. It is essential in our opinion that the methods of use of cameras and images should be clarified. Such is the aim of the work carried out by practitioners and experts with the support of the Forum.

Michel Marcus
Executive Director
European Forum for Urban Security

Introduction

Video surveillance on the rise

➤ The first decade of the 21st century began under the sign of an event that will have marked minds and practices. The attacks of 11 September 2001 imposed **security** as a priority on the world agenda. Since then, a plethora of means deemed useful in the fight against terrorism, including video surveillance, has been deployed at all levels. The questions of their effectiveness, of the appropriateness of the instruments used and their impact on freedoms in relation to objectives, especially over the long term, were secondary.

Terrorist attacks had been committed well before 2001 but had never attained this global dimension brought out by the media. It is no coincidence that the European nation that has experienced this in the most regular and prolonged way—the United Kingdom—is the one that has sought most to develop all possible responses, in terms of prevention as much as resilience.

The choice of technology for facing up to the growing demand for security on behalf of citizens has found its justification in the events of 11 September 2001, like those of 11 March 2004 in Madrid and 7 July 2005 in London. Since then, recourse to technology has continued to grow in all the other European countries.

Yet, like the impressive images presented merely a few hours after the London attacks showing how the presumed terrorists arrived on the scene of the crime, the 2008 declaration by the person in charge of London's video surveillance, describing it as a fiasco, went round the world. Once the emotion of the events had passed, it was advisable to question oneself as to the pertinence of the use of technology in preventive actions, its effectiveness and also the advantages and disadvantages ensuing from its use.

These questions are as topical in the countries that envisage resorting to more video surveillance, such as France decided in 2008, as in those that are already quite advanced in the use of this technology, such as the United Kingdom. For the past 25 years, the United Kingdom has experienced an exponential increase in these technologies and is now the world leader in the use of video surveillance. However, over the past few years, numerous voices have been raised to challenge the validity of 'complete video surveillance' and to learn the lessons from the experience. The British are now carrying out thinking on their systems and in particular the way of using them[1]. Thus, the new Deputy-Prime Minister, Nick Clegg, recently announced that the government was going to prepare a new law for the protection of fundamental rights. In a press conference on 19 May 2010, he declared: "*This government will end the culture of spying on its citizens. It is outrageous that decent, law-abiding people are regularly treated as if they have got something to hide….Video surveillance is going to be the object of custom-made laws…*''[2]

This questioning becomes all the more topical for European cities as technology is invited into the elaboration of local and regional security policies. Town councillors must both respond to their electors' demands for security and justify the choice of instruments they set up, out of concern for transparency and a democratic exercise of the decision-making process. By admitting that technology is the response considered most appropriate by states for

[1] National Strategy for Video Surveillance - 2008

[2] Deputy Prime Minister – Speech and Q&A – 19/05/2010, London

fighting against threats such as terrorism, what about the local level for crime prevention? Most European cities and regions are confronted with everyday crime, the effects of which are not as spectacular as those of a terrorist attack but which nonetheless challenge the overall well-being on a territory and can harm its sustainable development. They are therefore led to consider any instrument that might help them to guarantee the security of their citizens and cannot ignore the potential assets of technology.

Although it is true that citizens give a mandate to elected officials to ensure their security, they also invest them with their trust so that security choices not be made to the detriment of the respect for rights and liberties guaranteed by the law. This trust also presupposes that the authorities assume responsibility for the choice and the transparent use of the instruments employed for security ends.

The right to security, the right to protection of one's private life? Is there an order of priority? Does one prevail over the other? In theory, citizens should be able to enjoy both without having to choose between them. The two go hand in hand in a democratic society and are guaranteed equally as much by the national legislative frameworks as by international texts such as the Council of Europe's Convention on Human Rights (1950) or the European Union's Charter of Fundamental Rights (2000). Yet, in practice, the reconciliation of security and freedoms is far from being evident. Liberty is a weak right, which is easily relativised in face of problems of insecurity. Video surveillance is a technology that raises many questions in this sense. What can be filmed? Is there a right to private life in public areas? And if so, how to protect that right? How to avoid discriminating against certain groups and how to put the advantages of this surveillance tool at the disposal of the whole population? How to ensure that video surveillance works and when to resort to other instruments? When is it effective in a cost-benefits ratio? How to protect personal data and how not to produce it needlessly? How to use video surveillance with citizens as a crime prevention tool and guarantee of public peace?

Thought and exchange of experiences on video surveillance practices in the respect and protection of individual freedoms

It was to respond to all these questions and identify good practices that this European project 'Citizens, Cities and Video Surveillance' came into being. This reflection was able to be developed thanks to the involvement of ten partners, namely the cities of Le Havre and Saint-Herblain (France), Rotterdam (Netherlands), Liège (Belgium), Ibiza (Spain), Genoa, the Veneto and Emilia-Romagna regions (Italy), the police of London and Sussex (United Kingdom), as well as European experts. The project received financial support from the European Commission ('Fundamental Rights and Citizenship' programme).

The project aimed at providing cities with the necessary knowledge and tools for setting up an integrated security policy in which social realities and freedoms are taken into account in the same way as public peace.

To meet the challenges posed by video surveillance in terms of rights and freedoms, the partners set as a specific goal going more deeply into the fundamental question of the responsibility of the elected official who must find a balance between the demand for security and the strategic choices enabling him to respond in a democratic manner.

As the title of the project indicates, the citizens are at the heart of local policies. Therefore, it was necessary to pay particular attention to taking them into account in the setting-up or evaluation of video surveillance arrangements. In fact, insofar as these arrangements are intended above all to serve the citizens, the latter must be not only consulted as to their expectations and needs in terms of security but must also be fully informed as to the functioning, costs and benefits of these new tools. The partners therefore examined how to take these issues into account at all stages of the implementation of a video surveillance project, from installation to evaluation, by way of functioning, and they discussed and proposed alternate or complementary solutions.

Furthermore, the ambition of this partnership of cities, regions, municipal and regional police was to formulate a *Charter for the Democratic Use of Video Surveillance*, i.e., in accordance with fundamental rights. The eventual objective is to implement this Charter and define a label that identifies the cities respecting its principles and recommendations.

The underlying idea of this joint approach is also to establish a common language on video surveillance in Europe, accessible to, and comprehensible by, all. This is a necessary approach to ensure transparency of political decision-making.

Cities helping cities…

The methodology of the project is based on the fundamental mission of the European Forum for Urban Security: '*Cities helping cities*'. The cities, regions and police authorities hope to improve their system by sharing their experiences and drawing information from them. This exchange has been enriched and supplemented by contributions from experts such as the French Forum for Urban Security, a number of professors from major universities and high-ranking civil servants who allowed for enriching the discussion and making the link between research and practices. The experiences of each partner were analysed according to an analytical grid. These exchanges of practices and know-how were given concrete expression in the form of the *Charter for the Democratic Use of Video Surveillance*.

...to create a Charter for the Democratic Use of Video Surveillance in the framework of a European cooperation

Beginning with the project's kick-off meeting, held in Paris in April 2009, the wealth of experiences and diversity of situations presented by the partners came out. Technical diversity first of all, with notable differences concerning the number of cameras (from four to 60,000!), as well as the types of camera and their functionality or geographical coverage. Diversity, too, of political contexts: which authorities can decide to install cameras on the public land; which operators can be the managers; which persons are authorised to pass on information and those who can be the consignees; what legal framework, what debates on video surveillance at the national and local levels (see Part III of this publication). Diversity, too, in terms of legibility and perception of video surveillance by the citizens of the project's partner cities: favourable with some, distrust and reservations with others, which induces different levels of public debate on the use of cameras and the protection of fundamental rights. Diversity of situations and legislations finally, which brought out the difficulty of reaching an agreement on the project's field of application: video surveillance solely on the public land? How to treat semi-public lands or private spaces for public use? The chosen approach was to concentrate on the public spaces for which all the partners are competent without, for all that, losing sight of video surveillance systems on semi-public land, which represent a very large portion of existing systems and for which the project's conclusions could also be a source of inspiration.

The project's first objective was to have an overall view of video surveillance practices and the measures taken for protecting the private life of citizens. The analytical grids of the practices of the project's partners allowed for seeing how data protection was integrated into the different phases of the life of a video surveillance system, namely the analysis of needs, installation, management and evaluation.
To complete this overview and to have a common understanding of the problem, the project partners benefited, as of the first work seminar, which took place in Le Havre 3 and 4 June 2009, from the contribution of experts coming from different sectors—legal, political/sociological, technical, philosophical—and representatives of human rights protection NGOs and police associations.

Experts and professionals were in agreement on the principal challenges of video surveillance on public spaces, which would be:

➤ on the one hand, finding a way to preserve the social codes of intimacy on the public land in a video surveillance framework. This theme is developed in this book by Benjamin Goold. It is also present in the jurisprudence of the European Court of Human

Rights in Strasbourg focussing on complaints against 'paparazzi';

➤ on the other hand, finding a good balance in terms of the cost-benefits ratio between the price that people are willing to pay by giving up, to a certain point, their intimacy and the benefits that they obtain thanks to increased security. Which means that decisions would be made in full awareness of consequences.

➤ Breaches of respect of one's intimacy are not perceived by the citizen as being terribly important. However, when all is said and done, the sum of every little intrusion in a citizen's private life can take on considerable proportions, and this trend is increased tenfold with every technological development. The protection of private life on the public land stems from the political authority, and the players concerned should be given a share in this approach. So it was necessary to take into account the protection of data and individual freedoms at every level of video surveillance use.

Secondly, the project allowed for seeing video surveillance practices in detail during in-situ visits organised by three partners of the project: the city of Genoa (Italy), the Metropolitan Police of London and the police of Sussex (United Kingdom) and Lyon (France), an associate city in the project.

First of all, these visits allowed for obtaining detailed knowledge on the use of video surveillance, seeing in the field the way a system is run and having exchanges with diverse stakeholders about the problems and assets of this technology.

The study visit to London and Brighton allowed, in particular, for obtaining information on the English experience with video surveillance, integrated as an investigation instrument in criminology, and becoming aware of the debates that are current in the United Kingdom as to its impact on private life, thanks to meetings with experts employed by the government in the anti-terrorist fight and militants of NGOs like Liberty.

The visit to Genoa illustrated the reality of an Italian city where several video surveillance systems are in operation, run by different institutions. Here, the challenge is the sharing of information: just how far and under what conditions?

The visit to Lyon allowed especially for understanding the approach of a city that had already accompanied its video surveillance system with a charter of ethics and which had also set up a college of ethics in charge of overseeing the system.

These study visits also showed how cities and regions use video surveillance in different ways, in relation to the objectives they are pursuing, and in what ways the management protocols, communication, the public cameras-private cameras ratio and the attitude of citizens, ranging from support to opposition, vary. It clearly came out that the impact of video surveillance varies according to the nature and size of the areas under surveillance, the type of offence and the possible combination of this technology with other prevention measures.

These visits also allowed for identifying a certain number of arrangements and measures put in place to guarantee the protection of the citizens' private life, including the special parametrising of cameras, the training of operators on the legal framework governing data protection, the 'proper use' charters where cities agree to respect fundamental rights, and independent supervision systems.

The perspective contributed by the experts, the on-site visits, the meetings with local professionals, and the analytical grids describing partners' practices subsequently served as a basis for discussions for the two working seminars that were held in Budapest, 2 and 3 December 2009, and in Bologna, 11 and 12 March 2010.

The Budapest seminar was first of all the occasion for including Central European practices in the project, with contributions and visits of the city of Budapest, the ombudsman for the protection of data and Hungarian NGOs, and contributions of the city of Brno (Czech Republic) and the Czech Ministry of the Interior. The seminar also illustrated the difficulty of finding a common language reflecting the various problems across Europe, going beyond political divisions to arrive at a common denominator that is not simply an *a minima* agreement of the partners' positions. For example, the notion of an 'ethical' charter, well accepted in France, was not unanimously approved on the European level. The accepted solution of a charter for the 'democratic use' of video surveillance best translated the spirit of the project, which puts citizens at the centre of local policies in a concern for the democratic exercise of elected officials' power of representativeness. The choice between the notions of 'video protection' or 'video surveillance' was also discussed at length.

The debates also focussed on the creation of a label for the implementation of the charter; this label would be intended for cities respecting its principles. Here, too, opinions were mixed: whereas some immediately saw this as the logical continuation of work for the implementation of the charter, others were more doubtful as to the idea of being auditioned to receive this label. That said, the idea was not to create a label in the framework of this project but simply to study its feasibility.

The Bologna seminar served to identify the charter's key principles, stated at every phase of the system's life. The challenge was to find independent but complementary principles, which, together, would characterise a democratic use of video surveillance.

This was also the occasion for proposing an initiative going towards the creation of a common video surveillance language across Europe: the creation of a common, standardised means of signalling, which might get a clear, complete message across to any citizen across Europe. Several discussions focussed on the indispensable information that such a means of signalling should include in light of what already exists in the cities and countries represented in the project.

The definition of the seven federating principles that are at heart of the *Charter for the Democratic Use of Video Surveillance*, as well as explanatory comments accompanying them, were written by the partners during joint work at the final seminar, which took place in Paris on 9 April 2010.

The project's final conference, hosted by the city of Rotterdam 27 and 28 May 2010, marked both the final outcome of the partners' 18 months of work and the recognition of the town councillors' responsibility in the use of video surveillance. By becoming the Charter's first signatories, the mayors of Rotterdam, Ahmed Aboutaleb, and Saint-Herblain, Charles Gautier, also senator and president of the French Forum for Urban Security, thereby reaffirmed that town councillors are responsible before the citizens for the tools they choose for implementing their policy, and that they also have an obligation of transparency. Moreover, they both invited the other European cities to sign the charter.

This publication therefore reflects this long work, which enabled the project's ten European partners to share the points of view of experts from various countries in Europe, exchange practices tested by the cities, discuss stakes and challenges of video surveillance as regards the respect of private life and, finally, formulate together proposals of responses.

Part I

➤ *The challenge: Reconciling the use of CCTV and individual liberties*

CCTV and Human Rights

Benjamin J. Goold
University of British Columbia

➤ Over the past twenty years, the use of CCTV cameras has become increasingly common throughout Europe. Although countries like France, Germany, Holland and Italy were initially slow to follow the United Kingdom's lead, CCTV systems are now being installed in towns and cities across the continent, with the result that public area surveillance is an inescapable fact of life for a growing number of Europeans. Although it appears that there is considerable public support for the use of CCTV, the spread of this technology has serious implications for civil liberties and the relationship between citizens and the state. In particular, CCTV cameras represent a substantial threat to individual privacy and to the exercise of rights such as freedom of expression and freedom of association. As a consequence, it is vital that those responsible for the management and operation of these systems are aware of the dangers of public area surveillance, and that they work to ensure that CCTV does not threaten fundamental human rights.

This chapter provides a brief overview of the human rights implications of CCTV surveillance, and aims to help CCTV managers and operators develop public area surveillance policies and practices that are consistent with a commitment to the protection of individual rights and a respect for civil liberties.

CCTV and Privacy

All of us need a degree of privacy. Without it, it would be impossible to maintain a sense of dignity, develop meaningful relationships with others, or simply find time to be alone with our thoughts. Privacy is crucial to the development of the self because it frees us from having to worry about being constantly watched and judged by those around us, and it enables us to control how and when we share information about ourselves with others.[1] It is for these reasons that most countries recognize at least some basic right to privacy, and limit the ability of individuals, private organizations, and the state to collect information about people's personal lives, or to monitor them without their knowledge or consent.[2]

It is important to recognize that the right to privacy does not disappear as soon as we step outside our homes. Although no sensible person would expect to enjoy the same level of privacy in the street as they would in their own living room, most of us do expect to enjoy a certain degree of privacy and anonymity as we go about our business in public. Indeed, one of the great joys of living in cities is the ability to lose oneself in the crowd, and to be free of the demands of our families, friends, and colleagues. In part, it is this promise of anonymity and the freedom that goes with it that attracts many people to town and city streets. Equally, although few would expect to meet a friend at a restaurant or a coffee shop and be entirely free from scrutiny, there are strong social conventions that help us to enjoy a reasonable level of privacy in such circumstances. While nowhere near as extensive as in such obviously private spaces as the home or car, it is clear that we do have a right to some privacy in public.[3]

By its very nature, public area CCTV undermines this right. By exposing us to scrutiny every time we walk down the street, cameras strip us of the possibility of anonymity and make us visible to the watchful eye of the state. While we obviously surrender a great deal of privacy every time we go out in public, it is still no defense for users of CCTV to point out that other members of the public are also watching us. Being watched – and possibly recorded – by a camera is different from being looked at by a stranger. The former type of observation is typically longer, more intense, and intimately connected with the power of the state. Because we cannot see or question the person behind the camera, it is hard for us to know how to respond to being watched, or to decide what we should do about it. Because we cannot know whether the images captured by the cameras will be kept or who might have access to them, we cannot be sure that they will not be misinterpreted or used in objectionable ways. As philosopher and criminologist Andrew von Hirsch has observed, being watched by CCTV "is like conducting one's activities in a space with a one-way mirror; while one may know that someone is watching behind the mirror, one does not necessarily know who they are or what they are looking for."[4]

[1] For an overview of the different theories of privacy, see: Solove, D.J. (2002), "Conceptualizing Privacy", California Law Review 90: 1087-1155; Solove, D.J. (2009) Understanding Privacy (Harvard University Press: Cambridge, Mass.); and Nissenbaum, H. (2010), Privacy in Context (Stanford University Press: Stanford, California)..

[2] One of the clearest assertions of the right can be found in Article 8 of the European Convention on Human Rights, which states that: "Everyone has the right to respect for his private and family life, his home and his correspondence."

[3] See: **Goold, B.J.** (2002), "Privacy Rights and Public Spaces: CCTV and the Problem of the 'Unobservable Observer'", *Criminal Justice Ethics* 21(1) Winter/Spring; and Goold, B.J. (2008) "The Difference between Lonely Old Ladies and CCTV Cameras: A Response to Jesper Ryberg", Res Publica (March).

Aside from the obvious intrusion, it is this uncertainty that poses one of the greatest threats to our experience of privacy in public. Faced with the prospect of constant video surveillance, it is reasonable to expect that some members of the public will feel the loss of privacy keenly and change how they behave; not because they believe they are doing anything wrong, but because they don't want to be the subject of police attention or risk having their actions misinterpreted. This is likely to be especially true for young people and certain minorities, who may already feel unfairly targeted by the police and local governments. As Giovanni Buttarelli, the Assistant European Data Protection Supervisor has argued:

"*Being watched changes the way we behave. Indeed, when watched, many of us might censor our speech and our behaviour. This is certainly the case with widespread or continuous surveillance. Knowing that every move and gesture is monitored by a camera may have a psychological impact and change behaviours. This constitutes an interference with our privacy.*"[5]

How should operators and managers of CCTV systems seek to ensure that the use of public area surveillance does not fundamentally undermine the right to privacy or negatively change the way in which people enjoy public spaces? First and foremost, it is essential for such systems to be operated in accordance with local and national laws, and every effort must be made to prevent abuse of the cameras and breaches in system security. Secondly, the cameras should only be used for those purposes originally identified when the decision to install them was taken: gradual "function creep" must be avoided. Finally, systems must be open and transparent, and those responsible for running them directly accountable to the public. Although the installation of surveillance cameras in public places will inevitably have a negative effect on individual privacy, by ensuring that the above steps are taken CCTV operators and managers can help to minimize the loss of privacy and ensure surveillance is both lawful and appropriate.

CCTV, Freedom of Expression, and Freedom of Association

Although it is clear that CCTV cameras have serious implications for privacy, the use of public area surveillance technologies by the police and local governments can also undermine other fundamental human rights. In particular, CCTV surveillance has the potential to discourage people from exercising their rights to freedom of expression and freedom of association in public places. Both of these rights are essential to the idea of democratic self-government, and must be protected in order to ensure that individuals are free to organize themselves politically, criticize the decisions of their elected representatives, and hold their government to account. If citizens know that they may be captured on video every time they attend a public rally or take part in a protest march, then there is a very real danger that the presence of CCTV cameras could have a substantial chilling effect on these rights, eventually leading to a reduction in political freedom and democratic partici-

[4] **von Hirsch, A.** (2000), "The Ethics of Public Television Surveillance" in von Hirsch, A., Garland, D. and Wakefield, A. (eds.) *Ethical and Social Perspectives on Situational Crime Prevention* (Hart Publishing: Oxford)

[5] "Legal Restrictions – Surveillance and Fundamental Rights", Speech delivered by the Assistant European Data Protection Supervisor Giovanni Buttarelli at the Palace of Justice, Vienna, June 19th 2009 (availableat: www edps.europa.eu/.../site/.../09-06-19_Vienna_surveillance_EN.pdf)

pation.[6] This is a point that was recently acknowledged by the U.S. Department of Homeland Security in a privacy impact assessment of a CCTV system operated by U.S. Immigration and Customs:

"*Cameras may give the government records of what individuals say, do, and read in the public arena, for example documenting the individuals at a particular rally or the associations between individuals. This may chill constitutionally protected expression and association.*"[7]

Given the potential threat to freedom of expression and association, it is important that CCTV is only used to prevent crime and promote public safety, and never for the purpose of gathering information about the political views or activities of citizens. Where, for example, the police plan to use CCTV to monitor a protest march in their efforts to maintain order or prevent violence, they must be careful not to retain any images of individuals unless they are to be used as evidence in a criminal investigation. Similarly, where images of a person are recorded with a view to prosecuting him or her for a criminal offence, these images should not be subsequently passed on to security services or other law enforcement agencies unless there is a compelling reason to do so.

In addition to these restrictions, the police and other users of public area CCTV must ensure that the public are fully informed about the purposes, operation, and regulation of the systems. If the chilling effects of surveillance are to be avoided, it is not enough to restrict the use of CCTV and adopt robust privacy protections. The public must also be able to trust that the systems will not be abused, and that over time they will not be used for political purposes. This is especially important in countries that have only recently made the transition to democracy, and where memories of political repression are likely to be relatively fresh. Trust in the police and government is hard won and easily lost, and it is not difficult to see how the misuse of CCTV for political or some other illegitimate purpose could seriously undermine that trust.

Reconciling Safety, Security, and Rights

"*There are indeed circumstances when it is legitimate and necessary to sacrifice privacy and other fundamental rights to a certain degree, in the interest of security. Our society must be able to defend itself in the best way against threats. However, the burden of proof must always be on those who claim that such sacrifices are necessary and the proposed measures are all effective instruments to protect society.*"

Giovanni Buttarelli, Assistant European Data Protection Supervisor, Vienna, June 2009[8]

One of the most difficult questions society faces is how best to reconcile the public's demand for safety and security with the need to respect and protect individual rights. Although CCTV cameras in public

[6] As Keith Boone has argued, privacy is "vital to a democratic society [because] it underwrites the freedom to vote, to hold political discussions, and to associate freely away from the glare of the public eye and without fear of reprisal." As a consequence, where surveillance threatens privacy it also threatens political freedom. See Boone, C. K.

[7] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Livewave CCTV System* (September 17, 2009). This point has also been made by Buttarelli, who notes that: "CCTV may discourage legitimate behaviour such as political protests supporting unpopular causes. Participants traditionally had the right to anonymously participate in a peaceful assembly, free of risk of identification and repercussions. This is fundamentally changing." See: "Legal Restrictions – Surveillance and Fundamental Rights", Speech delivered by the Assistant European Data Protection Supervisor Giovanni Buttarelli at the Palace of Justice, Vienna, June 19th 2009, p. 8.

places like streets and city centers can play a major role in reducing crime and disorder, they can also constitute a serious threat to individual and political rights. As a consequence, it is vital that the police and other users of CCTV keep the following in mind when engaging in any form of public area surveillance:

➤ *CCTV surveillance inevitably infringes an individual's right to privacy*
As a consequence, it is for the police and local governments to ensure that they can provide a convincing and lawful justification for the use of cameras in public spaces, and that they develop systems of control and accountability that seek to minimize the negative effects of surveillance on individual privacy

➤ *CCTV surveillance poses a significant threat to the exercise of political freedom*
Because state-sponsored surveillance of public spaces and events has the potential to seriously undermine the ability and willingness of individuals to exercise their rights to freedom of expression and association, CCTV must never be used for the purpose of collecting information about the political activities or affiliations of citizens. Users of CCTV must be able to guarantee that cameras will not be used for political purposes, or to discourage public assemblies or protests.

➤ *The public must be able to trust the users of CCTV to respect their rights*
Perhaps most important of all, the public must be able to trust users of CCTV to respect their rights, and for that trust to be justified. Even if CCTV is not being misused, if the public believe that their rights are being infringed then the presence of cameras may still undermine trust and confidence in the police and government. It is not enough for the users of CCTV to respect the individual rights; the public must believe that they are committed to protecting privacy and respecting rights to freedom of expression and association.

Operating public area CCTV systems necessarily requires the police and other public bodies to confront one of the most fundamental tensions in modern democratic societies: the competition between the demand for security and our shared commitment to the protection of individual rights. If they are to successfully reconcile these two objectives, then the police and others must first begin by acknowledging that it is the state to justify why it should be allowed to watch its citizens, and not for citizens to have to explain why they shouldn't be watched. As soon as this fundamental truth is forgotten, it is only a matter of time before surveillance begins to place rights in jeopardy.

[8] "Legal Restrictions – Surveillance and Fundamental Rights", Speech delivered by the Assistant European Data Protection Supervisor Giovanni Buttarelli at the Palace of Justice, Vienna, June 19th 2009, p.4 (available at: www.edps.europa.eu/.../site/.../09-06-19_Vienna_surveillance_EN.pdf).

Evaluating CCTV: Lessons from a Surveillance Culture

Peter Squires
Professor of Criminology and Public Policy at the University of Brighton

➤ The deployment of close circuit television (CCTV) surveillance in the UK provides an invaluable learning opportunity for other societies. Even this claim might be a too controversial starting point for some. As Professor Marianne L. Gras has argued in her 2004 paper, *The Legal Regulation of CCTV in Europe*, while the UK may have led Europe in terms of the scale of its CCTV investment, other commentators are not so convinced that the UK's mechanisms of legal and political oversight have kept pace or that the UK model is one to be followed anyway.

For the past twenty years, the British government has been a world leader in CCTV investment. In the bold words of the UK Home Office, "In many ways, we have led the world from its early introduction in the 1970s to the massive growth in CCTV installation and use in the 1990s." Between 1999 and 2003 alone, a total of £170 million (roughly €200 million as of 2010) CCTV funding was made available to local authorities following a competitive bidding process. This led to over 680 CCTV schemes being installed in town centres and other public spaces throughout Great Britain.

Perhaps understandably, with the rapid rolling out of a relatively untried technology, many mistakes were made; lessons were often learned only slowly, and sometimes the hard way, about what CCTV could and could not achieve. Associate Professor at the Faculty of Law of the University of British Columbia, and formerly a lecturer at Oxford, Benjamin Goold went so far as to note in 2004 that, although the

Government was prepared to fund the development of new CCTV systems in many British cities, “it apparently has no great interest in seeing whether they actually work”. Accordingly, CCTV grew very fast in the UK context, rather faster than was justified by any evidence of its impact or effectiveness for CCTV appeared to have only a negligible effect on crime rates in the areas where it had been deployed. Yet, a wholly unrealistic expectation prevailed, sustained in part by an unholy alliance of enthusiastic police entrepreneurs, security industry marketing agents and fearful citizens, that CCTV could solve many of our public area crime and disorder problems.

As a Home Office evaluation from 2005 concluded:
“*[CCTV] was oversold – by successive governments – as the answer to crime problems. Few seeking a share of the available funding saw it as necessary to demonstrate CCTV’s effectiveness... Yet it was rarely obvious why CCTV was the best response to crime in particular circumstances*”.

As other countries increase their levels of CCTV investment, the UK experience can provide useful lessons, significantly improving the process of policy transfer, avoiding mistakes, developing better practice, clarifying issues, and even saving money. It can also make a reality of the promise of “evidence-led” policy development. In an area of policy-making that goes to the heart of questions of state power and security versus citizen privacy and individual rights, the issues surrounding the management, governance and oversight of CCTV systems in the UK can provide a useful basis upon which other societies can plan their own. As the European Forum for Urban Security moves towards the development of a Europe-wide code of practice and ethics for CCTV, the British experience can provide a salutary lesson. In a wider sense, it also bears out an uncomfortable truth of the politics of law and order:. As David Garland pointed out in his 2001 book *The culture of control*, “Crime control strategies ... are not adopted because they are known to solve problems.”

Policies and strategies are often adopted because they are politically expedient, popular, cheap, consistent with existing priorities or favoured by dominant interests. As Stephen Savage (Professor of Criminology and Director of the Institute of Criminal Justice Studies, University of Portsmouth) has noted, much of the law and order politics of the 1990s were fundamentally driven by politics and ideology rather than research. It is as plausible to argue that the various “CCTV challenge” funding competitions organised by the Home Office since the 1990s – and the form that these took, matched funding-bids based upon public/private partnerships - were as much about kick-starting local crime prevention partnerships as they were about funding CCTV itself. It is arguable that the CCTV industry in the UK was a spectacular beneficiary of a unique combination of circumstances and its own slick publicity. We might proceed rather differently a second time around.

At a time when the perceived threats posed by crime, violence, disorder and terrorism are generating new demands for security and when the security industries themselves are sensing lucrative new markets, the research community should do two things:

- to ensure that the measures of crime prevention adopted actually deliver the crime reduction benefits promised,
- to ensure that these measures avoid becoming expensive ways of intensifying an already tense and often dysfunctional law and order politics, for instance by augmenting the powers of the police *vis à vis* the rights of citizens; reinforcing problematic so-

cial boundaries between supposed "innocent citizens" and "others"; demonizing youth and other "visible" public groups; subsidising the security of the affluent and redistributing (displacing) crime risks onto the already vulnerable, and facilitating the emergence of more risk averse and ultimately less accountable public order.

French author and social commentator Loic Wacquant has catalogued such developments in the USA over the past decade and cautions against Europeans following suit, trying to tackle crime and disorder problems by criminal justice and security measures alone. He notes, "Any policy claiming to treat even violent crime solely with the criminal justice apparatus is condemning itself to programmed inefficiency… aggravating the disease it is supposed to cure."

Accordingly, the adoption of CCTV in the UK, while resembling a search for the "magic bullet" cure-all, accompanied by a populist, but ill-informed, wave of public support, does not represent a path one would recommend that any other countries should necessarily or blindly follow. This is not because the technology has simply not delivered the promised benefits (many of these were exaggerated, unrealistic and unreasonable anyway), but rather because the adoption of CCTV begs many other questions about law enforcement and the practice of policing, all of which require serious consideration if this technology is to be effectively integrated into the criminal justice and security infrastructures.

Outside of the UK, citizens and political authorities may answer such questions in quite different ways and they may want CCTV cameras to help solve other problems. This, in a sense, is the very first point. We should ask not: what can CCTV cameras do for us? But rather, what problems do we want to tackle and how might CCTV surveillance help?

Policing perspectives

By 2007, while acknowledging that there was still a "debate" over "how effective CCTV is in reducing and preventing crime", the UK Home Office and the Association of Chief Police Officers (ACPO) were sufficiently forthright to acknowledge that while CCTV has made a contribution to "protecting the public and assisting the police", this had occurred "*despite* CCTV systems being developed in a piecemeal fashion with little strategic direction, control or regulation [and] this approach has failed to maximise the potential of our CCTV infrastructure." This "lack of a coordinated approach to CCTV development," the report continued, "poses significant risks in terms of compatibility of systems, cost of accessing the images and the potential loss of operational effectiveness."

Yet, as we have noted, beyond these essentially operational issues of utility, impact and effectiveness lie many further questions pertaining to democracy, rights, citizenship, oversight, accountability and redress, all of which have a bearing upon public trust and confidence in policing. Societies developing their own CCTV surveillance systems need to consider these matters too, not just the technical questions.

Whereas the police were now willing to acknowledge criticisms that the academic, research and evaluation community had been making for nearly a decade or more, the response has not entailed any unpacking of the complex CCTV systems currently in place. Rather, a "national strategy" has been advanced to address the failings of the hitherto "haphazard and incremental" CCTV expansion of recent years. Of course this would not be the first time that criminal justice policy-makers have called for "more and better" of something to tackle the perceived failings of an earlier, seemingly insufficient, dose of the same solution.

Unsurprisingly perhaps, the British Security Industry Association was having none of it, their spokesperson noting that, while CCTV growth may have been piecemeal, the real faults lay with police forces which had not maximised the potential of their own systems. It seems that, as in other areas of criminal justice, a troubling circularity of thought prevails. Whatever problems are associated with CCTV, more CCTV is the solution, both our police and our security industry seem to agree on this simple fact. The real issue, however, and this is the lesson for other societies, is to try to think outside this particular box – or even beyond the camera.

More recently, enthusiastic support has been voiced for CCTV from another policing source. In his controversial memoir, *The Terrorist Hunters*, former Assistant Commissioner of the Metropolitan Police, Andy Hayman, wrote of the significant contribution that he believed surveillance technologies were making to contemporary policing: “Despite the concerns of civil liberties groups, the surveillance society of CCTV cameras, listening devices and databases recording our e-mail and phone activity, our criminal and car records, and anything else we care to think of, is paying off big time when it comes to catching criminals and terrorists.”

That brief comment, the points it makes explicit and those it doesn’t, connects with so many of the issues which run to the heart of many questions about the role of CCTV in effective public safety management. In the first place Hayman presents the contribution of surveillance technologies “despite the concerns of civil liberties groups” as if there is always an inherent contradiction between policing and freedom. It is not necessarily so, although this debate takes us back to the first establishment of uniformed policing in London. As Robert Peel, founder of the Metropolitan Police in 1829, remarked, “Liberty does not consist in having your house robbed by organised gangs of thieves, and in leaving the principal streets of London in the nightly possession of drunken women and vagabonds. Properly established, appropriately managed and effectively monitored, surveillance can enhance safety, security and freedom.”

Yet Hayman also refers to surveillance technologies *other than CCTV*, making the point that this whole area of policing and security management has changed rapidly during recent years such that the social implications, the law and principles of governance have not always kept pace with the technological potential. Yet, a kind of “mission drift” can occur where technologies are used in ways that were never intended, resulting in costly and inappropriate investment and supposed solutions (“technological fixes”) that are ineffective, leading to scepticism and disillusion when the system does not deliver the anticipated results.

Some of these problems have certainly been true of CCTV use in the UK, for example they also arose in the investigation of the 2005 London suicide bombings “in relation to the lack of [system] integration, the quality of images and the difficulties associated in retrieving digitally recorded footage,” as ACPO has acknowledged. Furthermore, at least one study has concluded that improved street-lighting could have a more significant preventive impact on crimes recorded than CCTV (Farrington and Welsh, 2002) – and street-lighting was much cheaper.

In a related fashion, Hayman talks of the use of surveillance technologies for “*catching* criminals and terrorists" and yet the widespread adoption of public area CCTV surveillance systems in the UK was based upon the cameras' crime prevention potential. CCTV, operating within the paradigm of *situational crime prevention* would, it was assumed, deter offenders by making them visible and identifiable and by bringing the principle of "guardianship" from routine activity theory to otherwise relatively unguarded areas.

Both approaches suggested some connection between surveillance and rational choice, that the fact of being observed and caught on film would influence behaviour and deter offenders from offending. In practice, however, CCTV proved to have relatively little impact on some types of offences, for example inter-personal violence (perhaps due to the influence of alcohol). In fact, of virtually all of the evaluation schemes established to monitor the effectiveness of surveillance cameras on town centre crime, few looked any further than to assess the impact of CCTV on recorded crime trends. Very few studies followed through to explore CCTV in relation to incident management, evidence development, case preparation and prosecution, even as police officers themselves were realising that it was here that some of the major benefits of CCTV might be found.

A final issue relating to Hayman's observation concerns what we might call the "police point of view". CCTV's most enthusiastic supporters are often the police themselves, and when presented with a new crime control technology, they may be keen to try it out. However, the police are not necessarily the best equipped to undertake the problem analysis, and for a long time, CCTV has been likened in the UK to "a cure looking for an illness". Commentators may have had a strong intuitive sense that CCTV would – indeed *should* - influence crime levels, but there was little available evidence of its effectiveness.

Some commentators have been sceptical arguing that police managers might adopt CCTV to allow them to save resources by reducing police patrol levels in certain areas. At other times the lobbying and marketing of CCTV by security industry representatives has been called into question. Thus, marketing by vested interests may have generated unrealistic expectations about what security cameras could achieve.

Facing two such sets of potentially vested interests, the case for an independent evaluation of CCTV schemes might seem incontrovertible. However, the limits of the early CCTV evaluations were often restricted to simple questions of crime reduction *impact*. The potentially much wider role that CCTV technologies might play across a wide range of policing activities was rather overlooked: a case of restricted vision, perhaps. When future CCTV systems are considered or when systems are to be modernised and developed these issues need appropriate consideration – systems may need to be fit for a variety of purposes as the Home Office and ACPO have acknowledged.

There are further complaints, emanating from the ACPO CCTV survey team itself, that "the quality of images recorded by CCTV systems varies considerably", whilst anecdotal evidence also suggests that "over 80% of the CCTV footage supplied to the police is far from ideal, especially if it is being used for primary identification" purposes.

Finally, the case for civilian oversight, public accountability, and independent monitoring is as important in relation to CCTV as in other areas of contemporary policing. Not only is this important in terms of the public understanding of the purpose of CCTV but it also helps establish its acceptability, and while enhancing public trust and confidence, can improve the effectiveness of policing systems. This is an area often overlooked, even in the recent UK Home Office CCTV strategy document. While the document considers the necessity for inter-agency collaboration, the importance of local stakeholders and partners, and the need for effective governance and oversight of CCTV planning, it is rather silent about the systems of local accountability to which such surveillance systems might be subject.

Reference is made to *national* processes of inspection and oversight such as the UK Information Commissioner and the Surveillance Commissioner but local arrangements are overlooked, even though there are many good examples or templates to draw upon. Conversely, this may be an area in which different political cultures or contrasting policing traditions suggest alternative solutions. After all, the point here is not to impose "one size fits all" solutions across diverse European cultures, but rather to raise issues that experience has shown are important when CCTV surveillance is considered.

As Gras has argued, a number of other cultures, amongst them Germany, France, the Netherlands and Sweden, might lay claim to rather more stringent regulatory regimes than the UK. For her part, speaking at the Efus Zaragoza conference Riches, has pointed out that in the UK, CCTV was developed in a largely pragmatic fashion with little thought given to the monitoring and accountability issues until systems were already up and running.

Drawing conclusions

Problem analysis and Implementation

Taking these issues together we can draw some important lessons from the best available UK experiences of CCTV installation and use. First of all it is worth noting the somewhat surprising conclusion drawn by Martin Gill and Angela Spriggs in their 2005 evaluation for the UK Home Office:

"It would be easy to conclude ... that CCTV is not effective: the majority of the schemes evaluated did not reduce crime and even where there was a reduction this was mostly not due to CCTV; nor did CCTV schemes make people feel safer, much less change their behaviour."

With such a conclusion, the main surprise might be why CCTV systems ever took off in the UK to the extent that they did. Apart from the political issues, we also must consider other questions related to the implementation of CCTV, and which security managers and police, in particular, have often been slow to acknowledge and act upon. As Gill and Spriggs noted, suggesting that CCTV is a failure is just as misleading as the security industry's over ambitious claims for CCTV's success.

To take a more nuanced and evidence-led view, we need to bear in mind a number of issues, and consider a number of factors.

Crime rates or criminal incidents *alone* are not necessarily a good indicator of crime and disorder problems, or of public fears and concerns in an area, or of the quality and experience people have of their community safety. Policing and crime prevention initiatives have to take this complexity into account.

The complex and varied roles and purposes of a CCTV system: intelligence development, evidence gathering, incident management, and order maintenance all need to be acknowledged. Situational crime reduction, via prevention or deterrence, is not the only outcome. Clarity about a variety of purposes is essential. As the Home Office noted in its 2003 evaluation of CCTV projects implementation: "When considering which type of crime prevention mechanism to use, it is important to be clear about the problems in the area and specific about the capabilities of a CCTV system to address them. If the two do not correspond, CCTV is not the right solution."

Finally, CCTV systems have to be integrated with existing policing and crime management initiatives. This might mean that other policing processes might have to change. It was quite unrealistic to imagine that CCTV systems could have a sustained impact on their own. In a similar fashion, policing priorities had to be determined by reference to the problems requiring solution not driven by any *a priori* assumptions about the need for surveillance cameras.

By 1999, the Home Office guidance for CCTV development partnerships was insisting that any application for funding had to set out "the criteria for identifying a relevant crime prevention mechanism". This is to say that CCTV proposals had to be supported by evidence of "theoretically sound crime reduction principles which suggest plausible causal mechanisms by which [the CCTV system] could work against the current crime or disorder problem in the current context."

However, Gill and Spriggs went on to note in their final report that even where CCTV projects had discernible objectives which "had to be stated in tender documents", these "often did not drive the scheme… and were rarely embedded in day-to-day practice". So even when funding applications did contain evidence and problem analysis, these were often overlooked as soon as the funding was achieved.

Crime reduction and community safety impacts

When it claimed that "there is an ongoing debate over how effective CCTV is in reducing and preventing crime", the 2007 Home Office *National CCTV Strategy* document sought, perhaps understandably, to keep that very debate alive. In fact, the accumulated evidence from research and evaluation, a combination of rather mixed, unimpressive and otherwise disappointing or unreliable results, provides the more compelling story.

Many local CCTV evaluations were carried out in the UK on the back of the various waves of CCTV installation although these were not always very methodologically rigorous and often confined to *impact* assessments. Many were also rather too short term to provide any reliable evidence of sustained influence on crime trends and patterns. That said, a number of larger and/or comparative projects began to emerge later, as did a growing picture of evaluation experience.

In 2002, Brandon Welsh and David Farrington undertook for the Home Office Research Study a survey of 46 CCTV evaluation projects worldwide.

The results were rather mixed, half of the eligible studies "found a desirable effect on crime" although five found an "undesirable" impact, and five more found no significant impact. The CCTV schemes in the UK generally showed a greater range of impacts than those in North America. Furthermore, CCTV "had no effect on violent crimes but … a significant desirable effect on vehicle crimes", and on crimes in car parks. Finally, "In the city centre and public housing setting, there was evidence that CCTV led to a negligible reduction in crime of about two per cent in experimental areas compared with control areas."

Noting that "surveillance studies" was still a relatively new area, the authors went on to suggest that there needed to be further research on both the optimal conditions for securing CCTV effectiveness and the mechanisms by which positive results are obtained. It seemed fairly clear that an appropriate package of interventions was necessary for the best results. They concluded rather optimistically that "CCTV reduces crime to a small degree". They advised that "future CCTV schemes should be carefully implemented in different settings, and should employ high quality evaluation designs with long follow-up periods. In the end, an evidence-based approach to crime prevention which uses the highest level of science available offers the strongest formula for building a safer society."

Such conclusions about CCTV surveillance impacts have been confirmed in many other similar studies especially the large national study by Gill and Spriggs, in 2005. These authors also concluded that CCTV appeared to have limited crime reduction effects in town centres and residential areas but appeared to work best in relatively contained and controlled access locations (hospitals, car parks, shopping malls). CCTV had poor results on impulsive violence and alcohol-related offending, but better results on more premeditated crimes.

As in other studies, they also noted "halo effects", in other words crime reduction in adjacent areas, and crime displacement. The technical attributes of particular systems appeared to have either marginally positive or negative influences on the effectiveness of particular systems but these were of relatively little overall significance.

Finally, surveys of members of the public in all the CCTV scheme areas found very little evidence of significant changes in either behaviour or levels of fear or concern about crime.

Gill and Spriggs concluded: "Assessed on the evidence presented in this report, CCTV cannot be deemed a success. It has cost a lot of money and it has not produced the anticipated benefits." However, they noted, lessons are being learned and the technology is improving rapidly with new "event-led", proactive, "intelligent" behaviour recognition and biometric systems presenting new safety management opportunities - whilst also bringing new threats and challenges.

Above all, their "evidence based" conclusion represents a warning against an all too tempting search for technical solutions. CCTV is but a tool, and where it was perceived to have failed this was often because the expectations were too ambitious or because it was being used in unsuitable places for the inappropriate problems. In those cases, CCTV may have been poorly planned or badly implemented, or perhaps not effectively integrated into other community safety strategies and policing systems.

As Kevin Haggarty, a Canadian criminologist writing on surveillance, has noted, perhaps one beguiling myth we need to question is the unproblematic assumption that there are "surveillance solutions" for social problems. What the Home Office referred to in 2007 as "the search … for the panacea of CCTV" may be a futile one. Such "solutions" will undoubtedly generate still further problems and dilemmas.

Issues here might include the question of who benefits most from the umbrella of protective surveillance: in the UK town centres, high value retail areas were the first major beneficiaries, as opposed to residential areas, children's playgrounds or schools. These were not necessarily the most obvious community safety priorities or the most needy areas, but the nature of the funding arrangements in the early schemes meant that occupiers of these areas could most readily afford the matched funding investment costs.

Another issue of inequality arises: at whom are the cameras mostly directed, who is most frequently under surveillance? There are profound social and ethical questions associated with surveillance processes.

These ethical questions stretch to the definition of the crime and security problems that we are seeking to solve and into the design, monitoring and integration of the systems developed. They also involve the processes for oversight, monitoring, evaluation, accountability and redress that need to be part of effective community safety strategies. If these issues are not considered at every stage, problems will likely emerge that will diminish the effectiveness of the system itself. However technically sophisticated a system is, it will only be as effective as those who operate it, and it will only enhance community safety if it meets the needs and reassures the citizens it is intended to serve.

As Gill and Spriggs have said:
"*Too much must not be expected of CCTV. It is more than just a technical solution; it requires human intervention to work to maximum efficiency and the problems it helps deal with are complex. [It can] help reduce crime and boost the public's feeling of safety, and it can generate other benefits. For these to be achieved though, there needs to be greater recognition that reducing and preventing crime is not easy, and that ill-conceived solutions are unlikely to work no matter what the investment.*"

NOTE: this is an edited version of Professor Squires' paper. The complete version is available online from the following research page: http://www.brighton.ac.uk/sass/contact/details.php?uid=pas1

Bibliography

Armitage, R. 2002 *To CCTV or not to CCTV?* London, Nacro.

Brown, B. 1995 *CCTV in Town Centres: Three Case Studies, Crime Prevention and Detection Series,* no.73. London: HMSO. Deane, A. and Sharpe, D. 2009 Big Brother is watching: A comprehensive analysis of the number of CCTV cameras controlled by local authorities in Britain in 2009. London, www.bigbrotherwatch.org.uk

Clarke, R.V. 1995 Situational crime prevention. In M. Tonry and D.P. Farrington (eds.), *Building a Safer Society: Strategic Approaches to Crime Prevention*: Vol. 19. *Crime and Justice: A Review of Research* (pp. 91-150). Chicago, Illinois: University of Chicago Press.

Clarke, R. V. and **M. Felson** (Eds.) (1993). *Routine Activity and Rational Choice. Advances in Criminological Theory*, Vol 5. New Brunswick, NJ: Transaction Books.

Crawford, A. 1998 Crime Prevention and Community Safety: Politics, Policies and Practices. London, Longman.

Farrington, D.P. and **Welsh, B.W**. 2002. *Effects of improved street lighting on crime: a systematic approach,* Home Office Research Study 251.

Felson, M. 1998 *Crime and Everyday Life*, Second Edition. Thousand Oaks, CA: Pine Forge Press.

Gras, M.L. 2004 The Legal Regulation of CCTV in Europe. *Surveillance & Society* CCTV Special (eds. C. Norris, M. McCahill and Wood) 2(2/3): 216-229

Garland. D. 2001 *The Culture of Control,* Oxford, Oxford University Press.

Gill M. and **Spriggs, A**. 2005 *Assessing the Impact of CCTV.* Home Office Research Study No. 292. London: Home Office Development and Statistics Directorate.

Gill M. et al., 2003 *National Evaluation of CCTV: Early Findings on Scheme Implementation – Effective Practice Guide*. Scarman Centre National Evaluation Team, London, Home Office Development and Practice Report No. 7.

Haggarty, K. D. 2009 'Ten thousand times larger' – Anticipating the expansion of surveillance, in B. Goold and D. Neyland (eds) *New Directions in Surveillance and Privacy*. Cullompton, Willan Publishing. TV Evaluation Team

Hayman, A. 2009 The Terrorist Hunters: The ultimate inside story of Britain's fight against terror, (with M. Gilmore). London, Bantam Press.

Home Office/Association of Chief Police Officers (ACPO) 2007 *National CCTV Strategy. London*, Home Office. Hope, T. 2001, Crime victimisation and inequality in risk society, in R. Matthews and J. Pitts (ed.) *Crime, Disorder and Community Safety*. London, Routledge

Honess, T. and **Charman, E.**, 1992, *'Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness*, Police Research Group Crime Prevention Unit, 35, London: Home Office Police Department.

ICO (Information Commissioner's Office) 2008 CCTV *Code of Practice: Revised Edition*. ICO Office, Wilmslow: www.ico.gov.uk

Loader, I. 2008 Evidence to the House of Lords Select Committee on the Constitution: *Surveillance, Citizens and the State*. May 14th 2008.

Norris, C., Moran, J., and Armstrong, G., 1998 Surveillance, *Closed Circuit Television and Social Control*, Aldershot: Ashgate.

Norris, C., and Armstrong, G., 1999 *The Maximum Surveillance Society: The Rise of CCTV*. Oxford, Berg Publishers.

Riches, J. 2006 CCTV: Does it work? EFUS: Zaragoza Conference. http://zaragoza2006.fesu.org/IMG/pdf/CCTV_PresentationJames_RICHES.pdf

Shearing, C. 2000 Exclusion From Public Space. in Ethical and Social Perspectives on Situational Crime Prevention. (eds) A. von Hirsch, D. Garland and A. Wakefield. Oxford, Hart Publishing, 2000.
Short, E. and Ditton, J. 1998 "Seen and Now Heard: Talking to the Targets of Open Street CCTV", *British Journal of Criminology*, 38/3: 404-428.

Skinns, D. 1998 "Crime Reduction, Diffusion and Displacement: Evaluating the Effectiveness of CCTV", in C. Norris, J. Moran, and G. Armstrong (eds.): *Surveillance, Closed Circuit Television and Social Control, Aldershot: Ashgate.*

Squires, P. 2006 Introduction: Asking Questions of Community Safety, in Squires, (ed.) *Community Safety: Critical Perspectives on Policy and Practice*. Bristol, The Policy Press.

Squires, P. and **Measor, L.** (1996a). *CCTV Surveillance and Crime Prevention in Brighton: Half-Yearly Analysis.* Brighton: Health and Social Policy Research Centre, University of Brighton.

Squires, P. and **Measor, L.** (1996b). *CCTV Surveillance and Crime Prevention in Brighton: Follow-up Analysis.* Brighton: Health and Social Policy Research Centre, University of Brighton.

Surveillance Studies Network, 2007 Evidence to the House of Lords Select Committee on the Constitution: *Surveillance, Citizens and the State*. 28th November 2007.

Von Hirsch, A. 2000 The Ethics of Public Television Surveillance, in Ethical and Social Perspectives on Situational Crime Prevention. (Eds) A. von Hirsch, D. Garland and A. Wakefield. Oxford, Hart Publishing.
Wacquant, L. 2009 Punishing the Poor: The Neo-Liberal Government of Social Insecurity, Duke University Press.

Welsh, B. and Farrington, D. 2002 *Crime Prevention Effects of Closed Circuit Television: A Systematic Review, Home Office Research Study*, No.252, London: HMSO.

Privacy by Design: the case of CCTV

Jeroen van den Hoven
Delft University of Technology

I defend the idea of Privacy by Design for CCTV applications in policing and in the security domain as a way to overcome deep ideological, political and philosophical controversies concerning the nature and importance of privacy. Privacy by design is rapidly becoming more prominent in data protection policy and software engineering. The EU is promoting the idea as a new standard in *The EDPS Video surveillance guidelines* (Brussels, March 17 2010: p. 10):
"*Data protection and privacy safeguards should be built into the design specifications of the technology that the institutions use as well as into their organisational practices*".

I believe this is the preferred approach, but in order to make this idea succeed, two conditions need to be fulfilled:
1 - we need to realise that *Privacy by Design* or *Privacy Enhancing* applications are part of a more global approach to technological innovation, which is sometimes referred to as *Value Sensitive Design* or *Design for Values*. This approach requires a specific methodology in order to avoid improvisations in software engineering that might increase the risk of lack of transparency and accountability;
2 - Privacy by Design can only succeed if we are clear about the moral values underlying data-protection and have access to a fairly detailed and fine-grained account of the moral justifications of data protection, since all design decisions, however small and seemingly unimportant, will have to be argued for on the

basis of clear and convincing moral considerations.

The privacy issue lies at the heart of an ongoing debate in nearly all Western democracies between liberalists and communitarians over the question of how to balance individual rights with collective goods, individual rights and community interests. In the case of the issue of privacy, this debates opposes those who argue that it is necessary to protect the privacy of individuals by limiting the access to personal information, and those who believe that it is necessary to open this access because it will benefit the community. Some have argued that this is a contrived opposition, but it remains a real tension which emerges in all sorts of cases involving the infringement of privacy, such as, for instance, undercover actions led by the police on the internet, the disclosure of medical files for health insurance purposes or epidemiological research, the linking and matching of databases to detect fraud in social security, soliciting information about on-line behaviour of internet users from access providers in criminal justice cases and the use of Closed Circuit Television (CCTV) in public places for crime prevention.

The political philosopher Michael Walzer correctly observes that, “Liberalism is plagued by free-rider problems, by people who continue to enjoy the benefits of membership and identity while no longer participating in the activities that produce these benefits. Communitarianism, by contrast, is the dream of a perfect free-riderlessness.” Communitarians are looking at information technology to help them in the pursuit of the dream of perfect free-riderlessness.

Privacy has also been the subject of much philosophical discussion (Nissenbaum, 2004; Roessler 2005; Decew, 1997, Van den Hoven 2009) and many different authors have presented varying views on what is privacy. Different conceptual and philosophical accounts give different answers to the question of what privacy is and why it is important. Unfortunately, there is hardly any consensus and it does not seem likely that we will easily reach one.
Added to the controversy is now the idea that privacy is completely obsolete – “you have zero privacy, get over it” -, that modern technology has turned it into something of the past, and that we should accept this as a fact of life.

Many different concepts underly the idea of privacy, and no one is very clear about what it really means nor understand clearly how technology, software engineering and systems development affect it. For practical purposes, such as the formulation and design of laws, policy and technology, the conceptual muddles and confusion concerning the nature and importance of privacy lead to practical indecision, delays, inefficiency, high costs and failures in ICT projects.
It is necessary today to “reconstruct” the notion of privacy, in order to move on and tackle the urgent issues that we are facing on a daily basis without getting bogged down by endless debates.

The central role given to the concept of privacy when we debat about the moral issues surrounding the protection of personal data obfuscates the search for practical solutions. It leaves us stuck in a deep and irresolvable controversy about the nature of the Self and the Community, opposing liberals and communitarians. Since it is not easy to take sides, I suggest we address the issue from another point of view and simply ask ourselves: why should we protect personal data; what moral reasons do we have to do so?

Can we consider that we should protect them just as we protect, say, nuclear reactors, medieval manuscripts, babies or bird sanctuaries? In each of these cases we have good reasons to restrict access, limit visiting hours, stipulate what behaviour is acceptable, who is allowed to get near or interact, and how. In each of these examples protection takes on a different form and has a different rationale. What would count as a good moral reason to protect personal data and what type of reason would justify limiting the right to others to access these data?

The moral reasons why we should be concerned with our personal data are the same ones that justify imposing limitations on what others can do with it (generate, process, store, disseminate, access). They are the following:

First, the protection of the individuals whose personal information is available to others. In an information society, people are at risk of being harmed precisely when and because others have access to their personal information. This is what we would like to prevent: the use of personal information against the people.

The second reason is related to fairness in the market of personal data. We protect personal data, and have laws to that effect, because so many people would like to have a cheap and easy access to them. A lot of people and organisations have good reasons to hide from the public the market value of personal data and the secondary use that can be made of it. Contracts offered to clients in order to get access to their personal data, such as loyalty cards, are often not fair. Data protection regimes should guarantee a fair bottom line and protect citizens against abuse and breach of contracts.

The third reason has to do with a fair management of information. Information about individuals has a "natural habitat", so to speak. It is gathered and exchanged in the framework of a series of well delimited situations, and managed by specific groups of people, such as doctors, police officers, human resources managers, lawyers etc. It is inappropriate to divulge this information across those social boundaries, for instance if information is leaked out of the medical sphere into the commercial sphere, or out of the family sphere into the political sphere. Each of these spheres should be kept separate.

Finally, the fourth reason is that each individual has the right to his/her moral autonomy and control over how he/she presents him/herself. People want to be identified as the people they themselves identify with. They want to be seen as the person they see themselves as. This requires discretion and choice about the personal information that they disclose. This also requires data protection and the respect of the sovereignty of each invidual over his/her personal information.

Value Sensitive Design and Privacy by Design

The integration of security and privacy in design, architecture and engineering are not new. As far back as in the 18th century, the philosopher Jeremy Bentham conceived what he believed would be the ideal architectural design of prisons. He said: "Morals reformed— health preserved — industry invigorated — instruction diffused — public burthens lightened — Economy seated, as it were, upon a rock — the gordian knot of the poor-law not cut, but untied — all by a simple idea in Architecture!" His idea was that security and control over prisoners would be greatly enhanced by the design of a dome-shaped prison, which he named the "Panopticon" because the obervation deck of the guards would be situated in the center, allowing them to see everything around. This is a very early example of incorporating concepts into design. Today, incorporating ethical values into the design of technology is referred as Value-Sensitive Design (VSD). Privacy by Design is one of the applications of Value Sensitive Design.

Value Sensitive Design incorporates moral values into the design of technical artifacts and systems by considering design from an ethical perspective, and by researching how moral values (e.g. freedom, equality, trust, autonomy, privacy, or justice) may be fostered or curbed by the design itself (Friedman 1997; Friedman 2005). Value Sensitive Design focuses *primarily* and *specifically* on *moral* values, whereas traditional design focuses rather on functional requirements such as speed, efficiency, storage capacity and usability. Although building a user-friendly technology might have the side-effect of increasing a user's trust or sense of autonomy, in Value Sensitive Design the incorporation of moral values into the design is a primary goal, rather than a by-product. Value Sensitive Design is also, as I have argued (Van den Hoven 2005: 4), "a way of doing ethics that aims at making moral values part of technological design, research and development".

VSD can only be used in the data protection area if we manage to clearly define which moral values need to be incorporated in the design of a system, and how they can be translated into "non-functional requirements". The following step is to detail these requirements in a very precise and clear set of functions that need to be assigned to the system. But this methodology doesn't exist yet, and the danger is that with the evolution of technology, systems may become even more obscure than they are now.

VSD aims at reconciling different and opposing values in engineering design or innovations (Van den Hoven 2008b). This is directly applicable to the opposing values at stake in the debate about CCTV: security and privacy.

As a society we value privacy, but at the same time we value security and the availability of information about citizens. This tension is exemplified in the debates about CCTV cameras in public places. We either accept to trade our privacy for security by installing cameras everywhere, or we refuse to do so in the name of the respect of privacy, and thus settle for less security. Smart CCTV systems allow us to have our cake and eat it, because their smart architecture integrates the surveillance function with systems that limit the flow and availability of recorded information.

The first generation of CCTV cameras offers relatively little in terms of security. The images are blurry and they infringe on the privacy of passers-by by recording their whereabouts. The second generation offers much better quality and thus provides more security. But precisely because the quality of the images is so good, they are more invasive. Now, the third generation of "smart camera systems" records only suspicious events and are equipped with an integrated function that blocks the recording of images inside private houses. It is a perfect technology-based solution to our moral dilemma. For example, the Rotterdam police already uses such "smart" systems, equipped with software tools that prevent camera operators to film inside private houses.

The technological parameters of these smart systems can be configured in such a fine-grained manner that they offer all the advantages and functionality of cutting-edge CCTV without any infringement of data protection norms. When previous systems were based on "all or nothing", we now have a technology that allows to choose who gets access to which recordings, on which conditions, how long the images are stored, and how the recordings can be used and merged with other databases.

A common trait of many "smart", innovative technologies is that they allow the combination of previously irreconcilable values or preferences. For instance smart environmental technologies reconcile the quest for economic growth and sustainability, and so-called smart bombs promise to hit the enemy without causing civilian casualties.

Privacy by Design: a moral innovation

It seems legitimate to affirm that since society has the moral obligation to both guarantee the privacy of its citizens and maintain the safety and security of all public places, then it also has the moral obligation to do what it takes in order to satisfy these two obligations. It is morally imperative that we keep researching and innovating along the lines of Privacy By Design, a technology that allows to combine security with privacy.

Such an endeavour that requires a fine-tuning of the technology and a fine-grained reflexion on the moral justification of data protection. Moreover, it requires a systemic methodology in order to connect both realms, the technology and our moral values.

Bibliography

Batya Friedman E. A. Value Sensitive Design: Theories and Methods. Technical Reports, Department of Computer Science and Engineering, University of Washington, 2002. Report 02-12-01. http://www.urbanism.org/papers/vsd-theory-methods-tr.pdf

Jeroen Van den Hoven & **John Weckert**, Information Technology and Moral Philosophy. Cambridge University Press, 2009.

Urban Video Surveillance in Europe: A Political Choice?

Eric Töpfer
Technical University of Berlin

Urban video surveillance became a European issue for the first time in 1997, when it was picked as one of the key themes of the European conference on "Crime Prevention: Towards a European Level", organised by the Dutch Presidency of the European Union in Noordwijk (Netherlands). The closing declaration of this conference stated, in particular, that:

> "*Cameras as crime prevention tools are, in general, a new and cost-effective way to reassure citizens preoccupied by their security. They deter criminality and can support public prosecution. [However], closed circuit television (CCTV) techniques should only be used [within the framework] of a comprehensive local and/or national crime prevention policy [...] and they should be] monitored by trained personnel [...]. The public should be aware of their use. Privacy should be safeguarded.*" [1]

These were the early days of CCTV. Three years earlier, in 1994, the British Home Office had kicked off a "surveillance camera revolution" by funding a series of City Challenge Competitions with a first tranche of £2 million.[2] In France, the parliament had passed in 1995 the so-called Pasqua law which explicitly authorised the deployment of CCTV in a series of "hot" areas of France's main cities. This move had followed the controversial installation, two years earlier, of 96 surveillance cameras in the Parisian suburb of Levallois-Perret.[3] In the Czech Republic, the government started in 1996 to finance local crime prevention initiatives, which included, among others, the installation of CCTV systems. The same year, following the Czech example, the local police department of Leipzig installed one camera in the centre of the city, the first one ever installed in Germany.[4] In the Netherlands the first system was launched in 1998, a year only after the Noordwijk crime prevention conference, when the city council of Ede decided to install 12 cameras to monitor, at night-time, an area situated near the central railway station.[5]

Referring to the Noordwijk conference, the French delegation initiated at the end of 1998 a debate about video surveillance in the "Police Cooperation Working Party" (PCWP) working group of the Council of the European Union. The PCWP report concluded that "local authorities make little use of video systems, except in the United Kingdom and Finland" and stated that the PCWP itself "could promote the development of such systems".[6]

Towards ubiquity?

CCTV surveillance or "industrial television", as it was called at first, is as old as broadcast television. But during several decades, the use of surveillance cameras in policing was limited to either the monitoring and managing of traffic flows or, occasionally, the surveillance of crowds at major events as well as criminal investigation. Permanent CCTV surveillance of public urban areas was the exception. In the UK for instance, CCTV systems had only been installed in a few areas of national interest such as Westminster and Whitehall, where a camera network had been set up by the London Metropolitan Police in the wake of the political unrest of the late 1960s.[7]

Today, 13 years after the Dutch crime prevention conference, which obviously initiated a process of international policy transfer, there are CCTV systems in thousands of cities and towns across Europe. As Steve Graham, Professor of Human Geography at the University of Durham (UK) and one of the world's leading scholars specialised in the cybercities phenomenon, predicted back in 1999, it seems that CCTV has become the "fifth utility" of modern urban life, after water, gas, electricity and telecommunications.[8]

The rise of open street CCTV, understood here as the 24/7 surveillance of urban public areas for declared purposes of crime control and public order management, started in the 1980s. Three main factors explain the "boom" of CCTV throughout European cities:

➤ the emergence of a new paradigm underlying our criminal justice policies, whereby the traditional approach that considered crime as an essentially individual deviance has been replaced by the idea that its roots lie rather in specific groups and places considered to be "criminogenic". And hence, that the risk

[1] Recommendations of the EU conference 'Crime prevention: towards a European level', Noordwijk, 11–14 May 1997. In: *European Journal on Criminal Policy and Research*, Vol. 5, No. 3 (September 1997), pp. 65-70 (66).

[2] Norris, C. et al. (2004): The growth of CCTV. A global perspective on the international diffusion of video surveillance in publicly accessible space. In: *Surveillance & Society*, Vol. 2, No. 2/3, pp. 110-135 (111).

[3] Töpfer, E. & Helten, F. (2005): Marianne und ihre Großen Brüder. Videoüberwachung à la Française. In: *Bürgerrechte & Polizei/CILIP*, No. 81, pp. 48-55.

[4] Müller, R. (1997): Pilotprojekt zur Videoüberwachung von Kriminalitätsschwerpunkten in der Leipziger Innenstadt. In: *Die Polizei*, Vol. 88, No. 3, pp. 77-82.

[5] Gemeente Ede (2000): *Ogen in de nacht. Eindevaluatie cameratoezicht Ede*. August 2000. Online: http://www.hetccv.nl/binaries/content/assets/ccv/dossiers/bestuurlijk-handhaven/cameratoezicht/1_ede_effectevaluatiex2000.pdf.

[6] Council of the European Union: Doc. 5045/99, 12 January 1999.

can be assessed, prevented and managed thanks to actuarial methods.

➤ the decline of industry as the basis of urban economies and the rise of consumerism and services, together with the emergence of "place marketing", or "city branding". Nowadays, safety and security are considered to be key elements of a city's attractiveness, in the global competition for investment and economic activity.

➤ the trend towards decentralisation that saw local municipalities taking charge of local crime control and urban order. Many countries have given municipalities an explicit legal mandate to install cameras on their territory in order to fight crime.[9]

The diversity of public area CCTV in Europe

Apart from the global factors that we have just mentioned, it is also important to take into account the specificities of each European country, their distinct socio-economic context, institutional systems and experiences of crime. As the Canadian sociologist David Lyon points out:

> *"It is true that some structural similarities and the common problems facing (late) modern states may produce similar techniques in different places. [...] It is also true that local and regional social, political and cultural contexts will experience surveillance in different ways. [...] The mere existence of new technologies is far from being a sufficient reason for them to be used."*[10]

In the Grand Duchy of Luxembourg, the first open street CCTV system was installed in 2007, 13 years after Britain had launched its first City Challenge Competition.[11] In Norway, there is only one system -six cameras operated by the local police of Oslo, the capital-, which was installed in 1999.[12]

By contrast, there are in the UK an estimated 40,000 to 50,000 cameras installed in public areas in more than 500 cities.[13] In France, some 500 municipalities -most of which large agglomerations- are reported to operate around 20,000 cameras. Furthermore, the French Interior Ministry announced in 2009 that the number of cameras in use throughout the country would be multiplied by three.[14] In the Netherlands, a fifth of the 443 local governing bodies use video surveillance in public areas, with a total of some 4,000 cameras.[15]

In Eastern Europe, Poland, the Czech Republic, Hungary and Baltic countries are known to operate hundreds of cameras in their major cities.

Southern European countries have varying positions towards CCTV. Portugal and Spain have been reluctant to use it. Greece installed some 1,200 cameras for the Olympic Games of 2004, a move that generated protests among the population. Some 200 cameras were nevertheless kept after the games.[16] By

[7] Williams, C. (2003): Police surveillance and the emergence of CCTV in the 1960s. In: CCTV, ed. by M. Gill, Leicester: Perpetuity Press, pp. 9-22..

[8] Graham, S. (1999): Towards the fifth utility? On the extension and normalisation of CCTV. In: Surveillance, Closed Circuit Television and Social Control, ed. by C. Norris et al. Aldershot: Ashgate, pp.89-112.

[9] For a detailed theoretical discussion see McCahill, M. (1998): Beyond Foucault. Towards a contemporary theory of surveillance. In: *Surveillance, Closed Circuit Television and social control*, ed. by C. Norris et al., Aldershot: Ashgate, pp. 41-65.

[10] Lyon, D. (2004): Globalizing surveillance. Comparative and sociological perspectives. In: *International Sociology*, Vol. 19, No. 2, pp. 135-149 (141-142).

[11] Tageblatt. *Zeitung für Luxemburg*, 12 December 2007.

[12] Winge, S. & Knutsson, J. (2003): An evaluation of the CCTV scheme at Oslo Central Railway Station. In: *CCTV,* ed. by M. Gill, Leicester: Perpetuity Press, pp. 127-140.

contrast, hundreds of Italian towns (*communi*) are using CCTV systems.

In Germany, where the Conference of Interior Ministers endorsed CCTV as an "appropriate tool to support police work", in 2000, there are today less than 200 cameras in operation in around 30 to 40 cities.[17]

In Austria, where a first system was launched in 1994 around the railway station of Villach, a federal level initiative accelerated the growth of CCTV after 2005. After an amendment of the Security Police Act, the Interior Ministry announced the expansion of public area surveillance.

In 2006, five Austrian cities had installed CCTV systems in 11 public areas, and applications had been registered for the installation of CCTV in 17 new locations.[18]

In Denmark, the government presented a new set of measures aimed at reinforcing security, which included the official authorisation of CCTV in public areas, for the first time ever.[19]

This brief overview shows that the use of CCTV in Europe varies according to each country. It also varies in the cities themselves, where some areas are covered by a dense network of hundreds of cameras, whereas other urban zones are only covered by small systems of less than a dozen cameras.

Support and regulation

CCTV is broadly supported by major political parties as well as by the general public, as opinion polls regularly show. However, support varies depending on the location and extent of surveillance. According to a survey conducted in 2003 in five European capitals, 90% of the people interviewed in London were in favour of open street CCTV, whereas in Vienna, only 25% shared this view.[20] In Britain, following the Bulger case in 1993, there was a large consensus around the idea that CCTV could be the magic "silver bullet" against the evils of crime. Indeed, the images showing two 10-year old boys abducting in a shopping center a two-year old toddler, James Bulger, whose mutilated body was found two days later on a nearby railway line, were broadcasted during several weeks on all major TV channels. The case prompted a national trauma, while offering a promising "techno-fix" to prevent such horrible events in the future.[21]

However, British-style CCTV is seen in some continental European countries as a kind of "Big Brother" surveillance. In Germany for example, the former

[13] Williams, K. S. & Johnstone, C. (2000): The politics of the selective gaze. Closed Circuit Television and the policing of public space. In: *Crime, Law and Social Change*, Vol. 34, No. 2, pp. 183-210.

[14] *France Soir*, 16 February 2009.

[15] Dekkers, S. et al. (2007): *Evaluatie Cameratoezicht op Openbare Plaatsen. Éénmeting*. Eindrapport. Regioplan publicatienr. 1515. Amsterdam, Mai 2007, p.IV.

[16] Samatas, M. (2007): Security and surveillance in the Athens 2004 Olympics. Some lessons from a troubled story. In: *International Criminal Justice Review*, Vol. 17, No. 3, pp. 220-238.

[17] Figures updated from Töpfer, E. (2005): Polizeiliche Videoüberwachung des öffentlichen Raums. Entwicklung und Perspektiven. In: *Datenschutz Nachrichten*, Vol. 28, No. 2, pp. 5-9

[18] *Salzburger Nachrichten*, 4 February 2006.

[19] *heise online*, 4 novembre 2005

[20] Hempel, L. & Töpfer, E. (2004): *CCTV in Europe. Final report of the Urbaneye Project. Zentrum Technik und Gesellschaft,* TU Berlin. (Urbaneye Working Paper No. 15), p. 44. En ligne : http://www.urbaneye.net/results/ue_wp15.pdf.

[21] McGrath, J. (2004): *Loving Big Brother. Surveillance culture and performance space*, London: Routledge.

Federal Interior Minister, Otto Schily, supported open street CCTV when it became a political issue in the late 1990s, but he also warned against "blanket surveillance", arguing that it constitutes a disproportionate violation of fundamental rights.[22]

To some degree, such attitudes are mirrored by the legal regulation of open street CCTV. In Britain, the early expansion took place within a regulatory vacuum: The UK Data Protection Act of 1984 only applies to digital data processing, thus leaving out the analogue systems put in place in the early days of CCTV. Moreover, the Criminal Justice and Public Order Act of 1994 explicitly authorised local authorities to provide "apparatus for recording visual images of events occurring on any land in their area", and released them from the duty to pay expensive licensing fees for system's cabling, contemplated under the Telecom Act. The regulatory framework only changed with the implementation of the EU Data Protection Directive through the modernisation of the Data Protection Act in 1998, and the incorporation, in 2000, of the European Convention of Human Rights into the national Human Rights Act.

Contrarily to Britain, most European countries have considered since the beginning that open street CCTV constitues an infringement of fundamental rights. In France, an administrative court in Marseilles ruled in 1990 against plans of the local council of Avignon to launch a 93-camera-network, considering that the optional recording represented a disproportionate violation of privacy. Open street CCTV and footage-recording was only authorised in 1995, by the Pasqua Law, which prescribed its usage in areas where there exists "a high risk of being assaulted or stolen".[23]

In the Federal Republic of Germany, the 1983 Census Decision of the Federal Constitutional Court developed the concept of a "right to informational self-determination", declaring illegal any collection of personal data without informed consent, except when undertaken in the "prevailing general interest", in line with the principle of proportionality and with a clear legal basis. In effect, open street CCTV in Germany is usually regulated by the regional police, and limited to so-called "crime hot spots". Similar legal approaches that limit the use of open street CCTV cameras to more or less clearly defined areas can be also found in several other countries. However, in countries such as Hungary and Norway, data protection legislation is the legal point of reference. This is also the case today in the UK. Some of these data protection acts address explicitly CCTV, while others only mention video surveillance in general terms. In Britain, for instance, the first "CCTV Code of Practice" was issued in 2000 by the Information Commissioner.[24]

Organisation and supervision

The organisation of open street CCTV in European countries varies according to their legal framework. In some countries, the surveillance of public streets is the exclusive domain of the police, who owns, maintains and operates CCTV systems. This is the case in Germany, where the regional police forces of the Länder are in charge, although they sometimes share information with the Federal Police and local public order departments. In Austria, it is the Federal

[22] Speech in Federal Parliament, 9 November 2000. Plenarprotokoll 14/130.

[23] Section 10 of LOI no 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.

[24] A revised version can be found at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf.

Police who is in charge. In Norway, the Oslo CCTV system is run by the national police. In other countries, CCTV is mainly a local authority affair. In Britain for instance, some 80% of the open street CCTV systems are estimated to be owned and operated by local councils.[25]

CCTV systems are usually run by local or municipal police forces, in countries that have a local police. Most of the time, the actual management of CCTV is done by civil staff, in collaboration with the municipal, regional and/or national police forces.

There are also examples of public-private partnerships. For instance, in Vilnius, the capital of Lithuania, control room operations are contracted to a private security company.[26] In the UK, the first wave of CCTV systems was often co-funded by local business communities, and in several cases, a close network was established between the public CCTV control room and private "ShopWatch" schemes.[27] Also in the UK, there have been initiatives aimed at enrolling the general public, such as the experiment conducted a few years ago in the London area of Shoreditch, where local residents received CCTV images on their personal TV.[28]

Part of this diversity in terms of organisation has to do with each country's regime of supervision and licensing. In many countries, open street CCTV falls under the supervision of the data protection authorities who are usually authorised to inspect video surveillance systems, denounce bad practices, and recommend improvements in the management of data. However, some countries do not include CCTV among the areas covered by their data protection authorities. This is the case of Austria, for instance, where it is the Representative for Legal Protection (*Rechtsschutzbeauftragter*) at the Federal Interior Ministry who has the authority to check CCTV systems prior, but his recommendations are not mandatory. In France, the national data protection authority (the CNIL according to its French acronym) was bypassed by the "Loi Pasqua" which created new bodies in each territorial district, the "Commissions Départementale de Vidéosurveillance" (CDV). Headed by a judge, the Commission revises each CCTV project and its members vote in favour or against it. The final decision, however, rests in the hands of the "Préfet", who is the representative of the central government in the territorial "département". Most of the times, the Préfet follows the Commission's recommendation.

Global vs local approach

Cost is a key-factor determining the extent of CCTV. Unsurprisingly, CCTV's expansion is more limited in countries where only trained police officers are authorised to monitor CCTV images in the control room, compared to countries employing lowly paid, civil staff.

In some countries, the central government made significant investments in street surveillance. This is the case of the UK, where the Home Office funded between 1994 and 1998 four rounds of *City Chal-*

[25] *CCTV Image*, No. 25 (février 2008), pp. 5-6.

[26] Töpfer, E. (2008): Videoüberwachung in Europa. Entwicklung, Perspektiven und Probleme. In: *Informatik und Gesellschaft. Verflechtungen und Perspektiven*, ed. by H.-J. Kreowski, Münster: LIT Verlag, pp. 61-82 (65-66).

[27] Coleman, R. (2004): *Reclaiming the streets. Surveillance, social control and the city*, Cullompton: Willan Publishing.

[28] Guardian, 11 January 2006.

lenge Competitions for a total of £85 million, or 75% of the overall budget for crime prevention. After 1998, the New Labour followed the same policy and invested some £170 million in its *CCTV Initiative* until 2002.[29]

Other countries where public investment has been significant are the Czech Republic, where the government's crime prevention budget includes a significant allocation to CCTV, as well as Italy and Germany, where regional governments have supported video surveillance.

Europe's national and/or regional governments have promoted the local adoption of CCTV not only by setting legal rules and providing financial resources, but also by defining how to use it. In several countries, the central government has issued guidelines for local authorities, in order to avoid a permanent "reinvention of the wheel" at the local level. The UK Home Office's booklet *CCTV: Looking Out For You*, published in 1994, can be seen as an early example, though it mainly served purposes of promotion rather than guidance. More advanced was the guidebook *Handreiking Cameratoezicht* issued by the Dutch government in 2000, and distributed to all the municipalities of the country. The booklet presents a summary of experiences with public area CCTV in the Netherlands and abroad, and gives information about technical aspects of CCTV, together with practical tools such as a check-list and a CD with additional information.[30] The government of Belgium did something similar, providing guidelines, advice and promoting the exchange of experiences.

In the UK, where the expansion of CCTV and its effectiveness against crime has attracted growing critics over the past few years -in particular since the publication, in 2005, of a national evaluation- the Home Office and the Association of the Chief Police Officers issued in 2007 a National CCTV Strategy. This document outlines 44 recommendations for "potential improvements". Among others, it recommends the standardisation of all aspects of CCTV, the creation of a network of live and stored CCTV images, the training of all personnel, and more synergy among the different actors involved in CCTV management. Furthermore, it calls for increasing the power of the Information Commissioner in order to ensure compliance with the Data Protection Act. The strategy is backed up by the establishment of a national CCTV strategy programme board which will advise on taking forward the recommendations in the report and coordinate future activity.[31]

France is heading in the same direction, as its government is currently working on a national CCTV strategy.

Most other European countries are far away from devising such strategic approaches, leaving the development of CCTV mainly to local initiative.

Political choice or technological momentum?

As we have seen, the European landscape of urban CCTV surveillance is characterised by a huge diversity in terms of political support, legal regulation, organisation, data protection regimes and national strategies. The evolution of video surveillance in

[29] Töpfer, Eric (2007): Entgrenzte Raumkontrolle? Videoüberwachung im Neoliberalismus. Paru dans : *Kontrollierte Urbanität. Zur Neoliberalisierung städtischer Sicherheitspolitik,* ed. by V. Eick et al., Bielefeld: transcript, pp. 193-226 (204-206)r 2006.

[30] Les directives sont régulièrement mises à jour. La version actuelle est disponible sur : http://www.hetccv.nl/binaries/content/assets/ccv/dossiers/bestuurlijk-handhaven/cameratoezicht/handreiking_cameratoezicht_mei_2009.pdf.

[31] Gerrard, G. et al.. (2007): *National CCTV Strategy.* Londres : Ministère de l'Intérieur.

public spaces varies according to each country's institutional framework, the financial resources available and, last but not least, the prevailing consensus among the public.

Throughout Europe, however, the real engine for development is found at the local level. Public officers, local politicians and the police either support or prevent the development of CCTV according to their views, their interests and their intentions.

But to what extent do politics, rather than technology, influence the evolution of CCTV? Surveillance cameras have been used for policing in public spaces for more than 50 years. Since the 1990s, there has been a massive expansion of CCTV, which is promoted as an efficient tool to combat crime. At the same time, evaluation studies question its effectiveness as a "silver bullet" against crime. Today, the emphasis when justifying video surveillance in public debates has shifted from crime prevention to criminal investigation, with CCTV being presented as a useful tool to find evidence after a crime is committed.

Nowadays, CCTV surveillance is not limited to crime prevention. Once installed, a CCTV system can be used to control misdemeanours such as littering and unauthorised parking, or to watch municipal staff working in the streets. It can also be used to manage major public events, or any major emergency.

A new trend is emerging with the networking of formerly "discreet" systems. The police and other law enforcement agencies demand real-time access to CCTV images of a city's transport system, for instance, or other large public and private organisations. Today, public spaces are covered by intricate networks of video surveillance systems.[32]

In an effort to digest the increasing number of images, algorithmic surveillance is now taking over traditional methods, which means that crucial decisions are delegated to black-boxed technology of biometrics, automated pattern recognition, and GIS-based decision support systems. As it becomes more and more difficult for common citizens and decision-makers to understand the actual form and function of networked and semi-automated CCTV systems, the current trends raise serious questions regarding the transparency and democratic accountability of contemporary urban surveillance.

The growth and evolution of CCTV in Europe has reached a point where it is now urgent that we discuss, develop and implement common principles for its use.

[32] The term is borrowed from McCahill, M. (2002): *The surveillance web. The rise of visual surveillance in an English city*, Cullompton, Devon, UK: Willan Publishing.

The legislative framework of video surveillance in Europe

Laurent Lim, Legal Adviser, French National Commission on Information and Liberties (CNIL)

➤ Today, surveillance cameras are used, more or less massively, to monitor public and private areas throughout the world. Accompanying the general technological trend making the capturing of images increasingly easy, video surveillance systems are being perfected and evolving rapidly.

Thus, the tools of video surveillance now propose, in particular, the transmission of images by Internet (video IP), management interfaces integrating into the office environment, and ever-improved quality of image and storage capacities. Alert rise software, on the basis of an 'intelligent' reading of images, are available and should progress towards even more sophisticated analysis possibilities and, in particular, through the use of video images combined with other technologies (sound recognition, facial recognition).

These future evolutions, the diversification of uses, as well as the maturity of the video surveillance market, challenge European and national legal norms, which specifically restrict the use of video surveillance or treat personal data protection on a general basis.

Although European institutions restricted the gathering and use of personal data fairly early on, the first instruments specifically dealing with the question of monitoring have only appeared recently.

At the national level, the legislations of member states of the European Union, even though setting different rules and conditions, allow for resorting to video surveillance.

In Europe, the question of conformity in the use of video surveillance systems with the directive on data protection arises, and we shall see that there are varied legislative responses in the way of legally restricting these systems. It is advisable to stress that the law is not necessarily the only legal instrument for monitoring video surveillance: jurisprudence, the resolutions, opinions and recommendations of European or national institutions, as well as data protection authorities, must be taken into account. Finally, codes of good practices or charters of ethics constitute tools that are particularly useful for self-regulation.

I.THE EUROPEAN LEGISLATIVE FRAMEWORK

Certain fundamental principles have been adopted at the European level regarding the protection of fundamental rights and freedoms, as well as regarding personal data protection. These texts also concern data processing carried out in the framework of video surveillance operations.

A. The fundamental guarantees of the texts of the Council of Europe

The European Convention for the Protection of Human Rights and Fundamental Freedoms, adopted in Rome on 4 November 1950 by the Council of Europe, sets down in its Article 8 the right to the respect of private and family life, the home and communications.

This Convention was supplemented by an additional protocol, no.4 of 16 September 1963, guaranteeing in its Article 2 freedom of movement for whomever is regularly on a state's territory.

Moreover, the Convention No. 108/1981 for the protection of individuals as regards automatic processing of personal data, adopted by the Council of Europe on 28 January 1981 and ratified by 40 European states, is the first restrictive international instrument whose objective is to set minimal norms to protect individuals against abuses likely to occur during the gathering and processing of personal data concerning them.

It applies to the public and private sectors and lays down a certain number of general principles concerning the gathering, processing and communication of personal data via new information technologies.

Video surveillance activities enter into its field of application, insofar as they involve personal data processing in the sense of Convention no. 108 and where the advisory committee set up by this Convention reckoned that voices and images must be considered personal data when they provide information about a person by making that person identifiable, even indirectly.

These principles focus in particular on the lawful and loyal nature of the gathering and automatic processing of personal data, the principle of their recording for specific and legitimate purposes, the non-use of data for ends incompatible with these purposes, the limitation of the storing duration to the strict minimum, the appropriate, non-excessive character in relation to the purposes pursued as well as the pertinence of the data and the obligation of updating. The Convention proscribes the treatment of 'sensitive' data (relative to racial origin, political opinions, health, religion, sex life), and also guarantees the right of the persons concerned to know the information stored concerning them and, if need be, to demand rectification.

The European Court of Human Rights had the opportunity to specify the outlines of these guarantees as regards video surveillance. Thereby, the revelation and publication in the media, in the framework of crime-fighting campaigns, of images stemming from video surveillance systems of the public highway, unbeknownst to the person filmed, constitutes a violation of Article 8[1].

In order to respond to the need for proposing a more specific legal framework for video surveillance operations, and being '*concerned*' after finding that '*national laws are far from being homogeneous in this area*', the Parliamentary Assembly of the Council of Europe adopted a Resolution no.1604 on 25 January 2008, by which it formally called the member states of the Council of Europe to '*apply the guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance*'.

These principles, numbering twelve, take up and apply the principles set by the Council of Europe's instruments concerning video surveillance, stressing in particular the necessity of a pertinent, appropriate and non-excessive use in relation to the purposes; avoiding that the data collected be indexed, compared or saved without necessity; not indulging in video surveillance activities if the processing of personal data risks resulting in discrimination against certain individuals or groups of individuals owing solely to their political opinions, religious convictions, health or sex life, or their racial or ethnic origin; clearly informing individuals, in an appropriate way, by indicating the purpose as well as the identity of those responsible; guaranteeing the exercise of the right of access to images and recordings; as well as guaranteeing the security and integrity of the images by every technical and organisational measure necessary.

[1] Chamber ruling 28/01/2003 Peck v. United Kingdom App. 44647/98

The Council of Europe thereby encourages its members to make sure to lay down by law technical restrictions for installation limits of the equipment with reference to each place under surveillance; define privacy zones to be excluded from video surveillance by law, imposing the use of specialised software; provide for the practice of encoding video data, as well as provide access to a legal remedy in case of alleged abuse related to video surveillance.

In particular, it is necessary to note that the Parliamentary Assembly deems it necessary that a unified sign with an accompanying unified written notice be adopted as soon as possible and used by the member states. In view of the constant technical progress in the field of video surveillance, it stresses the need to continue the work on the issue of video surveillance in the future.

B. Other European texts

Like other European texts that can apply to video surveillance activities, it is necessary to mention in particular the European Union's Charter of Fundamental Rights. This solemn proclamation, adopted 7 December 2000 by the European Union, is henceforth mentioned in the Treaty of Lisbon of 13 December 2007, which went into force on 1 December 2009, in the article on fundamental rights. This aims at giving the Charter a legally restricting value (under strong restrictions for certain countries: Poland, the United Kingdom and the Czech Republic).

Article 7 of the Charter thus provides that '*Everyone has the right to respect for his or her private and family life, his home and communications*'.

In addition, Article 8 guarantees that '*Everyone has the right to protection of personal data concerning him or her'. It further specifies that 'such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority*'.

We must also point out that the European Data Protection Supervisor (EDPS)[2], who has competence for monitoring the processing of personal data implemented by European institutions, published a set of video surveillance guidelines, intended for European institutions and organisations (17 March 2010).

These detailed guidelines, elaborated following a consultation process, include a number of practical recommendations. In particular, they put forward the concept of 'privacy by design', according to which technical safeguards allowing for better protection of personal data and the private life of filmed individuals must be incorporated, beginning with the design, into the technological specifications.

C. Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 relative to the processing of personal data and the free circulation of this data

This Directive constitutes the legal instrument adopted by the European Union for setting the principles for the protection of personal data of European citizens. It is on the basis of this text that the member states adopted national legislations on data protection.

In principle, the Directive is applicable to video surveillance systems as soon as it applies to all information, including in the form of sound and images, concerning a person identified or identifiable, taking into account all the means that may reasonably be used by the person responsible for processing or by other persons in order to identify said person.

In fact, the images and sounds relating to natural persons identified or identifiable are considered personal data even if the images are used in the framework of video surveillance; even if they are not associated with data of the person's identity; even if they do not concern individuals whose face was filmed, even though they contain other information (for example, the number of his or her vehicle's registration plate).

However, video surveillance in public places is only partially the concern of Directive 95/46, insofar as it is not applicable to the processing of data in the form of sound and images carried out for purposes of public security, defence, national security, for the exercise of state activities in the domain of criminal law, or for other activities that do not fall within the field of application of community law.

Moreover, the Directive is not applicable to processing carried out by a natural person in the exercise of exclusively personal or domestic activities.

On the European level, the group of national data protection authorities (called 'group of Article 29' or 'G29') thus specified, in a 2004 opinion[3], the interpretation of measures of Directive no. 95/46.

[2] See the website www.edps.europa.eu

[3] Opinion of the G29 no. WP 89 of 11 February 2004

This opinion stresses, in particular, the necessity that the institutions concerned of the member states carry out, on the one hand, a general evaluation of video surveillance so that 'an over-proliferation of image-acquisition systems in public and private areas should not result in placing unjustified restrictions on citizens' rights and fundamental freedoms', which would make them 'massively identifiable in a number of public and private places'. It also calls for an assessment of the evolution of video surveillance techniques, 'in order to prevent the development of software applications based both on facial recognition and forecasting of the imaged human behaviour from leading inconsiderately to dynamic-preventive surveillance'.

These two messages remain topical since the definition of the most reliable tools and methods possible for evaluating the effectiveness of video surveillance remains crucial and indispensable.

II. NATIONAL LEGISLATION

A. A wide array of regulatory systems

In different member states, there are already cases of studies regarding video surveillance, which rely on constitutional norms or on specific legislative arrangements, prescriptions or other decisions issuing from competent national authorities.

In certain countries, there are also specific measures that apply independently of the fact that video surveillance does or does not include the processing of personal data. These arrangements also provide that the installation and implementation of a video surveillance system be submitted to prior authorisation on the part of an administrative authority, which can be represented, in full or in part, by the national personal data protection authority. Rules may vary according to the public or private nature of the person responsible for the functioning of the installation.
In other countries, video surveillance is not the object of specific legal measures. However, in certain cases, the personal data protection authorities have been able to play their role by means of opinions, guidelines or codes of conduct (United Kingdom, Italy), in order to guarantee appropriate application of the general measures for data protection.

The aforementioned G29 opinion of 11 February 2004 includes a summary chart of the principal known national legal sources regarding video surveillance within the member states on the day of its adoption.

NOTE: The list below is purely informative, and does not include any text that may have been issued after February, 11, 2004.

Belgium
Opinion of the Data Protection Authority, especially initiative opinion 34/99 of 13 December 1999, relative to the processing of images made in particular by video surveillance systems;
Initiative opinion 3/2000 of 10 January 2000 relative to the use of video surveillance systems in the entrance halls of residential blocks
Law of 21 March 2007 regulating the installation and use of surveillance cameras

Denmark
Synthesis law no. 76 of 1 February 2002 relative to the banning of video surveillance. This law forbids, in a general way, private entities from carrying out video surveillance on the public highway and in squares or any equivalent area of free circulation, whilst however

allowing for certain derogations to this ban.

Decision of the Data Protection Authority of 3 June 2002 concerning video surveillance by a large supermarket chain and direct transmission over Internet from a café.

Decision of the Data Protection Authority of 1 July 2003 by which video surveillance exercised by a private company of public transportation must be adapted and in conformity with the measures of the law on data protection.

Decision of the Data Protection Authority of 13 November 2003 imposing certain restrictions on video surveillance carried out by the authorities.

Two laws were adopted regarding video surveillance in June 2007: the first gives private enterprises the power to operate a surveillance of areas of which they are the owners, without obligation of prior declaration to the data protection authority; the second gives the police services heightened powers for imposing the installation and implementation of video surveillance systems on administrations or on private organisations.

Finland

In Finland, there is no special legislation concerning video surveillance but measures of a large number of different legislative texts apply to video surveillance as well as to other surveillance, observation and technical monitoring systems.

The mediator for data protection handed down an opinion on the recording of telephone conversations by customer services and in the workplace (file numbers 1061/45/2000 and 525/45/2000).

France

Law no. 78-17 of 6 January 1978 relative to data processing, dossiers and freedoms (CNIL)

Law no. 95-73 of 21 January 1995 relative to security (modified), decree no. 96-926 of 17 October 1996 (modified) and circular of 22 October 1996 (modified) on the implementation of law no. 95-73 oversees by specific regime prefectorial authorisation the implementation of video surveillance systems for security in public places.

The National Commission on Data Processing and Freedoms (CNIL), the data protection authority, published a Guide with recommendations concerning video surveillance in the workplace.

Germany

Article 6, point b of the federal law 2000

Article 25 of the law on the protection of borders.

Other regulations concerning video surveillance exercised by the police in Länder legislations on the police.

Greece

Letter no.390 of 28 January 2000 concerning the installation of a closed-circuit television system in the Athens Underground.

Directive no.1122 of 26 September 2000 concerning closed-circuit television.

Decision no.84/2002 relative to closed-circuit television systems in hotels.

Ireland

Law on data protection of 1998 and 2003

Study of case no. 14/1996 (use of CCTV)

Italy

Article 34 of the code for protection of personal data (D.lg. no.196 of 30 June 2003 bearing adoption of the code of conduct)

Decisions of the control authority (Garante) no. 2 of 10 April 2002 (promotion of the code of conduct); 28 September 2001 (biometric techniques and facial

recognition near banks) and 29 November 2000 (the 'Decalogue' on video surveillance) d.P.R. 22 June 1999, no. 250 (vehicular access to historic centres and areas of limited traffic)
D.l. 14 November 1992, no. 433 and l. n. 4/1993 (state museums, libraries and archives)
D.lg. 4 February 2000, no. 45 (ocean liners allotted to national voyages)
Article 4 l. 20 May 1970, no. 300 (workers' status)

Luxembourg
Articles 10 and 11 of the law of 02.08.2002 relative to the protection of individuals as regards the processing of personal data

Netherlands
The report of the data protection authority, published in 1997, contains guidelines concerning video surveillance, in particular with regard to the protection of individuals and property in public places.
Enquiry on video surveillance in all Dutch municipalities in 2003.
Modification of the legal code going into effect on 1 January 2004 and extending the field of application of infraction consisting of photographing places accessible to the public without informing people.

Portugal
Government decree 231/98 of 22 July 1998 (private security activities and self-protection systems)
Law 38/98 of 4 August 1998 (measures to adopt in case of violence associated with sports events).
Government decree 263/01 of 28 September 2001 (discothèques)
Government decree 94/2002 of 12 April 2002 (sports events)

Spain
Law no. 4/1997 (video surveillance by security forces in public places)
Royal Decree no. 596/1999 of application of the law no. 4/1997

Sweden
Video surveillance is specifically regulated by the law (1998:150) relative to general video surveillance and the law (1995:1506) on secret video surveillance (in criminal investigations).
In principle, general video surveillance requires the authorisation of a regional administration even though there are a certain number of exceptions, for example, as concerns the surveillance of post offices, banks and shops. Secret video surveillance must be authorised by a court. The Chancellor of Justice can appeal a decision of the regional administrative commission.
Video recording by digital cameras is considered processing of personal data and is therefore placed under the supervision of the data protection authority insofar as it is not specifically regulated by the law relative to general video surveillance.
An enquiry commission published a report on video surveillance (SOU 2002:110) in 2002.

United Kingdom
CCTV Code of practice (Information commissioner) revised in 2008

B. Towards specific European legislation?

This diversity of legislations, combined with the rapid technological advances of systems backs up the pertinence of a more harmonised legal approach. Several recent studies on the European level in fact lie within this perspective and recommend the reinforcement of European and national legislations.

In its report of 7 May 2010 on the role of data protection authorities in Europe[4], the European Union Agency for Fundamental Rights retains the development of video surveillance systems as a point of concern necessitating urgent action: '*Video surveillance in public spaces […] is widespread, but the legislative framework is lagging behind. As an example, the report reveals that in practice, CCTV cameras are often not registered and/or monitored in some Member States.*'

The report thus specifies that in Austria, the vast majority of cameras are not registered (and thereby elude the control of the data protection authority); that in Germany, certain cases of video surveillance in the workplace, unbeknownst to the employees, have been reported. It recalls that in Greece, the data protection authority was refused access to police premises where data processing was being carried out; and in the United Kingdom, there are few restrictions on the use of cameras in the public land, and there are more cameras in this member state than anywhere else in the world.

The Agency for Fundamental Rights thus deems that, whilst keeping in mind the intrinsic technical particularities of sound and visual data, as well as the potentially important impact on individuals' rights, a specific European legislative instrument should be envisaged in the future.

Finally, the Council of Europe, in its draft recommendation on the protection of individuals with regard to the automatic processing of personal data in the context of profiling, adopted 15 June 20102, observes that the gathering and processing of data for the purpose of profiling can use different types of data, such as coming from video surveillance systems.

In the absence of a European legislative initiative aimed at monitoring video surveillance operations in a specific manner, the players can rely on the opinions or sectorial recommendations of the national data protection authorities.

Some, out of a concern for ensuring the best legal supervision and the most coherent use possible of their video surveillance system, choose to provide themselves with a charter of ethics setting rules of good conduct and good management. It is in this perspective that the European Forum for Urban Security proposed its charter in the framework of the 'Citizens, Cities and Video Surveillance' project.

[4] Available for consultation on the website of the Council of Europe: http://www.coe.int/t/dghl/standardsetting/DataProtection/default_en.asp

Part II

➤ *Towards a Charter for the democratic use of CCTV in European cities*

“I call upon all elected representatives to examine and sign the Charter for a democratic use of video surveillance»

An interview with Charles Gautier, Senator and Mayor of Saint-Herblain and Chairman of the French Forum for Urban Security

➤ **With the Mayor of Rotterdam, you are one of the first two signatories of the *Charter for a democratic use of videosurveillance*. Why have a Charter?**

Charles Gautier: This Charter is the result of a European project for which several cities and actors involved in videosurveillance worked together.

For the past fifteen years, urban videosurveillance has developed rapidly in Europe, even though there are many significant differences from one country to another in terms of network density but also in terms of regulation and supervision. Nowadays, we are at the point where it has become necessary to reflect together upon this technology. Videosurveillance is not trivial. Because of its very nature, it invades the privacy of citizens whose images are collected from the streets in our cities without them knowing.

The EFUS has therefore launched a European project on videosurveillance, for which the French forum took on the role of expert. The aim was to organise debates on the political and social implications of urban videosurveillance. How should this technology be used? What are the legal and political frameworks? How is privacy guaranteed? Who is supervising? Who is watching? Who are we watching? What experiments conducted in such or such town or country can be used elsewhere? What lessons can be learnt from the “bad” experiences?

The Charter for a democratic use of videosurveillance reviews the key topics the team worked on. It mainly presents a number of founding principles to promote, as its title states, a democratic use of videosurveillance in compliance with citizens' fundamental liberties.

Who is the Charter aimed at and what is it used for?

I must first clarify that this Charter is, by no means, a statutory document requesting European cities to comply with a set of directives. It has been designed and prepared by these same cities to clarify a number of common ideas. It should therefore be considered as a tool that cities may use when defining the role of video surveillance in their urban safety policy as well as the practical details of its use. If you want, it's a sort of guide. It is also a declaration of principles.

In what capacity did you take part in this project?

Firstly, as the Senator and Mayor of Saint-Herblain, one of the ten partner cities in this project. Saint-Herblain is a city of 45,000 people, part of the Nantes population centre, in the department of Loire-Atlantique in the North West of France. The Nantes area comprises half a million people.

Saint-Herblain installed its first CCTV cameras in 1999. It now counts 18 cameras. As the mayor of this town, I have a clear political line: balance the need for public safety with the protection of individual liberties. The development of our CCTV system is based on this strategic choice.

I have also taken part in this project as a senator, as I was one of two rapporteurs, together with Senator Jean-Patrick Courtois, on a background report on videosurveillance for the Senate. Our recommendations followed the same line as the principles defined in the European project "Citizens, Cities and Video-surveillance".

Finally, I was involved in the project as the President of the French Forum, where discussions around this issue were also organised with elected representatives.

Is video surveillance a major topic for French elected representatives?

Undoubtedly. Not only because CCTV is an important component of urban safety policies but also because of the national political will. The government announced that, as part of the fight against terrorism, its objective was to multiply the number of CCTV cameras installed in France by three by 2011 in order to reach a grand total of 60,000 cameras. Large funds have been allocated to CCTV. Thus, part of the interministerial fund for crime prevention is dedicated to funding CCTV. It has also been funded by the departments, which spend a significant part of their allowance: at least 30 million Euros from a total of 49 million Euros in 2010.

What is the position of the Forum and of the French elected representatives on this issue?

We do not take a dogmatic position within our network. What's certain though, is that many communities are now trying to assess the efficiency of videosurveillance. They are also mainly trying to reconcile this technology with fundamental freedom.

There are many debates on these topics. As a summary, let's say there is a general consensus around four key principles:

Firstly, video surveillance is a tool which must be used as part of a comprehensive crime prevention policy. Not only technical aspects must be taken into account, but planning, human resources, financial cost and ethical dimension must also be considered.

Secondly, it seems fundamental that local communities invest in training their operators. The goals of local councils must be explained in addition to any training on the technical operation of the systems. Operators must be acquainted with the local safety and crime prevention policy as well as be informed of the objectives of their local council. They must also understand the current legislation, especially regarding the protection of privacy and individual liberties.

Third principle: the emphasis on establishing an assessment method for local video surveillance systems according to the objectives. These systems are costly for local communities. It seems therefore vital that the latter are provided with assessment tools, particularly to ensure the video surveillance system and other local safety operations are consistent with one another and, if required, to make the necessary improvements.

Finally, the fourth driving principle is that all video surveillance systems must be used in compliance with ethical principles. Two concepts seem particularly important: the transparent use of these systems and the traceability of the information gathered.

What does this Charter bring that didn't exist before?

As yet, there is no European text on videosurveillance. This Charter is therefore a first. It arises from the will of a number of European cities to create a frame of reference. This was needed by mayors as they are in tune with the safety expectations of their citizens, but are also aware of their fears regarding the protection of privacy. So this approach is anything but bureaucratic, trickling from the top down.

This Charter provides us, local elected representatives, with assessment criteria and practical recommendations in the current European and national regulatory framework. This is not a declaration in favour or against videosurveillance.

You have called upon your colleagues, mayors and European elected representatives, to sign this Charter. In practice, what does signing this charter change?

I am asking elected representatives not only to sign but also to examine this Charter for a democratic use of video surveillance as I believe it addresses an essential and urgent topic.

Nowadays, considering the expansion of video surveillance systems and their technological evolution, any mayor or local council representative (even for small councils) has to manage such systems and therefore take a stand.

This Charter allows elected representatives who wish to do so, the ability to use a number of principles which guarantee a democratic use of videosurveillance. Signing the Charter means we are publicly committed to ensuring the fundamental liberties of our city or local council citizens are protected.

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

VIDEO SURVEILLANCE IN FRANCE: KEY FIGURES

➤ **396,000** cameras are authorised in France - of which **20,000** in the public space (2007 figure)

➤ **9,772** permits have been issued in 2007 to public and private operators (an increase of 5 % compared to 2006) – of which 86% are for systems installed in public places or buildings open to the public and 14% used for monitoring public streets. *Note: This data should however be used carefully. Some systems have probably been installed without authorisation and have complied with regulations subsequently. Conversely, some authorisations have been granted but the cameras may not have been installed.*

➤ **1,522 French local communities** (out of a total of 36,682 on the 1st January 2009, according to the National Institute for statistics and economic studies) use at least one CCTV system.

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

THE FRENCH ARE LARGELY FAVOURABLE TO CCTV

According to a survey carried out in 2008, 71% of the French population is in favour of using videosurveillance in public spaces, and only 28% against it.

To the question "As a general rule, are you very favourable, rather favourable, not very favourable, not favourable at all to the use of CCTV in public spaces?",

➤ **21%** declared they were very favourable

➤ **50%** were rather in favour of CCTV

➤ **15%** were not very favourable

➤ **13%** were not favourable at all

➤ and **1%** had no opinion.

This survey was carried out between the March 14 and 17, 2008, by Ipsos, for the CNIL (National data protection authority), by interviews with a selected group of 972 people representative of the French population aged 18 and above.

Why (recommendations in the form of) a charter?

I. Why is a charter necessary?

➤ Through its project "Citizens, Cities and Video Surveillance", the European Forum for Urban Security sought to create an exchange of points of view and experiences about the use of video surveillance and its effect on the respect of individual rights and freedom. This project entailed, among others, a series of working visists in Genoa (Italy), London and Brighton (United Kingdom), as well as Lyon (France). Also, the partners of the project exchanged their experiences and analysed them. This work has enabled them to get an overview of video surveillance practices and of the methods put in place to ensure that the rights of citizens are respected.

What conclusions can be drawn from this project? What lessons can be learned from the experiences and know-how acquired by the cities involved? What advice can be given to the Efus partner cities and beyond that, to all actors involved in video surveillance? Are there codes of practice we can recommend?

Key principles for reconciling video surveillance and the protection of fundamental rights

Clearly, the project has identified practices which the partners have qualified as "good" when they are applied to a given problem, in a specific context. At the beginning of the project, the partners worked together to develop an interpretative framework for evaluating the different practices using the same criteria and addressing the same issues in each case: data protection, safeguarding the respect of privacy, citizen involvement at all stages of a video surveillance project - design, implementation, use, evaluation and system development. However, the partners thought that it would be hard to recommend to all cities to implement certain practices that had been designed and implemented by one city in particular, in response to a specific context. In fact, the project has shown that there is no such thing as a European code of practice, but rather, that it is interesting to exchange various ideas and practices so that each city may choose its own route to achieving the common goal: the protection of individual rights.

First of all, it was necessary to identify the general principles upon which the codes of practice were based. Secondly, the various challenges of video surveillance were examined. Finally, ideas for practices were drawn up in order to implement these principles, taking into account the challenges previously identified.

The idea of a charter for the democratic use of video surveillance that aims to be universally applicable and formulates the basic principles that should govern video surveillance is based on three considerations:

1) Principles that can be applied to video surveillance throughout Europe

When considering the use of video surveillance with regard to the respect of fundamental rights at European level, it is necessary to find a common denominator that can guide users outside of the various institutional, legal and cultural contexts. It is not a question of finding the lowest common denominator, but rather it is about finding the essential points on which everyone agrees, in the knowledge that each city or country is free to choose from a large range of options, and to adopt the solution(s) that best suit the country or region, depending on individual circumstances.

2) Principles that can be applied to all areas of video surveillance

The charter aims to draw up a set of norms which respond to all of the challenges of video surveillance. Partners have therefore tried to identify the basic principles that are the foundations of the right to respect of privacy in all aspects of the use of video surveillance. These principles are independent from one another, while also complementary. They can be applied to all cases in which video surveillance is used, whether in the project planning, system implementation, methods of use, data protection, or even evaluation of the system and possible modifications. It is only through application of these principles that the recommendations regarding the kind of actions to take become apparent. Then, the concrete examples of practices and techniques can inspire the implementation of actions.

3) Sustainable practices in a context of rapid technological development

Advances in technology and the constantly increasing capacity of video surveillance systems have been a key theme in debates regarding the protection of privacy. Systems are increasingly powerful and intelligent (automatic recognition of vehicles, people, behaviours, etc.) and increasingly often they are connected to other information systems. Video surveillance is just one aspect among many that make up the technological network that governs our cities, and which is irreversibly advancing, and at an exponential rate. This is why any recommendation on the correct use of video surveillance can quickly be overtaken by the technological reality.

On the other hand, technological advances offer new solutions to certain moral dilemmas. For example, systems exist today that can prevent cameras from filming the interior of private spaces (see Jeroen van den Hoven's article). For this reason, the recommendations drawn up in this Charter do not deal with practical methods for using this or that technique, but rather with the application of basic principles.

Nevertheless, one of the aims of this project was also to provide cities with concrete means of action. This is why the Charter offers, as a rough guide, a certain number of recommendations and practical methods.

It is also important to point out that the Charter for the democratic use of video surveillance *does not attempt to summarise all of the debates that have taken place within the framework of the project. However, the Charter cannot and does not claim to be a substitute for the exchange of concrete practices that has taken place as part of the project, of which this publication is a report. The publication is in addition to the charter and is the first step towards a practical guide.*

A European charter for cities and regions

The charter has not been drawn up based solely on the practices collected from cities. The debates are also clearly based on the national legislations in force, European texts and the first initiatives of local charters dealing with ensuring the respect of individual rights.

The Efus initiative is not the only one of its kind. It is more of a complementary project, which bridges the gap both at local and European level. Video surveillance is a European phenomenon that affects all citizens living, working and travelling in Europe. At the same time, video surveillance of public spaces is the responsibility of local authorities. The charter is original in the fact that it establishes a link between local and European dimensions.

The European texts regarding video surveillance can only provide the opinions and recommendations of experts. A charter for local and European collectivities reflects the commitment of all cities and regions throughout Europe to respect, locally, the principles guaranteeing the democratic use of video surveillance.

European institutions play an important role in the protection of fundamental rights and the protection of privacy: the Council of Europe Convention for the Protection of Human Rights (1950), article 8, Charter of Fundamental Rights of the European Union (2001/2009) articles 7 and 8, and the Council of Europe Convention (108) for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981, and Directive 95/46/CE of the European Union. They have also taken a position on the issue of video surveillance and have drawn up very similar recommendations to ours as contained in the charter, in the report of the European Committee on Legal Co-operation (CDCJ) (2003), Judgement 4/2004 (Article 29) of the Venice Commission Working Group (2007), in resolution 1604 (2008) of the Parliamentary Assembly of the Council of Europe, and the guidelines on video surveillance of the European Data Protection Supervisor (EDPS) (2010).

Although these very comprehensive texts have greatly inspired the project, they have not however clarified the principles on which the various recommendations are based. Although several countries have used the opportunity of the transposition of directive 95/46/CE into national law to also legislate on video surveillance, and although the conventions for safeguarding fundamental rights and protection of privacy result from European and international law, the European institutions do not currently have the power to legislate on video surveillance. They must make do with the opinions and recommendations and count on the fact that their message has been received, as well as on the good will of the parties involved. It is precisely in the absence of European regulation on the matter that the Forum's charter makes sense.

As regards national regulations, which dictate the restrictive framework for the use of video surveillance, they vary greatly from country to country (see Laurent Lim's article in this volume). While some countries have very precise legislations and regulations regarding video surveillance, others have kept a general legislation of protection of privacy and personal data. In some countries, a charter on video surveillance would be something of an innovation. In many others, the principles of the charter would complete the legislation in force and would above all highlight a political will and concern regarding the responsible use of this technology on the part of local authorities and representatives.

City involvement in the charter – a significant counterpart to the regulations in force.[1]

Charters and Codes of Practice are frequently referred to as forms of "soft law", as they do not typically give rise to substantive legal rights or interests. It would be wrong, however, to assume that Charters and Codes are not important forms of internal regulation. By providing a clear set of values and governing principles, they can play a pivotal role in shaping the organisational culture of CCTV schemes, and provide camera operators and scheme managers with goals that can be used to guide everyday decision-making. In addition, they can also serve as a benchmark against which the performance of a scheme can be measured, and provide the basis for the development of detailed procedures regarding the operation and management of a video surveillance centre.

Charters can also play an important role in public communication. By providing an explicit statement of the purpose and limitations of a given CCTV scheme, a Charter can help to provide the public with a set of criteria against which they can judge the continuing operation and success of the system. In this sense, it can provide citizens with a clear framework in which they can express their concerns or fears. Such a framework can consequently help to ensure that those responsible for the systems are both accountable and prevented from exceeding their democratic "surveillance" mandate.

As regards the relation between Charters, Codes of Practice, and official discretion, it is clear that to a large extent the importance of "soft law" will depend on local needs and conditions. In many towns and cities there is a strong assumption that CCTV schemes should be under the direct control of elected

[1] This part is by Benjamin Goold, University of British Columbia/ Oxford University.

public officials, and that their operation should be subject to the exercise of official discretion. Clearly, because Charters do not have legal status and are not legally enforceable, they cannot displace the operation of executive discretion, or be used to interpret or modify existing law. One of the advantages of adopting a Charter, however, is that it can provide a structure for the use of executive discretion, promote transparency in the use of CCTV, and help to ensure that the aims and objectives of surveillance are well-known and understood by the public. Finally, Charters can help new officials to understand the workings of CCTV, and ensure a certain degree of operational and managerial continuity after local elections and during other periods of political change.

In summary, the primary advantages of Charters and Codes of Practice lie in their ability to help shape organisational and managerial practices, promote accountability and transparency, and foster public understanding of CCTV. It is for these reasons that they can provide an extremely useful addition to existing legal rules and regulatory structures, and complement the exercise of official and executive discretion regarding the operation of CCTV.

This is why several members of the Efus such as Lyon and Le Havre have already created their own charter. This is also the reason why the Commission Nationale de l'Informatique et des Libertés (CNIL) [French National Commission for Information Technology and Civil Liberties] has supported this initiative and contributed to a similar initiative by the Article 29 working group, an initiative assessed by the European Data Protection Supervisor (EDPS). Therefore, the project partners believe that any initiative for the creation of a charter might be of interest not only to European cities and regions but also to any actors with similar objectives.

II. THE PRINCIPLES OF THE CHARTER

1. The principle of legality

1.1 – Why?

The Forum is built around the belief that “cities help cities”, which is the inspiration behind all of the European projects that they develop. Reflecting on the central theme of the video surveillance project, each partner city has expressed the desire to learn from the experiences and contexts of other cities involved in the project.

These are, above all, defined by the legislation in force. Referring to a principle of legality is has not been the obvious thing to do. In fact, should we talk about legality or legitimacy?

Legitimacy means having the right to carry out an action or occupy a position. For example, local representatives draw their legitimacy from elections, or policemen draw theirs from a status awarded to them. The only legitimacy that applies in all cases is that of the law. To declare legitimacy with regard to video surveillance is to declare that the first legitimacy of a CCTV system must be based on the legislations in force.

These legislations reflect a frame of mind and the choices of society. They are also telling of a culture, a history and relationships of power, balance or compromise between authorities/citizens, cities/State or even different regional levels.

They reveal relationships of trust or mistrust and are, essentially, a tool for legitimising a practice.
Legislation is therefore an essential basis for any project.

The first level of interest to partners is the community level. These legislations define the rules that are to be put into practice in all EU countries.

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

The charter therefore reminds us that:

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.

This being so, how can this principle of legality be put into practice?

This happens through knowledge of the legislative texts in force. The challenge for partners was to highlight those texts which do not specifically deal with video surveillance, but which should be taken into account by cities when installing their CCTV system, as well as their own legislation, if it exists.

1.2 – How?

➤ 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

➤ With regard 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.

By following this principle of legality, one thing becomes clear: respecting the regulations in force is the first act of democracy. These legislations, however different they may be, provide a framework for the development of video surveillance systems.

Taking into account the legislation in force guarantees sustainability.
This principle of legality provides a framework for the legitimisation and objectification of video surveillance, but like any framework, it must be clarified.

Putting the principle of legality into practice
This principle of legality exists in different forms throughout Europe. While in certain countries the operation of video surveillance is governed by a general law regarding data protection, in others, such as Belgium, Italy and Spain, the use of this technology is strictly defined. For example, in these countries the law imposes a technical setup of the system which enables images of private zones to be blocked (window and doors for example). The law also stipulates the duration for which personal data may be kept and makes it compulsory for the public to be informed of the identity of the authority responsible for the installation and management of the system. Regarding this last point, both Italy and Belgium impose a framework that must be respected regarding communication to citizens, requiring all cities to use the same descriptive signs and to make a certain amount of information clear, as specified by the law.

Another important aspect of the principle of legality relates to training of video operators. It is essential that these staff know the legislation regarding data protection. This is mandatory in some countries, such as the United Kingdom for example. In others, such as France, this training regularly features in ethical guidelines given to operators by local authorities. Finally, in other countries, this training is the responsibility of local authorities.
A third fundamental aspect of the principle of legality deals with the independent control procedures of the authorities. Many countries have therefore set up independent bodies to ensure that authorities using video surveillance systems are complying with the law. These include, for example, ethics committees in France, the “Garante de la Privacy” in Italy, or the Spanish Data Protection Agency (AEPD), which have, for example, the right to propose sanctions if the legal provisions are not respected.
The increasingly widespread use of video surveillance means that the law must be adapted so as to manage and restrict intrusions of privacy. Therefore, in the United Kingdom, a strategic national framework was defined in 2008 and the government elected in 2010 had included the issue of the protection of privacy with regard to video surveillance in its action plan.

Knowing and respecting the law is clearly an obligation *sine qua non*, but there is no reason why cities cannot take further measures beyond the law in order to guarantee the respect of privacy and fundamental liberties. Collecting experiences and drawing up recommendations on this matter was just one of the aims of the project which led to the creation of this Charter.
The law is not prescriptive: it provides a framework which enables systems to be implemented. This being so, which elements of a video surveillance system can be considered to be prescriptive? In other words, how can the principles of the charter be applied when it comes to installing and/or managing a video surveillance system?

2. The principle of necessity

All of the partners have observed that video surveillance is not a solution in itself but rather it is one of many tools that form part of a global security strategy. Faced with technological advances in video surveillance systems and the growing number of cities using them, it is important to remember that the installation of a system does not constitute an end in itself. It must be necessary.

But how can such a necessity be defined without lapsing into justifications of video surveillance?
How can a principle of necessity be defined, however, without prejudice to the freedom of each city to define its own strategic choices concerning security matters, with or without video surveillance? And furthermore, can it be said that necessity is, in itself, a fundamental principle?

It is never easy to define the choice of installing a video surveillance system as a necessity. This is because answering the question of whether or not it is a necessity, requires knowledge of the effectiveness of video surveillance. What part does video surveillance play in solving a specific problem? Does video surveillance seem to be the most appropriate response to a certain context?
There is no simple answer to these questions, which the partners of this project have discussed at great length. Scientific assessments offer mixed results, as show for example by studies carried out by the British Home Office (Welsh and Farrington 2002, Gill and Sprigg 2005, Gill et al 2005). First of all, it is advisable to work out the aim of the system: is it for preventing crime or for facilitating investigation *a posteriori*? As regards the expected effects, these can vary considerably over time and they are not the same for all types of crime. The role of *prevention* means that the potential criminal reasons and acts in a rational way. But as we well know, numerous crimes are committed with emotions “running high”. The effectiveness of video surveillance for investigational purposes is not guaranteed either, nor is its role in reducing feelings of insecurity.

There are so many considerations to take into account when talking about necessity. It is not a matter of necessity in itself, but rather a necessity that should be formulated in terms of a diagnostic process. It is reasoning which leads to the decision to install a video surveillance system, which reveals the necessity.

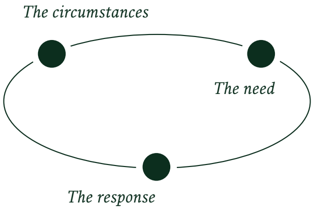
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

THE CHARTER DEFINES THE PRINCIPLE AS FOLLOWS :
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. The decision whether to install a video surveillance system or not depends on this principle of necessity. 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.

This being so, how can this principle of necessity be implemented. Using this principle, it is by focussing on reasoning that the installation of a video surveillance system is justified. This reasoning is structured around identifying the circumstances, defining the needs and the necessity of video surveillance as a response.

This principle of necessity is made up of three elements: :



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

Here, the charter uses a problem-solving method similar to that which is used by the British police force in its neighbourhood policing scheme. The "SARA" method is followed, which stands for *scanning* (reviewing a problem, a situation, circumstances), *analysis* (analysing needs), *response* (defining a response), and *assessment* (evaluating the response to the problem).
The approach is very interesting because it distinguishes between the problem to be dealt with and the symptoms observed. If the two first stages, "scanning" and "analysis", are not carried out thoroughly enough, there is a risk of achieving a response that only deals with the symptoms and not the real underlying problem.
In the case of video surveillance, the danger is that it is very tempting to think that it is the solution to everything, and that from then on, it is not necessary to follow through with the rest of the process. The key question is no longer "what is the most appropriate response to this problem?" but, "we want to install a video surveillance system, how can we justify it?".
The charter's principle of necessity takes a different approach, placing the problem before the solution, while considering that, depending on the case, CCTV may or may not be effective. This approach views video surveillance as one response of many, and it enables its effectiveness to be put into perspective compared to other urban security tools.

It is also very important to evaluate the system (the fourth stage of the SARA process). The principle of necessity does not just relate to the decision regarding installation of the system, but also to each development throughout its "life time". The issue of necessity is therefore a permanent one.
It arises, for example, when an expansion is planned. Is it a necessary investment for security[2]? It also arises if the initial situation changes. For example, what should be done when a significant improvement in security is observed? Is video surveillance still necessary? Although it would be irresponsible not to take into account the investments made, and although there is the question of what the consequences would be of removing the video surveillance, nevertheless, there is always the option of removing the cameras.

In this way, the city of Rotterdam at one time approved a project to remove some of its cameras, after carrying out an assessment. The residents of the neighbourhood concerned opposed the idea because they felt reassured by the presence of the cameras. Other European cities had the same experience, which reveals that the principle of citizen involvement may be more complex than you would think. In

[2] Obviously, the cost of enlarging a system is normally a lot less, because the expansion is able to take advantage of investments already made and no longer generates the same fixed costs.

the case of Rotterdam, the decision was taken *in fine* to reduce the number of cameras, offering an adapted response to a new necessity.

Another interesting example is the law in the German state of Baden-Württemberg. It stipulates that a video surveillance system can only be considered necessary if it is statistically demonstrated that an area is particularly prone to crime. In Mannheim, the local authorities and the police had to dismantle a system of six cameras installed in the city centre, approximately five years after it was installed, because the crime rate had significantly dropped. After the cameras were removed, the situation remained stable, which may also be linked to the measures taken by the local authorities, such as for example, development of public spaces and lighting.

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

RECOMMENDATIONS / FORMS OF ACTION

In this context, we can recommend that the principle of necessity should be applied

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 identified through the audit;

NEEDS

➤ Draw out the needs exposed by the audit and the analysis of local conditions. The needs should be as precise as possible as they will form the basis of the objectives for the project;

➤ Consider if there are less intrusive possibilities for responding to the problems to be addressed;

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 efficiently meet 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;

Once the necessity of the system has been established, the size and scale still need to be established, in relation to reasoning put into practice within the framework of the principle of necessity.
The scaling of video surveillance schemes should be done to the correct proportions.

3. The principle of proportionality

Proportionality is a principle that has always been hard to define. It can be defined as respecting a sound measure. But how can it be evaluated, when, and in relation to what? Furthermore, how can proportionality be defined outside of a specific context? How can something be stipulated in a European charter which is appropriate in a certain context, specific to a given city or region?

The main concern of the partners, when they debated this principle, was not to define a general norm, but rather to emphasise the need to scale the video surveillance system in relation to each particular context and to specific circumstances.

Comparisons are often made between video surveillance systems, based on the number of cameras. But this is not necessarily the best criteria because the number of cameras should be consistent with the needs identified in the city.

This principle of proportionality is based on respecting a sound measure. The deployment of a video surveillance system must be coherent with the reasoning recommended by the principle of necessity. This principle of proportionality is also linked to the principle of accountability. In fact, defining a system that respects a sound measure is an act of responsibility on the part of the authorities.

Therefore:
The design, installation, operation and subsequent development of video surveillance systems must respect a sound and suitable measure

The deployment of a video surveillance system must be appropriate and proportionate to the problem it is intended to address. The search for proportionality is above all the search for the adequacy between the objectives to be reached and the means to achieve them. The principle of proportionality is thus clearly a question of balance. This balance requires that video surveillance be not the only security and crime-prevention response developed in a location.

How should this principle of proportionality be implemented? The principle is applied to different levels of the definition and deployment of the system.

RECOMMENDATIONS / FORMS OF ACTION

Proportionality should be evaluated at each phase and with regard to each method of data-handling, particularly when it is necessary to define:

● *the number and scope of vision of cameras as well as their technical capabilities*

➤ The technical and human aspects of installation must be adapted strictly to needs. It is therefore necessary to use a technology that responds to the established objectives, without going further. The use of the video surveillance system should therefore be confined both in terms of time and space: on a given territory at a given moment to respond to a clearly identified need. Assigning any new function constitutes a new circumstance for the project, therefore requiring a repeat of the analysis carried out at the beginning of the project;

➤ Technical installation should include a system of concealment of private areas, through dynamic masking technology, since a public-space surveillance system cannot have as a "side effect" the surveillance of private spaces. The positioning and angling of the cameras, as well as their type (fixed or mobile) should also be adapted to requirements;

● *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;

It is therefore necessary to 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. In this way it will be applied most efficiently.

Proportionality put into practice....

The city of Saint-Herblain began, in 1997, a safety audit before implementing a CCTV system. This was carried out by an external agency. In parallel, the Security Committee of the "Conseil communal de prévention de la délinquance" (CCPD) was made responsible for holding a discussion regarding security in the city of Saint-Herblain. In 1998 it presented its report to the senator-mayor, who decided to create several working groups on themes involving security issues. In 1999, the group report of these working groups was presented to the City Council. Furthermore, an opinion survey on security, carried out using a representative panel, revealed that this issue was the main concern of the inhabitants of Saint-Herblain.

Building on all of these diagnostic elements, the mayor initiated a debate within the City Council regarding the application of the CCPD's propositions, which included video surveillance. In June 1999, the City Council voted for the installation of a system in the community and the creation of an Ethic Committee to accompany the implementation of this project.

In the case of Saint-Herblain, we can also see that the debate over video surveillance is part of a wider global consideration of security issues. The initial audit has enabled needs to be identified and to provide the elements for scaling the scheme.

Proportionality is applicable both when defining the scale of the video surveillance system and when integrating it into a local security and crime prevention policy. Video surveillance is integrated into a global policy and is proportionally coherent with other elements of the scheme.

This is because the installation of a system responds to a necessity and its deployment is carried out in respect of a sound measure that will be transparent.

4. The principle of transparency

Throughout the project, one of the essential issues for the project partners was to make video surveillance systems understandable to citizens and to guarantee the respect of individual privacy and fundamental rights.

Transparency is linked to the information that is given to citizens: which information is relevant? How much information should be given to citizens? Do citizens want to be informed? If yes, then informed of what?

The challenge of this principle is not so much affirming the need to inform citizens, but more defining the kind of information to be provided and the conditions of this information.

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. This principle is essential because 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/ FORMS OF ACTION

● The authority installing video surveillance cameras should give citizens clear information on:

➤ the project to install a video surveillance system;

➤ the systems' objectives;

➤ 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 identity, function and contact details of those 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 the rights of another. 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;

- The use of false cameras is discouraged. This misinformation is liable to discredit the system and bring its managers into question;

Transparency put into practice

All of the partner cities in the project have implemented a system for informing citizens about their video surveillance system.

In Rotterdam, for example, each time that a camera is installed, all of the actors involved are invited to see the control centre, including citizens. The experience has shown that transparency is highly appreciated and that it gives good results: 80% of the population asked in a survey aiming to evaluate the different security schemes said that they were in favour of the use of cameras, and only 1.2% were against, with the rest having no opinion. The problem arises when an incident occurs and there is no imagery recorded: then, the expectations of the inhabitants are more important.

The city of Lyon has also begun working strongly in favour of transparency through its ethics committee and descriptive signage. The committee has good visibility, as 30-40% of the population know about it. There is also descriptive signage which respects the regulatory framework and helps citizens to be better informed. At each site where CCTV is present, the signage is very clear and visible. The public is therefore informed that it may address any claims to the ethics committee. Furthermore, the ethics charter drawn up by the city of Lyon, which outlines the city's commitments in favour of protecting the rights of its citizens, is available at the city's website, at the municipal building of the arrondissement, the central town hall and in all the member associations of the ethics committee.

5. The principle of accountability

The principle of accountability must ensure that the responsibility for the system is assigned to a specific authority. It implies that these responsibilities are clear and understood and that this authority assumes all responsibility for the system.

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.

One might ask what accountability without sanctions would involve. The aim of the charter is not to define this, but to provide the responsible authorities with the marketing tools and to promote the practices of cities which oblige the operators to take responsibility.

The election of local representatives by universal suffrage is the ultimate measure of legitimacy and accountability. Elected representatives must shoulder their responsibilities under the scrutiny of the voters and risk not being re-elected if they are not seen to be doing this properly. It should be noted, however, that in the majority of cases, elected representatives are not usually directly responsible for a video surveillance system, particularly when they are not an exclusively municipal representative. In this case, identifying responsibilities is more complicated. This is why the principle of accountability relies on the principle of transparency.

The accountability principle does not just apply to the decision to install a video surveillance system, the correct operation of the system and the respect of the other principles. It also applies to the various different uses of the system, which should be in accordance with the objectives assigned to them. One of the risks is the phenomenon of “function creep”, in other words, the “sliding” towards new functions that were not planned for in the beginning and for which new justifications are found, or which are made possible thanks to technological advances. Logic should not be reversed and result in a system being used for something just because it can be, not because it is necessary (principle 1). If new functions are attributed to a system, the operator must be explicitly accountable for their application.

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

This is why the charter suggests the following recommendations and means 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 for publishing information required by citizens so that they may properly understand the use of video surveillance.

- Establish an appropriate mechanism for publishing information required by citizens so that they may properly understand the use of video surveillance.

6. Principle of independent oversight

One of the key ideas for a democratic use of video surveillance is to set up an independent control system for managers of video surveillance. As summarised by Richard de Mulder, of the University of Rotterdam, in the title of his speech at the project's final conference, "Citizen surveillance: no problem. But who oversees those in charge of the surveillance?". Citizens need to be reassured that the managers of video surveillance are respecting their rights. There is therefore a need for monitoring to ensure that system operators respect the rules and the other principles of the charter.

Independent oversight should not necessarily be carried out by a supervisory authority with powers to impose sanctions, the same as the public authority that regulated the video surveillance. The concept of independent oversight is both more flexible than the authority of the State, and more restrictive. **It reflects the idea of "check and balance" as the federalists called this principle, which was already the basis of the notion of the separation of powers as defined by Montesquieu (*Trias Politica*)**.

A hierarchy is not needed, but instead it is based on the idea that the responsibility does not lie with one actor alone. The video surveillance user's actions are observed (principle of transparency) and they must be accountable for their actions (principle of accountability). This monitoring must be carried out by a supervisory agent that is independent of the authorities that manage the video surveillance system.

Professor Richard de Mulder clearly explains how new technologies and video technology itself offer new powers to those who use them, which presents a new risk of an imbalance of powers and the system of check and balance that is the basis of democracy. The solution, in his opinion, is to install a fourth power (excluding executive, legislative and judicial powers), which would be responsible for monitoring/surveillance/supervision, i.e. implementing the *Trias Politica*.

There are already certain institutions exercising this "fourth power", such as for example the figure of the Ombudsman (mediator), which can supervise the correct operation and, yet more importantly, intervene when a system is not working as it should.[3] De Mulder also emphasises the fact that it is more important to ensure that an independent monitoring body like this exists, rather than trying to prevent any malfunctioning. The supervisor can, if needs be, intervene and rectify a malfunctioning. It is in this way that the oversight is independent.

The idea of oversight goes beyond the idea of authorisation. The process of independent oversight

[3] The media are also sometimes considered to be the fourth power. However, for De Mulder, the media can only partially fulfill this role, as they do not have their own agenda and their own interests, as well as the fact that they do not actually deal with the issues that are really the most important for society.

should be guaranteed for the duration of the scheme and should be applied to all of the challenges of video surveillance and all stages of a CCTV project.

This is why independent oversight is defined as:

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

Any control process entails the definition of norms. Independent supervision allows, thanks to these norms, to bring harmony to the various ways of implementing video surveillance following the guidelines of the Charter. Independent control can be carried out in various forms and at various stages of the development of a CCTV system. There can be an independent control during the conception itself of the system, so as to ensure that the response it will give does correspond to the problem that needs to be tackled. Also, the power to give the go-ahead to the installation of video surveillance can be given to an independent body.
Furthermore, independent control can be planned at further stages of implementation, such as the installation, the daily operations, the usage being made of the system, data protection, operators' training. Lastly, it can also intervene in the evaluation of the system and any decision to extend it or not.

The independent scrutiny might be carried out by a qualified individual or a specific body, including citizen participation.

There are many organisational methods for this independent oversight. Furthermore, in the vast majority of cases, it also exists to varying degrees. There are some authorities that give authorisation for installing a video surveillance system such as, in France, a departmental commission which is dependent on central government. In Italy, the data protection authority, the "Garante Privacy" plays a significant role in video surveillance, relying on detailed legislation, as in Spain, France and Belgium.

In cities, it is the city council that, traditionally, fulfils the role of supervisor and involved to a lesser or higher degree in managing video surveillance. The example of the city council also demonstrates the limits, because it is often the same majorities that decide and supervise the video surveillance. If the mayor is not elected by universal suffrage and is therefore independent from the majority in the city council, or if the opposition does not have a supervisory role, this can no longer be considered to be independent. In addition, the supervisor must be able to defend himself or be defended by an external party.

With the many checks and measures in place, the project partners identified two practices of particular interest, which both ensure supervision in very different ways. On one hand, an ethics committee (like the ones set up in Lyon or Le Havre in France); on the other hand, the figure of the "independent custody visitor" , as implemented in the county of Sussex in the United Kingdom.

Ethics committee (France)
The ethics committee is an institution specifically set up to monitor video surveillance, in the French cities of Lyon and Le Havre, with the specific aim of ensuring the respect of liberties. "Its formation re-

sponds to the objectives of balance, independence and plurality. It is made up of elected representatives shared equally between the majority and the opposition, of qualified individuals representing the legal, economic and educational spheres and representatives of human rights associations. It is responsible for ensuring, beyond the respect of legislative and regulatory obligations, that the video surveillance system set up by the city does not infringe fundamental public or private liberties. It informs citizens about the operating conditions of the video surveillance system and deals with any complaints." (Art. 4.1 of the ethics charter for video surveillance in public spaces in the city of Lyon). An ethics charter, like the one created by the city of Lyon or the one that the project proposes, can act as a reference point for the committee and regulate its operation. The committee ensures that the ethics charter is properly applied. To do this, it draws up a report every year regarding operating conditions and the impact of the system. Within this framework, it can ask the mayor to proceed with studies by independent bodies, as the city of Lyon is doing at the time of going to press (July 2010), with a global evaluation (technical and sociological) of its video surveillance system, carried out by the town and country planning faculty of the university of Lyon (professor Jacques Comby). Then, the ethics committee formulates recommendations for the mayor. In practice, the ethics committees of Lyon and Le Havre are very rarely approached by citizens, which might also be interpreted as evidence that they work well. Citizens know that an independent supervisor ensures the respect of privacy and monitors the correct operation of the system. Furthermore, it may deal with any issue that falls within its field of competence.

Independent custody visitors (United Kingdom)

The "CCTV" partnership that exists in the county of Sussex, involving the police and local authorities, has opted for another kind of supervision. The citizens themselves are invited to check the correct operation of the system and to check conformity with the Code of use. To this end, a group of a dozen citizens has been recruited following a call for candidates, in order to carry out "spot checks" of police surveillance areas and to ensure conformity with the Code of use. Furthermore, the independent custody visitors may go to review meetings of the police authorities and annual reports.

Checks can be carried out at any time, day or night, without previous warning. Mostly, the visits are carried out by two people. At the start of their assignment, these citizens are given training regarding the system and the Code of use, so that they know what they should be checking for. If they detect a problem or if they have concerns about something, they make this known to the police authority and video surveillance management.

Unlike the ethics committee system, this scheme mainly applies to the operation of video surveillance. That is why it is complemented by the work of the police authority involving local elected representatives. They work with the police on all of their activities, but also on planning, management, assessment and development of video surveillance systems. This scheme is particularly interesting for its simplicity, the involvement of citizens (principle 7) and its great transparency (principle 4).

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

Therefore, in order to apply the principle of independent oversight, we can recommend that:

➤ the independent authority is responsible, after studying the files, for providing the authorisations for the installation of video surveillance systems;

➤ the authority is responsible for ensuring that the implementation and use of the system respect the various regulations and norms.

7. Principle of citizens' involvement

This is undoubtedly the principle that is most directly linked to the theme of the European project "Citizens, cities and video surveillance": how can the rights and liberties of individuals be taken into account and how can citizens be involved in drawing up and considering the implementation of a local video surveillance system?

Involving citizens is not an easy task. How far should we intrude into the privacy of citizens in order to guarantee their security? How can citizens be involved in a system which is devoted to guaranteeing the confidentiality of the information which it creates?

Everything possible 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 / 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;

- 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 authorities' 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.

The principle of citizens' involvement in practice

For the cities involved in this project, this principle was already a reality, because the project for installing a video surveillance system came about in response to an increased demand for security on the part of the citizens. This is the case in the municipality of Ibiza (Spain), for example, which after having analysed the demands of the residents, the schemes already in place and their results, decided to install five cameras in areas where no other methods had proven to be effective.

Other municipalities, such as Genoa, Le Havre or Saint-Herblain, have organised public debates with the residents or meetings with neighbourhood associations in order to work out their needs and the best ways of responding to them.

In Rotterdam, this principle is integrated into all of the city's policies, including security policies. To ensure that the policies defined by the municipality adequately meet the citizens' demands, the municipality annually assesses the security schemes, which include the CCTV system. The mayor reserves the right to be able to install and remove cameras depending on the reaction of the public and the results obtained.

This principle does not only apply in the event that it has been decided to install cameras, or when assessing whether or not the response provided by the authorities has met the demands of the residents. It can be integrated into all stages of the implementation of an instrument of an integrated security policy, even in the operation of the video surveillance system itself. It is through consultation with residents that the authorities can choose the exact location for placing a camera, in order to make a space that is perceived as potentially dangerous more secure. This permanent dialogue strengthens the feeling of participation of individuals in political decisions.

The city of Liège organises "open days", when residents can go on guided visits of the control rooms. In Sussex, the population have voted overwhelmingly in favour of the "external visitors" scheme. These are just a few examples of the initiatives taken by responsible authorities to involve citizens in security policies.

III. TOWARDS A COMMON LANGUAGE FOR VIDEO SURVEILLANCE IN EUROPE: PROPOSAL FOR A COMMON SIGNAGE

How can we move forward together in the sense of creating a common language in Europe in terms of security and video surveillance? This was also one of the main threads of this project, focussing on the importance of communication that is transparent vis-à-vis the citizens. Faced with the increased mobility of people in and around Europe, it has become clear that there is a need to create common points of reference and to translate public policies into a language that is easy for everyone to understand. Hence the idea of proposing a common signage for cities using CCTV cameras. This proposal also responds directly to a demand formulated by the European courts: the Parliamentary Assembly of the Council of Europe called for the creation of European signage in its resolution 1604 of 2008, as did the Article 29 working group for data protection in 2004 with its Recommendation 4/2004 regarding video surveillance.

A primary study on existing signage has highlighted that there are some very good instruments for communication but that some shortcomings also exist. Some countries, such as Belgium or Italy, have a very precise legislative framework regarding signage, providing a fixed structure for all the details that need to be mentioned, including a standardised pictogram.

In others, the law states that citizens must be informed of the fact that they are in an area of CCTV surveillance, without giving precise details, and it is up to each authority to decide the way in which this communication shall be organised. It is in this scenario that one will find, for example, signs showing no pictogram, written in the language of the country only, therefore impossible for a tourist to decipher, without any information regarding the identity of the responsible authority.

In view of the results of this research, it was decided that the partners of this project would reflect on the creation of a common signage and the requirements:

➤ Signage should contain both text and images, so as to be understandable by anyone who does not speak the local language.

➤ The pictogram should reflect the current technological advances. Increasingly, "dome" type cameras are used in cities, and as they are new, they are not spotted or identified by citizens. By proposing a pictogram that resembles a dome, the project aims not only to inform citizens of the increasingly frequent use of this type of camera, but also to inform them of the existence of this kind of technology. Signage also plays an educational role.

➤ As regards the text, all of the partners agree that the word "video" should feature, because it is common to all European languages.

➤ It is also important for the term "public space" to appear, because it is necessary to signal that the public security policy concerns public and not private space.

➤ It was also deemed important to clarify the aim of the video surveillance system, so that inhabitants clearly understand the link between this instrument and the local security policy.

➤ The rules governing the transparency of public policies require the authority in charge of the installation and operation of cameras to be clearly indicated, and for at least one method of direct communication to be provided (telephone, website).

➤ Finally, the principle of legality - meaning that the installation and management of a video surveillance system can only be carried out in strict compliance with the law - should also be included in the signage and must mention the precise legal framework governing the system, along with the measures regarding data protection.

How would this signage be used?

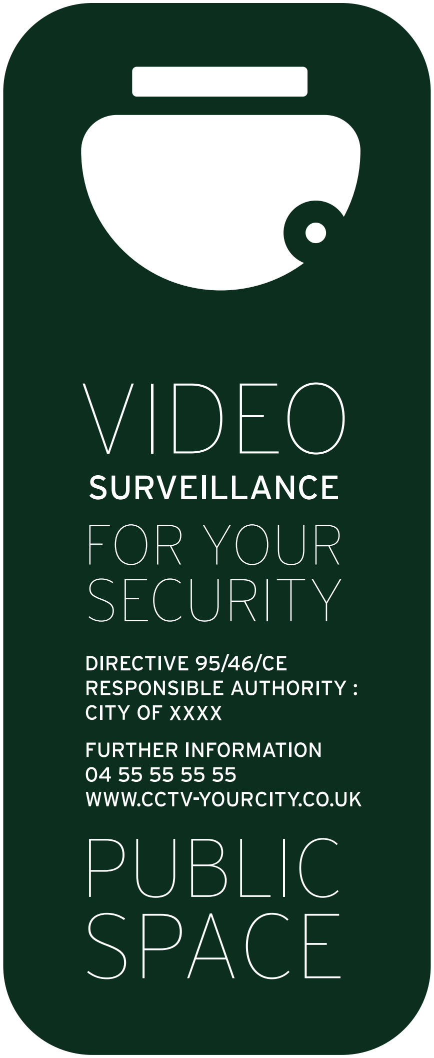
Insofar as the majority of cities have already implemented signage, the project partners obviously asked themselves what the added value of European signage like this would be.

Firstly, the Charter's recommendations for signage that provides maximum information might encourage cities to change and complete their own signage.

For cities that do not yet have their own signage, the recommendations can provide a guide that is easy to adapt, depending on the local context.

For other authorities in charge of financing video surveillance, such as regions or ministries, the above-mentioned elements can act as recommendations for the communication section.

Last but not least, the use of a common signage throughout the whole of Europe would contribute to a much greater transparency of public policies, thus benefiting citizens of all the member states.

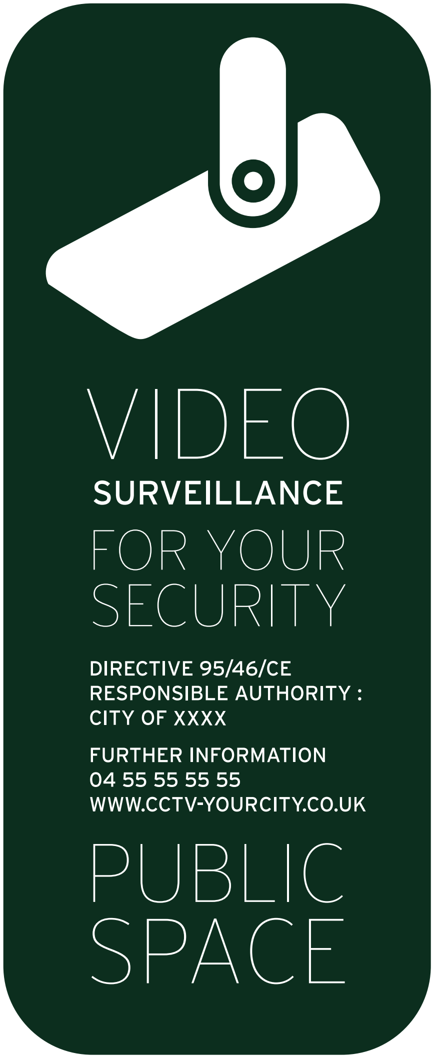


VIDEO
SURVEILLANCE
FOR YOUR
SECURITY

DIRECTIVE 95/46/CE
RESPONSIBLE AUTHORITY :
CITY OF XXXX

FURTHER INFORMATION
04 55 55 55 55
WWW.CCTV-YOURCITY.CO.UK

PUBLIC
SPACE



VIDEO
SURVEILLANCE
FOR YOUR
SECURITY

DIRECTIVE 95/46/CE
RESPONSIBLE AUTHORITY :
CITY OF XXXX

FURTHER INFORMATION
04 55 55 55 55
WWW.CCTV-YOURCITY.CO.UK

PUBLIC
SPACE

Part III

Zoom on the cities: How they use CCTV and how they protect fundamental rights and liberties

BOLOGNA

NUMBER OF INHABITANTS :
377,258

NUMBER OF CAMERAS :
291

RESPONSIBLE AUTHORITY :
City of Bologna

Video surveillance system: 'Integrated network system for protection and security'. The City of Bologna & The Emilia-Romagna Region

The city of Bologna's video surveillance project was born of the desire to find solutions to pressing problems such as the feeling of insecurity, which is linked to the presence of groups of drugs-dealers and the degradation of certain public spaces in the city's historic centre.

During April 2000, the municipal service responsible for security in Bologna conducted a survey of 753 of the city's inhabitants in order to improve understanding of their perception of insecurity. The results demonstrated that the problem of crime is rooted in a feeling of insecurity, especially in the historic centre of Bologna. In reaction to these findings, the city administration decided to install a video surveillance system in the north-east zone of the city's historic quarter.

In June 2000, this initial video surveillance project was presented by the city of Bologna to the Emilia-Romagna Region. The regional authority regularly funds improvements in urban security and public spaces, particularly urban renewal, street lighting and surveillance based on new technologies.

The project was 50 % financed by the Emilia-Romagna Region as part of a programme agreement signed in 2002 with the city of Bologna.

The total cost of the video surveillance system's installation was 1,829,164.80 euros. The cost of the network of fibre-optics transmitting the images is approximately 100,000 euros per year. There is also an annual maintenance cost of 50,000euros. Additionally, around 200,000.00 euros were provided in 2009 (66% financed by the Emilia-Romagna Region, the rest by the city of Bologna) to replace the oldest cameras (installed in 2000) and generally to improve the technological aspects of the system as a whole. The installation costs were equally divided between the city and the Region, while the operation and maintenance costs are met entirely by the city.

In total 291 cameras have been installed in the city. New funding by the Emilia-Romagna Region will raise this number to 315 by the end of 2010. The cameras are analogue and are equipped with nocturnal vision. Eighteen of the cameras are 'dome cameras' (these can be turned 360° horizontally and zoom). The images are transmitted by an analogue feeder network. Transfer of images between camera and recording system is by coaxial feeder cables, whereas the police operation centres are linked by fibre-optic cables. Future funding by the Emilia-Romagna Region will be used to connect the whole system with fibre-optic cables.

The Project 'Integrated network system for protection and security' is based on the installation of innovative technologies to prevent and limit the possibilities for committing a crime.

Images recorded by cameras on the busiest pedestrian routes and at bus stops in the town centre are sent simultaneously to the headquarters of both the national and municipal police forces. The National Police Headquarters can then send the images to the judicial authorities as items of evidence. The Local and National police can view the encrypted images and keeps them for up to 7 days until their destruction.

The operator in the National Police Headquarters of the Municipal Police station can:

➤ View the images from all cameras

➤ Control the cameras remotely

The Municipal Police manages the installation with the help of technicians from a private company and with the advice of the National Police. The National Police, the Municipal Police and the *Carabinieri* control the cameras.

In the Municipal Police's video surveillance central operations office, three police officers work relayed shifts to ensure 24 hour coverage.

Meanwhile, in the National Police headquarters, a State Police Inspector and two assistants are on hand twenty-four hours a day. The inspector and one of the two assistants have participated in training organised by the city of Bologna.

The choice of operators is limited by national legislation which restricts the choice to police officers of the judicial police. In total, the images are consulted by a dozen operators drawn from the national police, the municipal police and the *carabinieri*. The images cannot be shared in real time with other services.
Only agents of the judicial police can access the saved images, with the authorisation of a magistrate. To view the images, not only authorisation but also physically the key is needed. However, only the system manager has permission to consult the recordings and must use a specific access key.

The state police's role in real time is essentially repressive (following an alert raised by the cameras' images) but can also include a form of 'tracking' of suspects using the cameras' zoom capabilities.

The preventive function of the cameras is clearly linked to the increased risks faced by a criminal when committing a theft or other anti-social behaviour. A greater surveillance of the territory can give citizens a feeling of greater protection, with the possibility of a more rapid response from the Police.

The network has been evaluated before, during and after its functioning. Evaluation is carried out through crime statistics, reports of petty crime and anti-social behaviour, urban degradation and perceptions of insecurity.
However, it is difficult to measure precisely the project's results, as the crime statistics are not sufficiently detailed (notably from a geographic point of view) and do not allow a full analysis of the evolution of crime rates. The police forces have expressed their satisfaction, seeing video surveillance as an effective tool for the identification of individuals and for use in trials and legal proceedings (thereby a punitive aspect). The preventive aspect is less clear. Citizens' satisfaction is nonetheless high, even if the system does not meet all the expectations that were expressed before it was put in place. The displacement effects (relocation of criminal activities) are not quantifiable, due to a lack of reliable statistics.

Gian Guido Nobili

BRNO

NUMBER OF INHABITANTS :
405,352

NUMBER OF CAMERAS :
164

RESPONSIBLE AUTHORITY :
City of Brno

➤ The video surveillance system of the city of Brno (Czech Republic) was put in place by the national police and the municipality, within the framework of the Crime Prevention Programmes covering the period 1996 to 2008. The system includes 18 cameras, and its cost was roughly 627,000 euros (according to the exchange rate as of July, 15, 2010). These cameras cover mostly the city centre, various areas around the main railway and bus stations, and the city's busiest traffic areas.

Prior to the installation of the video surveillance system, local authorities conducted a series of investigations concerning safety in Brno, which included surveys among the population, socio-demographic analyses, and police statistics. The preliminary work also included interviews with local and national policemen, social workers, members of NGOs and other street workers.

The primary objectives assigned to the system were:
➤ to increase the feeling of safety among citizens in the areas of the city with the highest delinquency rates;
➤ to prevent crime;
➤ to facilitate the intervention of security forces when a crime is committed in the areas monitored by the video surveillance system.

Apart from this system, there are 57 other cameras installed in several districts of the city, operated by the municipal police and the district authorities. The total cost of this additional system is of approximately 2.3 million euros (according to the exchange rate as of July, 15, 2010). These cameras monitor areas considered as problematic, among others because of the presence of groups of people known to be prone to delinquency.

The CCTV system of Brno's public transport company is comprised of 24 units. Also, 38 tram cars are equipped with cameras. There are another 64 cameras installed by the city's road maintenance company. All of the above-mentioned joint stock companies do not provide in their official documentation (such as their annual reports) the amount invested in the installation of their CCTV systems, nor their operational costs.

According to the Czech law, CCTV operators can only be either the national or the municipal police. Financing is assured through the city budget or through subsidies paid by the Crime Prevention Programmes. The operational costs are paid by the police administration (both local and national), and by the Public Transport Company and Brno's Road Maintenance company. All the CCTV systems installed in Brno are part of an integrated network.

According to the regulation of the Office for Personal Data Protection -which has the authority to sanction-, private operators are allowed to monitor certain types of public areas such as parking lots, supermarkets etc. But their CCTVs cannot include the recording of images. Also, their images cannot be used in police investigations.

The video recordings from the CCTV systems of the city of Brno and the Czech national police are stored for 20 days and then recorded over. They can only be accessed by the national police (70 camera surveillance operators and three members of the police department of analyses). The criminal police and the road traffic police can also use recordings in the course of an investigation.

The recordings are kept in a special storage room at the national police's operational centre, to which no one has access except duly authorised officers, who receive a special training. The system is accessible through a code.

The Czech Republic's legislation on the protection of privacy is included both in the civil code and in the law on the protection of personal data. Czech authorities also apply the ISO code of practice for information security management (CSN ISO 27 001). Furthermore, there is a special police directive concerning the performance of the operational centre. The directives concerning the handling of video recordings are given by the national police. In order to control their application, a special section has been put in place in the national police, called the police administrator of personal data protection.

The current technology does not allow blacking out of private areas

One shortcoming that needs to be highlighted is the lack of information given to the public. People are only informed of the installation of new cameras through press conferences. On the other hand, in some problematic areas, the city has put up signs in the streets indicating the presence of video cameras, when actually there are no cameras there. This initative was taken because it does have an effect to prevent delinquency and increase the feeling of safety among the public, at a very low cost.

The city conducts regular surveys among its population about their feeling of safety and their appreciation of the CCTV systems. Surveys indicate that the majority of inhabitants have no idea where the cameras are installed although they believe that they are safer thanks to the CCTV. In 2005, 4.5% of respondents believed the installation of CCTV restricts personal freedom. In 2009, this figure had gone down to only 1.9% . Given the usual margin of error in such surveys, it is fair to state that the amount of people who believe CCTV infringes on personal freedom is now insignificant.

In fact, the video surveillance systems in Brno have not generated any kind of public debate nor opposition. There have been no public protests against it, nor any initiative in favour or against CCTV surveillance. All of the democratic political parties represented in the assembly of the city of Brno include in their programmes a chapter on safety and crime prevention. And from left to right, all of them are in favour of prevention.

Every phase of the installation of the video surveillance has been discussed in the Crime Prevention City Council, then recommended by the City Council and approved by the Assembly of the City of Brno. At the national level the Crime Prevention Department of the Ministry of Interior was consulted and the project has been approved by the National Committee for Crime Prevention.

The public is not allowed to see the video recordings, as stipulated by the legislation. In case of extremely serious crimes, the police is allowed to release some images to the media. This is done by the information department of the police, based in the regional headquarters of Southern Moravia.

The evaluation of the CCTV systems is carried out by the Crime Prevention Department of the Ministry of Interior, among others thanks to the information provided by the city and the police, including comparative analyses of crime and offence rates in the areas which are video-monitored and those which are not. It is worth noting that indeed, thanks to the video surveillance, there has been a decrease in crimes against property. Also, groups of pickpockets have left the areas under video surveillance and gone to other, less "attractive" zones. Furthermore, surveys show that citizens feel safer in the monitored areas.

All these elements show that CCTV systems can be considered a useful tool in the security policy of the city of Brno. It can be recommended in a functional, democratic society, provided data and recordings are properly secured by legislative and technical means, thus guaranteeing fundamental individual rights and freedom. The risk, as always when handling sensitive data, is in the human factor. We would certainly not recommend the use of CCTV in a non-democratic society where corruption, blackmail and extortion are commonplace.

Stanislas Jaburek

GENOA

NUMBER OF INHABITANTS :
610,766

NUMBER OF CAMERAS :
60

RESPONSIBLE AUTHORITY :
City of Genoa

CCTV in Italy led by the city council of Genoa

Italy witnesses an increase of citizens' requests in terms of security, despite the reduction, or at least the relative stabilisation, of serious crime. The factors contributing to the increase of this demand are essentially:

a) the media coverage of crime and the search for scoops, which can lead to the perception of exceptions as the general rule. The influence of a particular incident entails the risk of generalisation.

b) the fear of diversity, a challenge that we constantly face, because of the fast rhythm and the continuous evolution of social changes and difficulties in terms

of social inclusion;
c) the conviction that we should find a way to control all aspects of our environment, in its individual or collective components and therefore, we should be able to hold someone accountable for any negative incident that could happen to us, at least from the objective responsibility point of view;
d) the fact that 'our' behaviour is an independent variable and that someone else should guarantee our security.

In this framework, the intervention measures most called for are more severe sentences, more resources and powers for the police, and control technologies. Very often, the latter offers responses according to the circumstances and only in a limited number of cases.

In Italy, public order and security fall under the jurisdiction of the State. The recent legislation modification gives more competences to the mayors in terms of urban security, which they exert by means of ordinances and by developing CCTV systems.

In the city of Genoa, urban security policies started to develop in the mid 90s, following the increasing citizens' demand for security, which is addressed more and more directly to the elected representatives and especially to the mayors, while at the same time recognizing the role of the forces of law and order and of all the public authorities in charge of security.

Those security policies focused primarily on action in the historical city centre; they are part of the Urban II European Programme, which allowed, with the Police Headquarters' agreement, to install cameras, under the police responsibility, to watch a number of rough areas. Following the Security Pact concluded between the Interior Ministry and ANCI (Italian National Cities Association), the "Genoa safe city" Pact has been signed in 2007. Within this framework, a project to develop a local CCTV system has been funded. The main objective of the project is to establish a tool able to prevent criminal acts to happen, and to increase the citizens' perception of security.

In order to identity the city rough areas which would be appropriate to control with the CCTV installations, we considered necessary to involve the city council, as representatives of the population living in the areas concerned. Because we were convinced that spaces identification and choosing the technologies to adopt have to bring a real answer to the security need of the area and of the citizens, we initiated a location process of rough areas with a geo-classified information computer system, which enabled us to chose where to install the surveillance cameras. The results will be restored to the citizens via various forms of appropriate communication.

At the moment there are three CCTV systems on the city of Genoa territory. The first one aims to control traffic; it is composed of 38 CCTV devices watching the main roads. The National Police, thanks to its central control station, manages 97 surveillance cameras. Finally, in 2009, the first 60 cameras of the local CCTV system have been installed.

The main lines to ensure the appropriate development of the local CCTV system are announced in the personal data protection ordinance promulgated in 2004, in which are set out four general principles:
1-Legality
2-Necessity
3-Proportionality
4-Purpose

In order to ensure that those principles are respected, a special technical Commission has been created. It is composed of a representative of the local Police, a representative of the national Police and a government official, expert on CCTV. This Commission is in charge of identifying the spaces that should be subjected to CCTV, on the bases of the needs expressed by the citizens.

From a legislative point of view, image processing is generally assimilated to personal data processing. Given the great difference between the nature of images and the nature of personal data processed on paper or on computers, it was considered necessary to bring the images processing methods into line with the principles of the norms in force in terms of privacy protection, to guarantee the citizens protection and rights.

To that purpose, the city of Genoa elaborated a regulation, currently under inspection, which:

➤ Sets out the general principles that the local administration must respect in CCTV activities;

➤ Enumerates the objectives on which the administration can process images;

➤ Defines the scope of situations in which it is possible to apply these CCTV measures;

➤ Identifies the tools that can be used;

➤ Lays down the obligation of traceability of the access of recorded data;

➤ Defines the forms of communication to the citizens and decides of the period during which images can be retained, according to the different aims and objectives pursued;

➤ Recognises the rights of individuals being filmed, as well as those of the population in its entirety, and defines how those rights can be exercised.

The right of access to images from the people concerned should be proportional to the objectives of efficiency, of performance and of cost saving of public actors' action, of the protection of third party's privacy and of response to sensible requests, in the respect of fairness and efficiency principles of public administration, as enunciated in our Constitution.

It is undeniable that the importance of human and economic resources to implement CCTV systems requires verifying the efficiency of the choices made. In this optic, the city of Genoa equipped itself with a first tool, consisting of launching surveys of satisfaction to measure the perception of security of the citizens after the interventions, and of starting a research project to identify the impact of the city's policies in terms of urban security.

Mariapia Verdona

IBIZA

NUMBER OF INHABITANTS :
41,000

NUMBER OF CAMERAS :
4

RESPONSIBLE AUTHORITY :
City of Ibiza

The installation, in July 2009, of a video surveillance system in the city of Ibiza, capital of the Balearic island of the same name, was part of a series of measures taken by the municipality to rehabilitate the quarters of the historic centre, invaded by marginalisation and crime. Since 1987, the municipality has invested some 50 million euros in the renovation of the three most 'difficult' neighbourhoods of the old town —Sa Penya, La Marina and Dalt Villa— turning streets into pedestrian zones, creating new cultural areas, and improving infrastructures.

At the same time, the town council reinforced its crime prevention policy by increasing the number of community police in these neighbourhoods and, since 2006, by taking steps with the regional government to obtain the authorisation to install video cameras. The project presentation dossier included statistical data on local crime as well as newspaper articles devoted to crime in the old town. On the other hand, all the technical characteristics of the cameras as well as their planned emplacements were indicated in this dossier.

With a permanent population of some 41,000 inhabitants, the city of Ibiza (Eivissa in the local Catalan language) welcomes some 400,000 tourists every year. Thefts, minor drug-dealing, public drunkenness… The tourist success of Ibiza—one of the most heavily frequented sites of the Mediterranean and a Mecca of the legendary Spanish *movida*—has had a direct impact on crime, in particular that which is linked to the drug traffic. This is particularly substantial in the old town of Eivissa, the nerve centre of nightlife. According to information published in June 2006 by the local newspaper *Diario de Ibiza*, the reported crime rate in the islands of Ibiza and Formentera was, at the time, more than twice the Spanish average (118 offences per inhabitant versus 49.3 on average in Spain)*.

The town council requested the authorisation for a total of five video cameras, four of which were installed in July 2009. The cost of the installation was 89,600 euros, with maintenance being financed by the municipality.

Data protection and respect of private life

The town council is responsible for the storing of tapes, delegated to the municipal police, as well as their use or destruction. A team of eight video operators operates the cameras and has direct access to the images. Once these are recorded, only three police officers are authorised to view them. There is no other transmission, live or recorded, of the images.

However, the municipal police has, on occasion, turned over some tapes to the national police in the framework of its investigations.

The tapes are destroyed after a maximum waiting period of a month, unless they are being used in the case of an investigation on a serious crime or if legal proceedings are in progress.

When potentially criminal acts are taped, the videos are turned over to the legal authorities within a maximum of 62 hours after recording. When it concerns acts that may constitute an 'administrative offence' linked to 'civil security' (in the terms of Spanish law), the tapes are immediately turned over to the competent authorities in order to initiate criminal proceedings. In the event of the illegal recording of images and sounds, the tape must be destroyed immediately, in accordance with the Fundamental law 4/1997.

In the case where only partial destruction of the recording is necessary, and if total destruction is impossible or inappropriate for technical reasons or depending on the procedure used, the person responsible for storing the tapes must distort or block the sounds and images in question so as to make them unusable. This must be done according to the technical means available.

Public Information

The inhabitants of Eivissa were informed of the installation of the video surveillance system primarily via a campaign in the local press. The population of the neighbourhoods concerned was also informed by local authorities about all the measures of the law on personal data protection and recourse procedures in the event of anomaly. Furthermore, the inhabitants of the residential blocks where the cameras were installed were informed personally by those in charge of the installation, who requested their consent (even though this was not legally mandatory). On the other hand, one can note that, aside from the inhabitants of the residential blocks where the cameras were installed, the rest of the population of Eivissa was not informed as to the exact location of the cameras.

The setting-up of the video surveillance system provoked no contention or controversy. At very most, there were a few protests as to the waiting period for the installation, which some deemed too long.

Positive results

At the end of the first year of operation, the municipal team and local police judge the effects of the system to be positive. It has allowed for reducing criminal acts and also served in the framework of several police operations. Video surveillance therefore constitutes a useful complement to the work of community policing carried out in the quarters of Eivissa's old town. Generally speaking, this is also the opinion of a large part of the local population.

* 'Las Pitiüses duplican la tasa media de delincuencia por habitante de España', *Diario de Ibiza*, 6 June 2006

Manuel Ayala Garcia

LE HAVRE

NUMBER OF INHABITANTS :
180,000

NUMBER OF CAMERAS :
90

RESPONSIBLE AUTHORITY :
City of Le Havre

➤ In Le Havre, we have set up a permanent partnership with State services (the Subprefect), the Justice service (District Attorney), the National Police (the Chief of Public Security for the Arrondissement of Le Havre), the National Education service (Local Education Authority Inspector), who we meet with fortnightly, along with the Deputy Mayor, the Deputy Head of Security and the Municipal Security Department, within the framework of the limited unit of the Local Security and Crime Prevention Committee [*Comité Local de Sécurité et de la Prévention de la Délinquance*] (C.L.S.P.D).

➤ We have, since the first discussions regarding a project for the installation of video surveillance, submitted this question to our partners to get their opinions, then at each stage of the implementation, realisation, creation of a possible Ethics Committee, its composition and will pursue these exchanges whenever it seems necessary to extend areas of video surveillance.

➤ Sometimes, at the request of the National Police, we plan and propose a sustainable expansion of the system, depending on the number of actual incidences of crime in an area or neighbourhood.

➤ It is only after collective consideration, and always in due course, that we put extra cameras in place, and not by way of reaction to the demand of a fellow citizen, who may have been the victim of a crime.

There are so many requests for cameras, coming from all areas of the city, and from private individuals, shopkeepers as well as business owners, that we simply cannot respond to them all.

Between 2004 and the end of 2005, the date that the first three cameras were installed in a neighbourhood shopping centre which was going to close due to crime, which we succeeded in stamping out, the Deputy Head of Security informed the City Council of the project, and received representatives from various forms of the media: written press, radio, television and associations: the Human Rights League, neighbourhood associations and all residents of Le Havre who requested meetings to find out about the scheme. The maximum amount of information was communicated before, during and since the installation. This information was precise, transparent and in full.

We believe that urban video surveillance is a useful tool for security policies and crime prevention within the framework of the City of Le Havre's local security contract. It aims to prevent incidents involving people and property, to contribute to the feeling of security of individuals and to ensure the security of communal buildings and exposed public spaces.

This measure should accommodate the need to respect public and individual liberties, in accordance with the ethos of the Law on the Orientation and Programming for Internal Security (LOPSI) of 21 January 1995 and its decrees affecting the application thereof.

Out of a permanent concern to ensure that citizens have the maximum level of protection, the City of Le Havre created an ethics committee for video surveillance of public spaces.

This Ethics Committee is composed of three colleges:
➤ three elected representatives, one of whom is chosen by the municipal opposition.

➤ three qualified individuals:
- the ex-vice chancellor of the university
- a former President of the Bar of lawyers
- a representative of the Chamber of Commerce

➤ three representatives of associations:
- the chairman of the association Aide aux Victimes (Victim Support)
- the chairman of Conseil Supérieur des Sénégalais du Havre (Superior Council of the Senegalese people of Le Havre)
- the chairman of a social workers association

The ethics committee for video surveillance of public spaces is therefore responsible for:
➤ ensuring that public liberties are respected at all times
➤ informing citizens about the operation of the system
➤ examining, at the request of the mayor of Le Havre, any requests for access to images or other citizen complaints
➤ articulating opinions and recommendations to the mayor regarding the operation of the system
➤ presenting an annual report to the mayor of Le Havre with regard to the operation of video surveillance.

All of this information, and the reality of its usefulness, mean that there is currently no (or only very slight) opposition to operating CCTV protection in our city.

Bertrand Binctin

LIÈGE

NUMBER OF INHABITANTS :
190,000

NUMBER OF CAMERAS :
109

RESPONSIBLE AUTHORITY :
Police/boroughs

Presentation of CCTV use in the city of Liège,

➤ Liège, a thousand year old city, a city known for its century-old university, is a major economic and cultural engine of Wallonia. In the heart of a metropolitan area of 600,000 inhabitants, it is located at the crossroads of the fast railway “TGV” and trans-European roads networks, 100 km away from Brussels, 25 km away from Maastricht, and 40 km away from Aachen.

This fervent city, day and night, favours friendliness and hospitality. It receives many big sporting, festive and cultural events.

Since 2002, the CCTV renovation project was entered amongst the priority action proposals, subject to the citizens’ choice as part of the section “A safe city” in the citizen consultation about the City Project. The vote turned out overwhelmingly in its favour.

Since then, at the request of the Town Mayor, the services of the Liège Local Police Area have been installing successively a total of 109 surveillance cameras from 2003 to 2008.

On a technological aspect, the cameras are high technology “speed domes”, high-definition, allowing 360° rotation horizontally and 90° vertically. The zoom enables to read clearly a number plate 150 metres away, day and night.

All the cameras parameters are defined in a way that visualization is not possible in a private house. They are not equipped with an intelligence operating system, thus the importance of having in front of the screens properly trained staff who knows the neighbourhood they are watching and its usual population.

They are all interconnected with a closed circuit of optical fibres – thus excluding any hacking risk – and visualised in the Events Management Centre as well as in two Local Police Stations. The data are not shared with any other service or institution.

Visualisation is carried out exclusively by police officers – personnel on oath, bound by confidentiality.

The images are recorded and deleted after seven days, whereas the Belgian Law allows keeping images up to a month.

Individuals can request to visualise images concerning them, through a claim to the system administrator, who is the Town Mayor. Appeal against the system administrator is possible.

The tribunal prosecutor department and the examining magistrate can also seek images if they might interfere in a penal case.

The cameras installation location has been chosen according to the objectives pursued by this system. The aim is to provide a quality solution to the three types of issues raised below:
➤ circulation issue, with the viewing of the major roads penetrating into the city,
➤ law and order issue, with the viewing of recurrent demonstration places,
➤ security and environment issues, with the viewing of some sensitive areas such as the main nightlife streets.

Information signs are put on display in the urban area, indicating who is the system administrator.

For each of the four successive stages, the files had to be approved by the local Council, where concerns regarding respect of individual liberties have been publicly discussed.

The objectives pursued and the specific locations of the cameras are regularly promoted through the media via communiqués and press conferences.

Information to the population is also provided through contacts with local committees, before the installation as well as after, as part of the continuous assessment of the system. People attending those meetings are therefore openly invited by the Town Mayor to express their wishes concerning the cameras.

In 2007 was established a Local Control Commission, composed of representatives of each of the four democratic political groups represented in the Liège Local Council. They meet every two or three month.

The Local Control Commission objective is to guarantee the implementation of the 2007 Belgian Law.

In particular, it makes sure that:
➤ viewing in the "cameras" centre is carried out exclusively by police staff specifically trained;
➤ the statement to the Privacy Commission has been correctly fulfilled;
➤ parameters hide the private buildings particular areas;
➤ information signs in accordance with legal decrees are installed in the streets concerned;
➤ the images are retained, then destroyed after 7 days.

The town councillors are regularly informed of assessment elements: the results of the Local Control Commission works, Police special Commission meetings, Events Management Centre visits…

Such visits of the Events Management Centre are regularly suggested to the general public, as part of the Police "Open day" for example, and are always a success.

In terms of cost, the overall system installation represents a sum amounting to over 5 millions euros. The operating costs are null, since the red rests on optical fibre. However, an annual budget of around 100.000,00 euros for preventive maintenance has to be expected. Moreover, it is possible to adapt the installation to technological evolution by purchasing specific computer software.

The system impact is considered positive in terms of deterrence and security of the population; however there is still no extern assessment of the system.

Over a year period, the cameras enabled to constitute 54 red-handed criminal acts and brought 58 positive results to investigation follow-up requests.

Catherine Schlitz

LONDON

NUMBER OF INHABITANTS :
7,684,700

NUMBER OF CAMERAS :
600,000

RESPONSIBLE AUTHORITY :
Police/boroughs

Description of the project to create a CCTV installation

➤ The London experience, indeed the UK experience, with CCTV does not take the form of a single project. In the first instance, London is divided up into 33 administrative areas, each with its own CCTV system. In addition, there are many other schemes to which public authorities have access and there are also many private CCTV systems which cover public space (cameras owned by business covering access and exit points).

The use of video surveillance has been growing exponentially over recent decades. Initially cameras were introduced to control traffic in the 1960s. Later systems were introduced into large retail settings (1970s and 80s) where there was a certain ambiguity about the nature of the space. In other words, in large shopping malls the thoroughfare between individual retail units feels like public space although it is in fact private. Most of these malls are patrolled by private security guards, usually with a protocol with local police allowing/encouraging regular patrolling by them also. In addition, CCTV has been used for some time to manage large sporting events – notably football matches where it has proved a successful feature of the strategy to remove violence from the stadia and their environs. All this, coupled with an extended period with a real threat of terrorism has combined to acclimatise the UK public to the use of video surveillance. So complete has this been that very often it is communities themselves that demand the installation of cameras.

The desire to reduce crime has been a consistent factor in the development of schemes with the obvious additional potential objective of preventing terrorism as well as providing a valuable detective option. The use of CCTV is now so pervasive that there is a broad underlying assumption that one is being observed by camera even if this is not in fact the case. Most if not all of the town centres across London are covered extensively by CCTV cameras. It is not easy to say with any precision how many cameras there are, however, the Command and Control Centre for the Police is capable of accessing over 60,000 cameras. As a guide, Heathrow Airport alone has some 3,000 cameras.

It has been argued, with increasing determination, that the use and placement of cameras has been somewhat indiscriminate. It has tended not to take heed of the potential impact on the displacement of criminal or anti-social behaviour and, furthermore there is little evidence that once an identified problem has been reduced that cameras are removed or redeployed. These issues are now being addressed in a more structured way through the development of a national video surveillance strategy under the guidance of the Home Office. Clearly, this activity comes long after the use of such technology is well established. Indeed, we are into a second or even third generation of such technology as local authorities and their partners upgrade their systems to take advantage of recent developments in this field. For instance, there is a broad shift from analogue to digital technology and an increased use of dome cameras, with the particular advantage that those within the area being viewed cannot be sure which direction the cameras are facing. Of course, it is a common theme with popular technology that the desire to obtain the latest equipment obscures the rational reflection on what level of technological complexity best fits a given situation – the easy analogy being the purchase of a Ferrari to go to the supermarket shopping! There is now a growing desire to examine the benefits accruing from such systems, given the considerable costs involved. However, it would seem that the removal of systems would be a politically difficult decision.

With the emergence of local authority CCTV systems, from the mid 1980s onwards, there was a presumption that these systems should be under the control of these local authorities rather than the police. However, it has been a consistent feature of the approach that the police have had ready access to the cameras, either through officers in the control rooms or by having live images relayed to police control rooms and even with staff there being able to take control of the cameras to monitor specific incidents. The rapid development of partnership working between the police and local authorities has seen the further blurring of distinction between police and local authority in terms of controlling CCTV. A number of CCTV control rooms are now co-located with police control rooms and although the CCTV operators are local authority staff, there is constant police access to the live images.

A number of local authority control rooms have the facility to run sensitive operations from rooms within the complex which allow the monitoring of cameras in isolation from the main bank of monitors and without the direct knowledge or involvement of the operators. The obvious application for such a facility would be a live anti-terrorist or other major crime operation. This might be a good point at which to address some of the human rights and privacy issues!

The legislation affecting this area includes the Human Rights Act and also Data Protection Act. It should be noted that there is no specific statutory provision for video surveillance in the UK. However, the legislation, including the Data Protection Act applies to anyone and is not limited to public bodies. Alongside this, as noted above, the national CCTV strategy envisages the development of a code of conduct covering all aspects of video surveillance and, in common with other states, the UK uses various technologies to protect private space from intrusive surveillance. For instance, the practice of greying out or obscuring those parts of the camera image that involves private space is common to the Local Authority owned systems. An example would be where there is residential property above retail or commercial property on a High Street. As a camera moves across its range of observation, as it takes in the private areas, these are automatically obscured. However, there is scope to override this technology (with appropriate authority) for situations that demand it. Such situations would be restricted to serious crime including terrorism and require very high level authorisation.

All premises covered by CCTV must carry signs that indicate the presence of CCTV and how to contact operators if desired. However, it would seem that cameras are now so ubiquitous that such signage is largely ignored. As noted already, work is ongoing with regard to a national strategy for CCTV usage. The relevant documents can be found on the UK Home Office website. At the time of writing, the newly elected coalition government has indicated its intention to increase the regulation of CCTV. This will affect the implementation of the National Strategy but, as yet, details of the enhanced regulatory framework are not known.

There are already codes of conduct which apply to the operators monitoring the systems and these form the basis of the training they receive. For the most part CCTV control rooms are themselves subject to video surveillance around the clock – an example of ‘watching the watchers’! Furthermore, there is the practice of ‘lay visitors’ calling in to CCTV control rooms. The scheme comes from that which operates in respect of the access to detained persons in police stations. Volunteers from the community are permitted immediate access to the custody area and the opportunity to speak to prisoners to ascertain the conditions of their detention. In a similar manner, volunteers can attend the CCTV control room, unannounced, to speak to operators and to satisfy themselves that proper procedures are being followed.

There is, in all areas of public service provision, a drive to get citizens more actively engaged in the decision making process. In the context of policing, this can be observed in a number of ways including, by way of example, the neighbourhood panels. This initiative which is part of the national Neighbourhood Policing approach, brings together individuals from across a local community to set priorities for policing and to hold the local police and partners to account for their performance against these priorities. Such bodies can be the catalyst for the installation of CCTV systems.

The public perception being largely positive regarding the potential benefits of video surveillance, such groups become campaigners for local schemes. It can even generate the possibly counter intuitive image of the police seeking to dampen the enthusiasm for CCTV, pointing out that its place is always within a broad package of measures to address an identified problem that has been properly researched.

There is, over more recent years, an emerging groundswell of opinion in favour of caution though not outright opposition in respect of CCTV. This caution seems to be as much about cost versus the perceived benefit as about the invasion of privacy. It should be seen to derive from the experience in situations where cameras were deployed without proper thought or without the resources to respond effectively to what was observed; nothing more quickly diminishes the value of CCTV than the widespread perception that no one comes even if there is a crime taking place under the gaze of a camera.

As with any community safety or policing activity the task of evaluating the effectiveness of CCTV is a complex one. The assessment of performance against objectives is difficult if the objectives themselves are confused. For instance, does 'effectiveness' mean prevention or detection? Is there an intrinsic and measurable value in the perception of safety apparently engendered by CCTV? How are the effects of CCTV to be separated from any other intervention that may have been put in place to counter an identified problem?

There appears to be some evidence that CCTV can reduce crime and anti-social behaviour, although it is less certain that this effect is necessarily long term. There is some evidence that CCTV is of value in relation to major crime such as terrorism – even suicide bombings – perhaps more in relation to the curtailment of the necessary reconnaissance planning phase that precedes an attack.

There is perhaps somewhat more evidence that CCTV can provide valuable support for investigators. At its simplest, it provides often irrefutable evidence of conduct as well as identification evidence - it should be noted that research suggests that the existence of CCTV evidence leads to a high percentage of guilty pleas, obviating the need for a trial and resulting a cost saving. Furthermore evidence suggests that where CCTV footage is shown, a more severe sentence is imposed.

With regard to reassurance, again the picture is confused. The use of CCTV is so pervasive that in many situations it is ignored. At the same time, there might be a question about its tendency to increase fear in those areas not covered. The human need for security is its own driver for demanding more and more reassurance be that a police officer on every corner or a camera on every lamppost!

In conclusion, CCTV is a valuable tool in the community safety toolkit but it is not a self-contained answer; it must be part of a planned, well-researched and coherent strategic response. Its effectiveness needs to be established according to the objectives behinds its implementation on a case by case basis. The objectives will vary across the spectrum of crime types and physical locations and therefore the evidence of success will vary accordingly.

Andrew Bayes

LYON

NUMBER OF INHABITANTS :
472,000

NUMBER OF CAMERAS :
219

RESPONSIBLE AUTHORITY :
City of Lyon

Video surveillance ethics committee, Lyon

Ever since the city of Lyon decided to implement a CCTV system, it was also decided to set up an extra-municipal committee, named the *collège d'éthique*, or ethics committee. As the natural chairman of this committee, the mayor of Lyon delegated this mission to an independent agent, Jean-Pierre Hoss, member of the Council of State, who also filled the committee's first term of office. For the second term of office he was replaced by Daniel Chabanol, honorary member of the Council of State, and former chairman of the administrative court of appeal of Lyon.

The committee was formed with diversity in mind: besides the elected representatives of all political tendencies (including the opposition), other members of "civil" society form part of the committee, including representative of associations, such as the Human Rights League, or qualified individuals including an honorary President of the Bar of lawyers, and an honorary chief education officer of the Academy of Lyon.

The official mission of the committee is based on three main themes:

➤ Drawing up and continuously updating a set of recommendations for video surveillance: work which was accomplished under the chairmanship of Mr. Hoss, but which must be resumed in order to take into account legislative developments with regard to the issue. The aim of these recommendations, proposed by the elected representatives, is, while respecting legislative decrees, to define the complementary methods for capturing and using images for the purpose of increasing the guarantees for users of public space. Current discussions underway (besides the insertion of new legislative norms) are focussed on the right of access to images and their potential use: can people who have been filmed obtain the right to access the images that concern them; by what means / which authorities can see the screens in "real time" and for what purposes / who can access the recordings, and under what conditions?

➤ Receiving complaints put forward by people who have been filmed, providing advice about keeping images and making any proposals to this end. It should be noted, of course, that this activity is marginal, as serious complaints of this sort are extremely rare: by definition, people who might be filmed under questionable circumstances (for example in a private space, in the event of a malfunctioning of mechanisms that they disagree with), or whose images might be kept beyond the legal time limit, or might be seen by unauthorised persons, would not know that a breach or violation had been committed, and would therefore not have the chance to make a complaint…

➤ Creating a database of practices related to video surveillance, that are observed both in France and in other European countries. This objective is twofold: on one hand, this data must enable the issue of the usefulness of video surveillance to be dealt with in the most scientific way possible. We should point out that the city of Lyon - overseen by the ethics committee - has launched a university study dedicated to this issue: a PhD student is carrying out research within a strict university framework (Lyon-II and Geneva Universities), backed by financial support from the city, with full guarantees that the work will be carried as a completely independent university study.

On the other hand, contacts linked with this data collection should eventually lead to the implementation of a network of municipalities, the idea being to create a sort of spin-off of the Lyon institution.

Beyond exercising these powers, it is essential to point out that the existence of the ethics committee and the exchanges that are fostered through its meetings, by diffusing an often heated debate, lead to a calm and peaceful discussion of a delicate subject. Obviously this is not to say that a "loose consensus" takes the place of a necessary debate on an issue that is fundamental to society. This would not be desirable, and it is not the case. The opposing parties are present and vigilant and there are constant arguments between the enthusiasm of one side, and the restrictions of the other. But this enriches the discussion, much more than having static presentations from two fixed positions. And that is the essential contribution that our ethics committee makes.

Manuel Magne

ROTTERDAM

NUMBER OF INHABITANTS :
589,615

NUMBER OF CAMERAS :
289

RESPONSIBLE AUTHORITY :
The police

CCTV in Rotterdam: retaining an effective system, while managing expectations

➤ Rotterdam's participation in the Efus project on camera surveillance fits in with our aim to improve our CCTV system. What options do we not yet use? What is the balance between technology and the ability of individuals to respond to all these incidents? How do you interpret the concept of privacy in public spaces?

This article discusses our experiences with camera surveillance in Rotterdam, the rules under which our camera surveillance operates and what particular issues Rotterdam is still working on.

Experiences

Every city is trying to get a grip on crime and public nuisance. Every city is seeking smart and efficient methods to increase safety. Every city can make use of technological innovations. Rotterdam is no exception. Camera surveillance aims to reduce public nuisance and crime and increase the sense of safety and security among its population.

The very first cameras were installed in Rotterdam ten years ago. The immediate reason was the Euro 2000 football tournament that year. It was important for the tournament to run smoothly, and this meant being able to obtain a clear picture of the atmosphere and incidents as they arose. Cameras were installed in the city centre to monitor the mass influx of supporters
The same year cameras were installed in Saftlevenkwartier, an area close to the central station. In this project the goal was to reduce and prevent violence and harassment problems on the street.

Since 2000 the number of cameras in public spaces has increased steadily to 300. In addition there are 1600 camera's to be found on public transport such as metros, trams and buses as well as stations. These cameras are owned, controlled and monitored by private transport companies. When incidents occur, they can transmit images real time to the CCTV room.

Every application for camera surveillance is always accompanied by a detailed report, describing the number and type of incidents in the area and the current safety situation. Each decision to install cameras is considered very carefully. There is no point installing cameras willy-nilly. We must be genuinely convinced that it is a necessary tool to increase safety.

Camera surveillance is not a panacea for everything. In Rotterdam, however, it has developed to become the basic tool to ensure safety, such as in property and violent offences.
Violent offences, for example, are often committed on impulse, and often also under the influence of drugs and alcohol. The presence of cameras will probably not deter these offenders. However, camera surveillance does have its uses here. Police and the responsible bodies follows up all incidents and works on being on the spot as quickly as possible. Moreover, the images can be used effectively to provide evidence in court proceedings.

Property offences are usually committed less impulsively. These include pick-pocketing or car burglaries. If cameras have been installed and the police act quickly after a break-in or burglary, the offenders will tend not to target that area again. This can reduce the number of incidents.

Conditions

Ever since camera surveillance was introduced, the same question has been asked, which is also the theme of this European project: how can camera surveillance be used in an ethical and democratic way? The more cameras there are, the more necessary it becomes to manage these aspects properly.

Dutch law allows municipal councils to permit camera surveillance. If the council is in favour of camera surveillance, it can give the mayor the authority to designate areas. The mayor's decisions are made public and are then open to objection by local residents. Once the cameras begin recording images - and this is always the case in Rotterdam - the images are subject to the Police Data Act, which places stringent requirements on the use and exchange of these images.

From the very start, camera surveillance in Rotterdam has been based on a number of principles: All cameras are monitored live 24 hours a day, 7 days a week. Images are always recorded. Local residents can expect that any incidents which occur will be noticed.

Incidents observed must be followed up. Camera surveillance therefore means a considerable intensification of surveillance in a neighbourhood. Not only are there extra eyes permanently watching the area, but each incident requires a response by the police or other monitoring bodies.

Points of attention

Many parties have been working hard in Rotterdam to make the city safer. Our people expect the local government to ensure a clean, decent and safe city. They see the problems in their street, outside their own homes. It is vital for the local council to live up to these expectations, and camera surveillance forms an indispensable tool in this task.

This method in Rotterdam is expensive. It involves the costs of technology and maintenance, as well as the costs of extra personnel to monitor the images and take follow-up action. Rotterdam has studied what the limit is in the number of images that an individual can monitor simultaneously. This limit means that each area where a new camera is installed will also lead to recruitment of extra personnel. This remains a dilemma with each camera surveillance application.

The value of surveillance, however, is also significant. Incidents which would otherwise not have been noticed, or where the burden of proof is complex, are now investigated. In 2009 the camera surveillance department recorded 23,700 incidents. This is 65 per day. We have to continue to weigh up these benefits against the costs.

The attitude of local people to camera surveillance has changed over the past ten years. Ten years ago the first cameras were accepted with a certain degree of mistrust. People were sceptical about the need for them. There was little confidence in the professionalism of the users, and concern about the breach of privacy. Now, ten years later, the attitude has changed dramatically. In fact, local people have become attached to ‘their’ cameras. People increasingly say they want cameras in their neighbourhoods. An annual surveys study has also shown in Rotterdam that there is a high level of confidence in camera surveillance and that local people regard it as an effective tool.

Finally

Cameras have become a familiar feature of public spaces. In Rotterdam they have proven their worth at major events. We started using CCTV because of the EURO 2000 football tournament. It also proved its worth as we saw recently when there were some serious disturbances at a large event. Thanks to camera images we were able to apprehend a large number of the rioters.

Our experiences using CCTV have been positive in the last decade. The legal framework has developed to balance issues on civil rights and safety demands. We have built a strong organisation and management structure. Operational processes are clear. We need to maintain our efforts in guarding this system in the upcoming years, but our mission will shift as new questions are rising. Those questions will be based on the increase in citizens support. We will have to manage those high expectations. Also, we expect huge budget cuts caused by the economic crisis. Controlling the costs of CCTV, and maintaining our current budget will be a challenging task and needs to be thought about very carefully.

Afke Besselink, Niels Wittersholt

SAINT-HERBLAIN

NUMBER OF INHABITANTS :
43,510

NUMBER OF CAMERAS :
18

RESPONSIBLE AUTHORITY :
Saint-Herblain

➤ Saint-Herblain is a French city of 45,000 inhabitants located in the inner suburbs of Nantes' urban area (500,000 inhabitants). It is the second largest city of Nantes' urban agglomeration and the third city in the Loire-Atlantique department.

The CCTV system installation has been introduced by the mayor and senator, as well as elected representatives at the beginning of the 1996-2002 term of office. The first cameras have been installed in 1999. The city now has a system of 18 cameras. The city established its Urban Supervisory Control Centre (CSU according to its French acronym) in 2000, mandated by a decree issued by the prefect. This centre was initially supposed to be the CCTV management centre. Now it is used to manage simultaneously urban CCTV and the telesurveillance system and tends to become more and more a global urban management tool.

In 1997, a security audit has been carried out by an outside agency. At the same time, the city Council Security Commission for Crime Prevention (CCPD according to the French acronym) was in charge of leading a discussion about security issues in the city of Saint-Herblain. This Commission handed its report in to the mayor who decided to create several work groups about themes including those security issues. In 1999, the work groups' reports were presented to the city Council. At the same time of this work within the CCPD, a questionnaire about security was carried out with a sample group of Saint-Herblain inhabitants, which revealed that security was their first concern.

Thanks to all those diagnosis elements, the mayor introduced a debate within the city Council about the implementation of the CCPD suggestions, among them was CCTV. In June 1999, the city Council voted the CCTV system installation in Saint-Herblain and the creation of an ethic committee to accompany the project implementation.

The city of Saint-Herblain set three main objectives for its CCTV system:

➤ Secure the places where the flows of goods and persons are most important, in order to reduce public highway offences;

➤ Complement with technological means the crime prevention system existing (local police, prevention actions in schools);

➤ Reassure the inhabitants and enable the State police services to have at their disposal elements to clarify criminal acts. It was a double objective: in one hand assist the national police in the increase of clarified cases which was then very low, and on the other hand secure trading, industrial or large gathering public spaces.

The CCTV system was introduced to increase security for all the Saint-Herblain inhabitants. CCTV is understood as an additional tool integrated to the security and crime prevention local police. In this sense, the city's Urban Supervisory Control Centre manages the CCTV and telesurveillance system, which ensures a greater reactivity of the local departments (local police, technical department etc…) and the national police and the *gendarmerie*. In this sense the Urban Supervisory Control Centre is truly an urban management tool.

In terms of prevention and security, the local police has over twenty years of experience in Saint-Herblain. It always had the constant concern of preventing first-crime or high-risk behaviours, considering that this is a fundamental step before any repressive posture. The will for prevention can be found through various tools such as: prevention actions in schools, situational prevention, local police interventions, and local regulation deeds concerning public space management.

All the prevention actions are politically organised by the deputy mayor in charge of prevention and public and administrative security, within the Prevention and Public peace management, composed of 40 agents.

In this context, urban CCTV is one of the elements in the global prevention and security policy. CCTV has been created in the strict respect of the regulation texts which govern individual liberties, especially related to the use and storage of images. The city's will was to do it in all transparency towards the population. For this purpose, several presentations and visits have been organized to allow the citizens to appreciate the guarantees offered regarding privacy.

The system established is composed of 18 cameras. The CSU is composed of 14 agents and one person in charge of the CCTV system operation. Digital parameters enable to respect the prohibition of visualising private areas or making out an individual's face features. According to current regulation, sign posts are located in the city's various access roads to inform citizens of the presence of cameras.

The city's CCTV images are transferred in real time to the National Police Information and Command Centre.

The images can be consulted only when requested by the national police, in the case of a citizen's complain, or specific requests by state security.

CCTV system has had a positive impact on security and on crime reduction in the watched spaces. However, no displacement of crime has been observed.

An annual report is established on CSU activities (CCTV and telesurveillance). The operators have been trained by an external body on ethical aspects, on the environment, on the partnership and on responsibilities in terms of security.

Dominique Talledec

SUSSEX

NUMBER OF INHABITANTS :
1,392,737

NUMBER OF CAMERAS :
396

RESPONSIBLE AUTHORITY :
Local autorities and national police force

The birth of CCTV in Sussex

The use of public space CCTV in the County of Sussex dates back to 1993 when the first batch of 15 cameras were installed on the streets of Brighton, following a decision by Sussex Police and local authority partners to employ cameras for crime prevention, reduction and detection purposes. This initial installation was followed by further schemes in Brighton and other cities, towns and villages – financed by a combination of local authority funding and central government grants. From the outset, CCTV in Sussex developed through a close working relationship between police and local authorities, with monitoring rooms being established in police stations at Brighton, Haywards Heath, Bognor and Eastbourne, as well as five local authority monitoring facilities. At the same time, the principle of shared costs was adopted.

Central government initiatives to support CCTV growth continued in the shape of the 1994 CCTV Challenge competition, and the Crime Reduction Programme of 1999 to 2003. This process was given further –legislative - impetus through the Crime and Disorder Act 1998, which obliged public authorities to work together to tackle issues of criminality and anti social behaviour. As a result, by 2006, approximately 30 cities towns and villages across the County of Sussex had CCTV cameras, with 17 local authorities and 1 housing association involved.

Thus, the Sussex CCTV Partnership was created. This relationship is now defined by separate legal contracts between Sussex Police and each local authority, setting out operating protocols, roles and responsibilities, and financial arrangements.

CCTV in Sussex today

Currently there are some 400 cameras across the county. These are a mixture of analogue pan-tilt-zoom and dome cameras, linked to the various monitoring rooms through a network of fibre transmission lines. The control, monitoring and recording platform is a newly installed digital system called “i-Witness” – designed by Teleste, and installed by BT Redcare. This platform gives standard 2 frame-per-second “background” recordings, as well as 25 frame-per-second “real time” recording on selected pieces of footage.

In addition, “client” terminals have been placed in all major police stations and custody facilities, enabling local officers to have instant access to video footage for investigative purposes.

This fully networked system allows control of all “live” camera images from any one of the monitoring rooms across the county, as well as immediate access to historical footage at any one of the local “clients”.

Benefits

Having a fully networked system gives us a number of business benefits.

1.Business continuity – the system is inherently resilient. Cameras can be operated from any one of the many “entry points” on the system, thus ensuring a continuity of service to the public.

2.Officer time savings – investigating officers at local stations have quick and easy access to the video footage they need for their investigations. This has eliminated time consuming journeys across the county to retrieve – by appointment – the necessary images. The net result is that officers are spending more time in their neighbourhoods, policing their communities.

3.Environmental benefits – reduction in the number of car journeys required, thereby reducing carbon emissions, and saving in fuel costs.

4.Quicker justice – arrested suspects are now being confronted with video evidence at an early stage in the investigation, leading to fewer police bails, earlier guilty pleas, and ultimately a better service to victims of crime.

5.Security of images – password protected access and fully audited through a system activity log ensures better control of sensitive data.

Individual rights, privacy and the use of CCTV in Sussex

The proper use of CCTV in the UK is governed by 3 principle pieces of legislation, plus guidelines issued by the Information Commissioners Office. The Data Protection Act 1998, lays down 8 data protection principles, covering the fair processing of data, proper control of such data, the accuracy of all data retained, and proportionality in retention times of such data. The Human Rights Act 1998 adopts into UK law, the fundamental principles laid out in the European Convention on Human Rights – the right to privacy in article 8 being particularly relevant in regard to CCTV. The Regulation of Investigatory Powers Act 2000 sets out rules for the covert use of cameras, with stringent authority levels laid down.

In Sussex, all operators are trained to Security Industry Authority standard. This training covers the relevant law, and operator responsibilities when using the cameras, as well as respect for equality and diversity. In addition, a CCTV Code of Practice laying out best practice in terms of both operational and ethical use of CCTV, has been adopted. This Code of Practice has been shared between partners, and in conjunction with protocols between the police and local authorities, consistency and compatibility is ensured.

At the same time, all use of locally placed "client" terminals is quality-assured through a programme of training to ensure proper use and handling of sensitive video footage. Individual password with appropriate system access further guarantees proper usage.

Public confidence and accountability of police use of CCTV in Sussex

Accountability to the residents of Sussex is achieved through the twin processes of properly audited management meetings with all CCTV partners, and a ground breaking process of independent monitoring.

Partnership Management

The Sussex CCTV Partnership involves a shared approach to the management and operation of public space cameras. Local authority owned cameras are operated by a combination of police staff at police stations and local authority staff at local authority monitoring rooms, and the costs for maintaining the system are shared.

Regular quarterly meetings between Sussex Police CCTV management and local authority partners address such issues as performance of the system, technical developments, financial matters and any perceived challenges that lay ahead. Through this means, police use of council owned cameras is held to account.

We are currently developing an agreed process to initiate new camera installations, to ensure consistency of approach across the County of Sussex.

Independent Monitoring

In Sussex it has been recognised that it is essential to retain public confidence in the use of CCTV. An independent process of monitoring and verifying police use of the cameras has now been adopted. Sussex Police Authority has recruited 12 members of the public to carry out "spot checks" on police monitoring facilities to ensure compliance with legislation and the Codes of Practice. These checks can take place at any time of the day or night, without prior warning. Any issues raised, or concerns highlighted, are forwarded to the Police Authority and the CCTV Management. Publicly accessible police authority scrutiny meetings and annual reports ensure transparency.

It is now proposed to extend this scheme to our local authority partner rooms

Interestingly, the work with European partners through the Efus project has confirmed the validity and appropriateness of this scheme, and we in Sussex consider any such process to be an essential element in any future Charter of CCTV usage.

The National CCTV Strategy and Sussex

The National CCTV Strategy was first published in October 2007 and presents the results of a wide ranging review of CCTV in England and Wales. Initially undertaken by a joint ACPO / Home Office project team, the Strategy is now supported by a multi agency programme board with representation from a number of stakeholders.

The Strategy supports and develops recommendations that will deliver:

1. effective, well managed CCTV, taking into account the role of the CCTV industry and the views of the public
2. best practice for partnerships between local authorities, CCTV operators, police officers and the emergency services - offering better protection to the public both as a deterrent and in the investigation of crime
3. better standards in CCTV operation and in the presentation of imagery

Through the above outlined features the Sussex

CCTV Partnership seeks to adopt and implement each of these key elements, to ensure compatibility with nationally adopted best practice.

Christopher Ambler, Roger Fox

VENETO REGION

NUMBER OF INHABITANTS :
4,912,438

NUMBER OF CAMERAS :
1,973

RESPONSIBLE AUTHORITY :
Local authorities

Video surveillance in the Veneto Region

The region of Veneto in north-east Italy has an area of 18,400 km^2 and a population of almost five million, of which 7 % are of immigrant origin. The region is one of the country's principal economic and industrial areas and is in the top 30 of European regions economically. It is also the Italian region that welcomes the greatest number of tourists, attracting more than 60 million visitors a year. The region is divided in seven provinces and 581 communes; four fifths of these communes have a population smaller than 5,000 inhabitants.

According to general regional crime data, the past few years have seen a reduction in crime which is, however, accompanied by a growing feeling of insecurity, which has encouraged many local authorities to pursue the development of urban security policies. In 2002, the regional administration adopted a legal code (Law 9/2002) which supports and promotes an action plan for urban security. The Region wishes to create a 'system' intended to manage the complex problems that appear at a regional level in a coordinated manner, within a collaboration between the different levels of government (State, Region, Province, Commune) and the police forces (both national and local).

The communes and provinces have thus been invited to develop integrated urban-security projects, which habe subsequently been examined and financed by the Region. During the last five years (2005-2009), 278 projects have been approved, financed and put into action: many of them are video surveillance installation, either alone or alongside other initiatives. According to offcial data, 131 of these projects involved the installation of video surveillance systems (almost one in two projects).

In 2007, the Regional Security Monitoring Centre (the creation of which was intiated by the Regional Law No. 9, 2002, cited above) carried out its first enquiry into the number of CCTV systems in place and their effectiveness. Amongst the total of 581 communes, 215 have responded to the enquiry and results have shown that funding by the Region was one of the main reasons encouraging the installation of these systems; the demand for video surveillance was seen to increase.

In terms of the equipment chosen, more than 70%

of cases were digital video surveillance systems consisting of more than three cameras. The places most frequently chosen for installation of cameras were primarily public car parks, crossroads, public parks and schools. In approximately 60% of cases these systems have contributed to a reduction in petty crime and public disorder, according to the local police commanders who responded to the questionnaire. However, it should be noted that in 21% of cases it has been observed that these illicit activities have been moved to other areas that are not covered by video surveillance.

Another, specific project concerned the installation of cameras in the public transport of the Veneto Region's principal towns and cities. Public transport systems appear to be exposed to several risk factors, such as vandalism, violence and petty crime while also being potential targets for terrorist attacks (as demonstrated by the tragic events in London and Madrid). It is for this reason that video surveillance systems were installed in urban transport networks and bus-stops throughout the Veneto region, including obviously the city of Venice with its of *vaporetti* (the "boat-buses").

The Region has thus played an important role in the motivation and coordination of video surveillance installations by the various local authorities and provinces. This has contributed significantly to growth in the use and diffusion of video surveillance in areas of high, urban concentration. Overall, the results appear to be positive, as shown by the exponential increase in the putting in place of these technologies.

Following the activities and experiences provided by the Efus project, it is now important to consider the role of regional authorities in the management of urban security policies, particularly regarding video surveillance.

The role performed by the Veneto Region, as described above, seems to be the most natural and widespread, as other regions have followed the same pattern, at least in the first phase. This involves granting subsidies in order to encourage investment by local authorities and the suggestion of analytical tools to identify, within a local project, the most appropriate methods to put in place to tackle issues of urban security, given that the problems can be treated and resolved more easily if they are examined at the administrative level that is closest to the population.

However, it is also possible to envisage a second phase, which must still be developed, in the course of which it can be anticipated that the Region would have a role of closer coordination of communes, in order to ensure a greater uniformity and better technical integration as otherwise these installations risk isolation, each one operating in its own limited territory. Equally, supplementary instruments can also be encouraged, aimed at facilitating participation and control, which have not yet received great interest from local authorities, as they tend for the time being to focus on the strict, bureaucratic application of the standards set out by the organisation charged with the protection of privacy.

In other terms, the coordination of the technologies employed by the local authorities should be ensured to allow greater efficiency and to guarantee immediate and preventive action (through the use of other available databases and a better organisation of the service). In the mean time, these systems are often simply technical aids to police enquiries.

However, these technological tools must be supported by effective organisation of police services. To this end, the Veneto Region is currently reorganising the territorial partition of the local police forces (*distrettualizzazione*), pooling together several communes into units of at least 20,000 inhabitants, corresponding as far as possible to the organisational structure of the national police. This new division of territory allows the smallest communes to benefit from a full police service, in coordination with the national police and in turn guarantees faster interventions and actions of a preventive nature. It is only through prevention that the impact of video surveillance can be optimised.

At the same time, it is necessary to increase citizen involvement in communities and citizen awareness of the utility of video surveillance cameras (which, though somewhat invasive, are in general well accepted in the Region) and the benefits of civic surveillance. The importance of cooperation should also be highlighted as part of the fight against the phenomena of degradation and urban disorder by contributing to the maintenance and reinforcement of the social networks, which represent the structure of all life in civilised society and are therefore also an indispensable reference for the police.

The role that the Region can play in this domain can include the formulation of legal guidance (declaration of laws and appropriate regulations) as well as a financial role (directing the flow of funding towards a better technological integration according to shared standards). The Region is also committed to supporting local administrations, by providing direction and directives, helping them to establish urban security systems, including the installation of CCTV systems, within a coordinated approach that involves citizens. In this sense, the Region's activities could aid the evolution of the concept of security, in which video-protection constitutes but one part of the measures taken.

Giorgio Vigo

Conclusion

Towards a use of video surveillance respectful of individual freedoms

In 2008, more than 50% of the world population was living in cities, and the trend is towards greater mobility between urban areas. Consequently, there is an intensification of urban phenomena, and that is also manifested in terms of security. In this context, video surveillance is certainly a technological instrument but it also illustrates a form of social collaboration between the different institutions and administrations.

It poses several challenges that this project wished to examine in greater depth:

1.The relations between video surveillance, a technological tool, and the human factor controlling it. It is not the technology in itself that presents risks, but the use made of it; the risk that its potentialities be diverted must be monitored, beginning with the installation of the systems, both by technical measures and by a political engagement.

2.A video surveillance system can also be thought of as an intelligent terminal, not only for the retrieval of images, but also in terms of reorganisation of the city's different resources. It can facilitate the work of city agents, but that calls for responses that are less generic and better adapted to needs. So the question of security can benefit from greater visibility based on better information for citizens.

3.The small number of studies carried out to the present day with regard to the effectiveness of video surveillance has shown that the results obtained by this technology must be put in correlation with the particular context in which the cameras are supposed to intervene. That means taking into account the nature and size of the territory, the population as well as the need that must be identified through security audits. Experts and professionals have unanimously recognised that video surveillance is not the panacea that might solve all of a city's security issues but must be considered an instrument amongst others in the framework of an overall security policy. A balance must therefore be struck between the use of tools other than those the decision-makers have put at their disposal. It is also important not to limit oneself to the use of a single instrument, for the real effectiveness of a security policy depends on the complementarity of the tools implemented and the capacity to contribute coordinated responses adapted to every situation.

4.The quest for effectiveness is also translated by the possibility of integrating different video surveillance systems on public land. In certain cities, there are in fact several systems that are operated by different players. This possibility of integrating systems, which presupposes better sharing of information, does not apply only at the local level but also the regional and metropolitan levels. It could take the form of 'transversal' pacts between governments, regions and municipalities or, when legislation permits, public-private partnerships, in particular when it comes to the surveillance of semi-public spaces. Even then, it is necessary to define strict, precise protocols for sharing information in view of respect for the protection of personal data and private life. At the same time, crossing video surveillance with other information systems and databases, which is in the process of becoming technically possible, is double-edged. Even though this increases the systems' surveillance capability, the principle of necessity imposes a rigorous justification for the need to accumulate and connect so much information on individuals.

Finally, the transversal question examined through all these subjects has been to see how far one can go to ensure citizens' security without, for all that, interfering with their private life. Does the right to intimacy on public land exist? Up to what point? To what degree can the right to security affect other fundamental rights such as the freedoms of speech, association and demonstration?

These issues have been addressed through the prism of the inhabitants of the cities, during these 18 months of European cooperation. The partners placed the citizen at the centre of their concerns. The citizens indeed need to feel safe at home but this does not mean that they want to renounce to their right to the protection of their image. As guarantors of citizens' well-being, the political deciders must therefore consider this question a constant concern and weigh these different aspects. The balance in the way in which the demands for security and for the right to anonymity varies from one country to another, from one city to the next. In examining public policies as regards public perceptions, this project set itself the goal of reinforcing the citizens' place and information within the framework of the use of video surveillance systems, with a concern for transparency that is indispensable to a democratic setting-up of public policies.

Does the urban population seek video surveillance or not? Is this the response adapted to the fears expressed? Does it correspond to the budget available? What training and what means of control and recourse are conceivable?

How do citizens voice their request for or refusal of video surveillance? In what way are they informed and associated in the various steps of implementing a video surveillance policy? How do these measures influence the perceptions of citizens and the behaviour of victims and potential perpetrators?

These are all questions that the project partners asked themselves and to which they tried to provide responses, as much in the form of illustration of their practices as in the form of recommendations. The result of these interrogations and of this search for solutions is translated by the *Charter for the Democratic Use of Video Surveillance*, a document that attests to the cities' political will. These cities pledge to make use of video surveillance in respect of the fundamental rights of citizens and in full transparency vis-à-vis the decision-making process.

It is to go in this direction that the first signatories of the Charter, the Mayor of Rotterdam (Netherlands), the president of the European Forum and Mayor of Matosinhos (Portugal) as well as the president of the French Forum and mayor of Saint-Herblain (France) invite Mayors from other cities to join them and take part in this initiative.

Notes