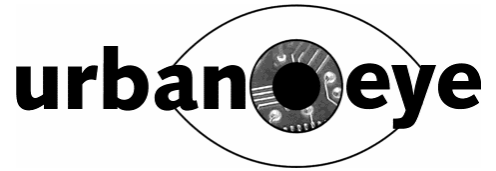


**On the Threshold to Urban Panopticon?  
Analysing the Employment of CCTV in European  
Cities and Assessing its Social and Political Impacts**



RTD-Project (September 2001 – February 2004)  
5<sup>th</sup> Framework Programme of the European Commission  
Contract No.: HPSE-CT2001-00094

**info@urbaneye.net**  
**www.urbaneye.net**

---

**Working Paper No.15**

**CCTV in Europe**  
**Final report**

**Leon Hempel & Eric Töpfer**

**Centre for Technology and Society**  
**Technical University Berlin**  
**Sekr. P 2-2, Hardenbergstraße 36a**  
**10623 Berlin, Germany**

**August 2004**

Project Co-ordination:

Centre for Technology and Society  
Technical University Berlin  
[www.ztg.tu-berlin.de](http://www.ztg.tu-berlin.de)



## **Abstract**

The proliferation of Closed Circuit Television (CCTV) in publicly accessible space across Europe has been the topic of the comparative research project "URBANEYE. On the Threshold to Urban Panopticon?". A multidisciplinary research team studied the rise, employment, and the social and political implications of CCTV in order to outline strategies for regulation. The work started in September 2001 and ended in June 2004 and was undertaken in seven European countries: Austria, Denmark, Germany, Great Britain, Hungary, Norway, and Spain.

CCTV is often deployed as an instrument of crime control. Semi-professional evaluations, referring to analyses of crime statistics, report an allegedly effectiveness. However, several criminologists have argued one should never assume that CCTV will have an effect on crime regardless of the mechanisms under which it is expected to work and the environmental context in which it is embedded. The URBANEYE results show: One cannot make any generalisations about the extent, nature and impact of CCTV surveillance from the mere existence of a system. CCTV systems are deployed for various purposes, have diverse levels of technological sophistication, operating procedures and staffing policies. Operation and impacts have to be understood as the outcome of the interplay between technological, organisational and cultural factors.

Moreover, the study shows two major trends that are of importance for the further development and thus for the regulation of CCTV. In terms of expansion there is a twofold trend. Firstly, CCTV has become an essential part of daily life. We found one third of all publicly accessible premises in selected high streets to operate a system which was very often not notified. However, most existing systems are small and isolated systems with poor technological standard aimed at symbolic deterrence rather than active surveillance. Secondly, there is a clear trend towards an integration and digitalisation of larger systems. Thus the often opaque character of visual surveillance is enhanced as surveillance webs and invisible algorithms tend to become the core of advanced CCTV networks. Nonetheless, our results show that CCTV is supported in general by a majority of people though often found to be rather uninformed about the actual functions and practices of CCTV.

Given this combination of increasing opaqueness and uninformed citizens, a political response should be found in the immediate future. To ensure democratic control of CCTV the black box should be opened. The extent of surveillance should be made transparent by registration, the proportionality of deployment and its fitness for purpose should be assessed by a licensing system, managers and operators should be made accountable and regular inspection should guarantee compliance with a common and consistent set of codes of practices.

## Table of contents

1	EXECUTIVE SUMMARY .....	3
2	BACKGROUND AND OBJECTIVES OF THE PROJECT .....	10
3	SCIENTIFIC DESCRIPTION OF THE PROJECT RESULTS AND METHODOLOGY ...	13
	3.1 UNDERSTANDING CCTV. THE STATE OF ART .....	13
	3.2 LEGAL FRAMEWORK AND PUBLIC DEBATE.....	21
	3.3 LOCATIONS AND ACTORS OF CCTV.....	25
	3.4 CCTV SYSTEMS AND PRACTICES.....	33
	3.5 THE SOCIAL EFFECTS OF CCTV .....	40
	3.6 THE POLICY IMPLICATIONS OF CCTV .....	48
4	CONCLUSIONS AND POLICY IMPLICATIONS.....	58
	4.1 CCTV: A EUROPEAN ISSUE? .....	58
	4.2 COMPARISON: COMMON TRENDS AND NATIONAL DIFFERENCES.....	60
	4.3 PURPOSES, ORGANISATION AND PRACTICES OF CCTV SURVEILLANCE .....	64
	4.4 POLICY IMPLICATIONS AND RECOMMENDATIONS .....	66
5	REFERENCES .....	69

## 1 Executive summary

### ***CCTV has become an essential part of daily life across Europe.***

For more than 40 years we witness the proliferation of video surveillance systems in public and private, but publicly accessible spaces throughout Europe. Driven by socio-economic transformation and technological progress the process of diffusion accelerated since the late 1970s. However, the rise of CCTV became a policy issue only since the 1990s as police forces or local authorities in a growing number of European nations utilised cameras for the permanent and intense surveillance of public urban areas in an attempt to control crime. Since that time a massive spread of surveillance cameras in all areas of the urban space – in particular due to decreasing costs – is recognizable: Today simple b/w-systems at prices of 20-25 € are available in chain store markets. Given this development the URBANEYE project started to study this increasing rise of CCTV throughout Europe. The survey of more than 1,400 publicly accessible spaces (such as shops, stations, cinemas, banks, etc.) in the capitals of six countries found in summer 2002 nearly one third (29%) of all premises and institutions to operate a CCTV surveillance system.

### ***The URBANEYE project***

The project is a comparative research project analysing the employment of CCTV in public accessible space in Europe. The aim was to clarify the current state of affairs in Europe (regulation, debate, extent, legality, sophistication, acceptance), to assess how CCTV works in different national, institutional, social and spatial contexts, to consider the political impacts of the rise of CCTV and to find out whether CCTV is to be regulated, and if yes how? The study was undertaken in seven European countries, Austria, Hungary, Germany, Great Britain, Norway and in parts in Denmark and Spain. It started in September 2001, ended in June 2004 and was realised by a multidisciplinary team assembling criminologists, philosophers, political scientists, sociologists and urban geographers.

### ***The data collection***

The URBANEYE project studied the rise, use and perception of CCTV from a whole range of viewpoints involved. Therefore a set of methods was used in order to achieve the objectives. For the analysis of four newspaper and their coverage on CCTV (Nov 2000 - Nov 2001) the research collated and analysed 1392 articles with „CCTV stories“. For the survey on the extent, technical sophistication and legality of CCTV in major urban infrastructures more than 1,400 publicly accessible premises and institutions in high streets and their vicinity in six European capitals (plus a partial analysis in Madrid) were studied. For the more detailed analysis of the practice of surveillance 40 CCTV systems

were chosen in a variety of institutional settings (open street CCTV, public transport systems, railway stations, shopping malls, etc.). 93 expert interviews were carried out with managers and operators of these CCTV systems. In 17 control rooms also short-term observation was undertaken and in another 12 control rooms 524 hours of long-term observation. Moreover, with around 1000 citizens on their attitudes, knowledge and experience of CCTV were interviewed and with 50 often these in-depth interviews were carried out. Finally a workshop with 27 experts was organised to discuss the policy implications of CCTV.

### ***Rather theses than final conclusions***

In statistical terms the findings are not representative for Europe or the respective countries. The research has rather been tentative and taken the speed of the further expansion of CCTV into account and also the technological development the results of the URBANEYE project rather formulates theses than conclusions. For the validation of the URBANEYE findings further research will be needed.

### ***National public discourses on CCTV differ notably...***

Print media and policy discourses on CCTV are shaped by national historical and political traditions and experiences with crime and thus differ significantly across Europe. CCTV – except speed cameras – is widely accepted in Britain and regular media coverage is dominated by “caught on camera”-stories which indicate how much it has become part of everyday life. In Hungary open street CCTV is seen as a “technological fix” for serious social problems, and it is thus rapidly expanding at least in the capital Budapest. In contrast its deployment in public areas is intensely contested in Germany while CCTV is more or less a non-issue in Austria except when a matter of tunnel safety or in tabloid papers (although the discourse is reported to change). Also in Norway there is little public discourse on CCTV while in Denmark critical discourse initiatives were taken by several organisations.

### ***... and legal regulations vary.***

The variations in legal regulation differ according to both institutional and national contexts in which CCTV is in operation. Such regulations may differ in connection with the public or private nature of the agency responsible for the operation. In particular CCTV surveillance for purposes of national security, public safety and criminal investigation falls under specific rules. Case studies have been carried out regarding CCTV based either on constitutional provisions or specific legislation or on orders and other decisions issued by the competent authorities. In a few countries such as France there are also specific provisions under which the installation and deployment of CCTV are to be authorised in advance by an administrative authority. In other countries CCTV is not currently the subject of specific laws. However, data protection authorities have

been working to ensure appropriate application of the general provisions for data protection by the way of opinions, guidelines or codes of conduct which have been adopted for instance in Britain or Hungary.

***International legal instruments provide a vague European framework.***

Besides Article 8 (right to privacy) of the Convention of Human Rights and Fundamental Freedoms and the Convention on the Automated Processing of Personal Data of the Council of Europe in particular the Data Protection Directive (95/46/EC) of the European Union is of relevance for CCTV in the 15 Member States and the Accession and Associated Countries. The Directive does not apply to CCTV surveillance for purposes of national security, public safety and criminal investigation. Moreover, its scope in regard to different technological form of CCTV is contested but the consequence of its implementation into national law was at least in some countries the explicit regulation of CCTV.

***In national comparison the diffusion of CCTV is rather similar in (semi)public space...***

Though our findings suggest that the diffusion of CCTV (and to some degree its technological sophistication) is most advanced in Britain (40%) and least developed in Austria (18%), the mere existence of a CCTV surveillance system in (semi)private but publicly accessible space is determined by the institutional rather than the national context. While religious centres, cemeteries and educational institutions are most unlikely to be found under surveillance across Europe, typical locations of CCTV are places of transit such as underground systems, train stations or airports. Moreover, the existence of a CCTV system is common at national government buildings, embassies, money institutions, museums, hospitals and petrol stations. Thus European citizens cannot avoid CCTV surveillance during essential daily routines such as being on the move by public transport or when getting cash money in banks.

***... but significantly differs in public areas.***

In contrast to the similarities in the extent of CCTV in (semi)private spaces it are the open streets where the deployment of surveillance cameras differs significantly across Europe. While it was estimated that around 40,000 cameras monitor public areas in more than 500 cities in Britain, less than 100 cameras monitor public areas in around 15 German cities, and no open street CCTV system is in operation in Denmark. Moreover, while extensive surveillance and large networks with more than 40 cameras are reported for cities in Britain, France, Hungary, Italy or Monaco it is the surveillance of limited but strategic locations (in particular the vicinity of main railway stations) that it is the model in Austria, Germany, Norway or Spain. Despite these differences the deployment of open

street CCTV against street crime has been adopted in the respective countries by most major parties as strategy of crime control.

***Impacts of CCTV are not technologically determined but contingent upon human mediation.***

One cannot make any generalisations about the extent, nature and impact of CCTV surveillance from the mere existence of a system. CCTV systems are deployed for various purposes, have diverse levels of technological sophistication, operating procedures and staffing policies. The operation and impacts have to be understood as the outcome of the interplay between technological, organisational and cultural factors

***CCTV is a multifunctional risk management technology but mainly deployed for social control.***

CCTV cameras are deployed for a variety of risk management purposes such as tunnel safety, the prevention and detection of traffic congestion, fire or accidents, and deviant behaviour such as unauthorised access, so-called "anti-social behaviour" and crime. Although the improvement of services (16%) and the fire safety (5%) were also among the publicly declared purposes of CCTV systems that were found in our 2002 survey, most CCTV systems (86%) were declared to be tools to prevent and detect theft. Many (39%) were also declared to serve the prevention and detection of violence against persons. However, the potential of expandable mutability characterises the use of CCTV because – once in place – other forms of use might occur.

***The average CCTV system is a small and simple island of surveillance in the retail sector.***

In statistical terms the average CCTV system in the publicly accessible spaces studied in our 2002 survey is owned and operated by the premise or institution itself. It is technologically rather simple with three fixed cameras, one monitor, sequential switching between the cameras and no linkage to third parties. Footage is recorded and stored on an analogue basis. Monitoring of images occurs only on an irregular basis by one observer who often has to fulfil other parallel tasks though staff is supposed to intervene if any relevant event is caught on camera. More than two third of such smaller CCTV systems with less than five cameras are in operation in the retail sector.

***Most large systems monitor semi-private or public space and are likely to be connected to other agencies.***

Only two out of hundred CCTV systems are larger systems with 20 or more cameras. These systems are found in semi-private space or public space such as large retailers, shopping malls, public transport, hospitals, museums, buildings of the local or national government or in the open streets. Larger systems a likely to be connected to other

actors or agencies such as the police, the fire department or private security services by dedicated communication links or the ability to switch images. Thus there is an increasing tendency for systems to become embedded in a complex social and technological web of surveillance which extends and diffuses the impacts of the surveillance gaze.

***The practice of CCTV is dominated by symbolic deterrence rather than active surveillance.***

In an attempt to approach the diversity of CCTV we developed a typology that locates individual systems between vision (the capacity to make those under surveillance visible to an observer in real-time) and visibility (the capacity to induce the feeling of being under the gaze of a camera). Matching our survey data with this approach suggests that the majority of CCTV systems aim to prevent deviant behaviour by symbolic but more or less incompetent deterrence because cameras are highly visible but those under surveillance are hardly visible for an observer due to irregular monitoring, informational overkill or even the deployment of dummy cameras. However, more than three fourth (78%) of the CCTV systems record footage on a permanent basis.

***Many CCTV systems in operation violate national data protection provisions.***

CCTV surveillance in one out of two systems (51%) found in our survey was not notified by signage. While in Norway only 20% of the systems were lacking signage, in Hungary and Austria more than 80% were doing so. And even if CCTV surveillance was notified the identity of the responsible data controller and contact information was often missing. Moreover, in 43% of the cases our request to answer the simple question on who is the owner of the system was rejected. The secrecy of CCTV was worst in Austria, Germany and Hungary where in between 55% and 87% of the cases an interview was rejected, while the rate in the two Scandinavian countries and Britain was only around one fourth. However, most managers of larger systems – in particular those of (semi)public bodies such as public transport, museums or open street CCTV systems – were cooperating.

***Discriminatory targeting patterns might amplify social exclusion.***

Ours and others research in CCTV control rooms suggest that the sensory limitations of the video screens and the distance between the observers and the observed encourage the application of categorical suspicion based on a narrow range of readily observable traits rather than the application of behavioural suspicion. Thus operators might tend to target whole categories of the public seen as likely criminals or nuisances. However, if this occurs and which consequences it entails varies according to structural factors such as the fit between mandated activities and available time, the relationship of CCTV operators and those in the field, and the function of monitored space. In particular the



growth of CCTV in semi-private spaces might bring with it an increasing emphasis on exclusion as dominant strategy of social control.

***Official policies, accountable management and operator training are important.***

Targeting, interpreting and reacting to a scene from a distance according to a stated purpose is a difficult task. Among the CCTV systems studied in detail we have found examples for both expansion and contradiction of functions due to occupational cultures which produced a divided and disillusioned work force, conflicting interests between the observers and the operators in the field and even the (non)ambitions of individual operators. Thus besides official policies of a CCTV system an accountable management and an adequate operator training are important to fulfil the relevant purpose.

***There is little knowledge, but rising consciousness about CCTV in the public***

Although people do not know much about CCTV, its growing presence in urban space has become part of their consciousness – they are feeling the gaze rather than seeing the eye. Moreover, many people tend to overestimate the technological potential of surveillance.

***A majority supports CCTV and a strong minority indicates concerns***

Recent research and our survey suggest that a majority of respondents throughout Europe is supportive of CCTV in general. However, the acceptance of CCTV differs significantly between different countries with Britons being most supportive and Germans and Austrians being comparatively sceptical. Scepticism is often based on the grounds of civil liberties in general or privacy in particular. Though around two third of the respondents to our survey agreed with the statement "who has nothing to hide, has nothing to fear from CCTV", more than 50% think that footage can be easily misused and 40% felt that "CCTV invades privacy".

***Attitudes towards CCTV surveillance differ markedly depending on where it is.***

Moreover, people draw a clear line *where* they accept CCTV. Most people support CCTV in banks or transportation facilities while they oppose it in "intimate spaces" such as changing rooms. In international comparison the most different attitudes are found towards open street CCTV which is seen as a good thing by 90% of the respondents in London and by only 25% in Vienna.

***In particular younger people have opposing attitudes towards CCTV***

In terms of socio-demographic rather than national background, gender turned out to be of minor importance as predictor for peoples' attitudes towards CCTV. Age was found

to be most likely to influence the opinion on CCTV. As a general rule younger people were much more likely to be found opposing CCTV and doubting its benefits than the elderly.

***... and believe that their behaviour is especially targeted by cameras.***

Teenagers found themselves most likely to be disciplined: Almost one third of the respondents aged under 20 thought that CCTV affects their behaviour while only 14% of those aged 60 and older thought so.

***People are sceptical about CCTV's crime prevention effects***

Despite majority support many respondents were sceptical about the crime effects of CCTV: More than 50% believed that CCTV displaces crime and does not protect against serious offences.

***According to the public opinion CCTV should be regulated by public authorities.***

In terms of trust, a majority of respondents prefer the police to operate an open street CCTV system. Moreover, regulation matters for most of them. In particular to limit access to footage by private third parties, and to inspect, register and license CCTV systems is seen as very important by more than two thirds of the respondents.

## 2 Background and objectives of the project

The employment and rapid proliferation of video surveillance systems, also known as closed-circuit television (CCTV), has drawn attention from policy makers and researchers across Europe in recent years. However, policy debates mostly took place within a national arena, and academic discourses were dominated by the experience in Britain with its advanced level of surveillance. Moreover, the overall discussion concentrated on public area CCTV while private surveillance was rarely addressed, with exception of limited topics such as the monitoring of workforce.

Given this background, the overall objectives of the URBANEYE project were, firstly, to provide a comparative and comprehensive analysis of CCTV in Europe, secondly, to assess the implications of the expansion of visual surveillance, and, thirdly, to support decision-makers by devising policy recommendations. The main focus of the project was CCTV surveillance in both public areas and private but publicly accessible spaces such as shopping malls or railway stations. Only marginally addressed was CCTV surveillance in locations not accessible for a broader public, such as residential areas, shop floors or offices.

In detail, URBANEYE should achieve six specific objectives:

1. to study discursive contexts and legal regulation that shape the diffusion and employment of CCTV in seven European countries (Austria, Britain, Denmark, Germany, Hungary, Norway and Spain) by textual analysis of print media, policy papers and legal regulation;
2. to identify locations and core features of CCTV in selected urban areas of seven European capitals (Berlin, Budapest, Copenhagen, London, Madrid, Oslo, Vienna) in order to develop a typology of video surveillance;
3. to examine the organisation and practices of two selected CCTV systems in six capitals (see above, except for Madrid) by interviewing staff and observing control room work;
4. to study the social effects in terms of changes in criminal and every-day behaviour by analysing crime statistics and interviewing observed;
5. to assess the policy implications of CCTV by realising an expert workshop with representatives of law enforcement and security agencies, the CCTV industry, R&D centres, data protection authorities and human rights organisations;
6. to devise policy recommendations based on the findings of research and a review of existing regulations.

Contrary to these original objectives of URBANEYE two major reorientations were made during the life-time of the project:

- Some local teams faced massive problems to get access to CCTV systems for long-term observation of control room work due to an attitude of suspicion by the management which might be explained by post-9/11 fears, worries regarding an inadequate privacy policy or simply concerns about disturbance of work routines. Thus it was impossible to carry out the comparative study of the organisation and practices of CCTV surveillance in twelve systems as planned. Instead, we chose to study those systems to which we could get access and by methods that were acceptable for the management. This eventually meant that 40 CCTV in very different contexts were studied in more or less detail.
- In addition, the URBANEYE team opted to waive the analysis of crime statistics as a method aimed to study CCTV effects. Several reasons justify this proceeding. First, it was initially planned to analyse crime statistics for locations which are monitored by those CCTV systems to be studied in-depth in order to correlate findings of the observational studies with data of the statistical analyses. As the in-depth study of comparable CCTV systems was impossible as noted above, we missed comparable locations for the analysis of crime data. Secondly, our research revealed that the geographical reference of registered crime was insufficient in some countries for a study of the crime effects of CCTV, as offences are only registered for geographical units covering much wider areas than those under surveillance. Thirdly, several criminologists contest the analysis of crime statistics as an instrument for CCTV evaluation as they point out that registered crime do not necessarily reflect actual crime and victimisation. Thus, we eventually chose to increase our sample of quantitative interviews with people about their experience of CCTV rather than carrying out a hash analysis of crime statistics.

A minor reorientation that was necessary, was to waive the production of an assessment tool, which was planned to be published as Deliverable No. 4 according to the Technical Annex. It was primarily meant as a check-list for decision-makers who either consider to install a CCTV network or are required to assess a running system. Contrary to the initial plan it became clear during the life-time of the project that the development of such a tool was too complex for several reasons. First, while we expected CCTV to be an instrument of crime control we actually found it to be a multifunctional tool of risk management. It is applied in manifold contexts and for diverse purposes that range from traffic management or fire safety to access control and crime prevention. Given this, it is clear that the variations in modes of operation are enormous as well as the complexity of legal regulations that frame CCTV surveillance in different nations and contexts of application. Thus, the reduction of this complexity to a rather simple and manageable tool for an assessment of its utility, effectiveness and legality proved to be impossible.

Moreover, being not aware of the reporting guidelines of the European Commission when drafting the Technical Annex, we initially planned a final report as Deliverable No. 8 entitled "Strategies for Regulation". As a chapter comprising our conclusions and the

policy implications of our findings is an essential part of this document, we waived to submit an additional document with more or less the same content.

### **3 Scientific description of the project results and methodology**

The following chapter comprises the different analytic sections of the research progress. It starts with an overview of the main discourses in which CCTV is discussed and analysed. To summarize the state of art was part of the research work. As literature report it is published on the project's website. However, to assess the progress that the URBANEYE project was able to achieve during its lifetime the main strands are reported here and also complemented. The second part of this chapter will summarize the research of the individual work packages, the methodologies used and the results. While the first work-package (work package 2) was concerned with outlining the context of operation of CCTV on the national level, specifically with the description of the rise of CCTV, the regulatory environment and the current public debate in each country, the analysis of CCTV systems started with work-package 3. The focus changed from the national to the city level and was then concentrated to the organisation and practice of the individual systems in each capital. Work package 5 looked on the people's perceptions of CCTV and final work package 6 asked for the political impacts of CCTV.

#### **3.1 Understanding CCTV. The state of art**

A key dimension of understanding CCTV is the rapid social change caused by economic globalisation and the revolution in information technology. Already by the end of the 1980s Gandy mentioned that there is a close relationship between information and communication technologies, ICT, and surveillance technologies. He reports "that the real source of growth in both the information work force and the development of information technologies is not to be found in any transformed consumer demand, but in the continually expanding surveillance requirements of multinational corporate enterprises. Indeed, for some observers, 'information society' is a misnomer that hides the extent to which industrial societies have in fact become surveillance societies" (Gandy 1989: 61). ICT connect people throughout the world, they provide new forms of communication, offer access to unforeseen sources of information and allow all actors, from individuals to cities, an infinite space to reach distant awareness of others. But at the same time ICT provides the basic technique for surveillance tools such as intelligent CCTV systems equipped with software capable to identify identities and behaviours.+

There are several strands in which CCTV is discussed. They give an idea of the complexity of the subject and underline the necessity that the rise of CCTV has to be analysed from different viewpoints. There is no dissent among the serious researchers that for an adequate description and analysis of CCTV there is a strong need to take technological as well as political, social as well as cultural, commercial as well as psychological aspects into consideration. Most empirical research was firstly done on the crime effects of CCTV and secondly on the public attitudes towards the use of CCTV or

what Koskela (1999) calls the "emotional aspects of surveillance". Research focusing on the effects of CCTV on non-criminal behaviour is just emerging, which in fact is no surprise, when remembering the methodological difficulties to isolate and study the crime effects of CCTV.

### ***CCTV and crime***

Most of the time video surveillance is introduced as an instrument to reduce crime. On the one hand, it is argued that CCTV prevents crime, and therefore strengthens the people's feeling of security. On the other hand it is sold as a tool to help to catch offenders and reduce criminality repressively.

**Standard evaluations** are mostly based on these intentions, which is often emphasised to the public. Consequently, they concentrate on changes in crime rates related to the employment of CCTV. Their main methodological tool is to highlight statistics in order to justify the efficiency of CCTV. Often they are influenced by those who ask for the evaluation and usually have a high authorial impact on public debates as well on political decision making processes. The British criminologist Tilley points out that "sadly, many really only want evaluations for self or political or organisational or civic aggrandisement, even when purporting to want an independent piece of work" (1998: 149).

The scientific value of standard evaluations is questionable. Pawson and Tilley even conclude that most of the time standard evaluations have been "post hoc shoestring efforts by the untrained and self interested practitioner" (quoted in: Norris/Armstrong 1999: 94). Not only is the explicit focus on changes in crime rates insufficient but the statistical evaluation procedure itself seems often to be very weak. It is doubtful how professional the crime statistics evaluations are.

Taking crime statistics as a basis for evaluation poses several problems, because recorded crime does not reflect criminal activity accurately: Not all criminal offences are reported to the police, not all reported offences are recorded by the police and not all recorded offences are not brought before courts and convicted as crimes. This discrepancy probably increases due to CCTV because of the enhanced visibility of certain crime types. The Scottish criminologists Short and Ditton (1995: 12) have outlined five problems regarding the evaluation of crime statistics:

- The before and the after periods are often not long enough to enable the researchers to address random fluctuations caused by seasonal effects and long-term trends in crime, both of which could influence the results.
- Different crime types are often aggregated into one overall figure. However, they have to be distinguished according to different crime forms in order to assess the impact of CCTV adequately. An increase in certain crimes can be seen as a failure, in regard to other types it can be seen as proof for the efficiency of the adamant camera eye.

- There are often no appropriate control groups used by standard evaluations to compare crime trends in the target area and the wider area without CCTV employment. Long term crime trends can show that a decrease first assigned to the presence of CCTV lays in the reduction of crime in the whole area.
- There is hardly any discussion on displacement to adjacent areas of criminal behaviour caused by CCTV. A detailed analysis of the crime activities in the adjacent areas is necessary. Coleman and Norris (2000: 158) have identified six types of displacement. Next to the geographical displacement, there also is temporal, tactical, functional displacement as well as target and perpetrator displacement.
- Presentation of percentages leads to erroneous conclusions regarding standard evaluations.

Furthermore, simultaneous applications of additional crime preventing instruments are of importance and have to be considered in the presentation of an evaluation (see also Coleman/Norris 2000: 153-155). Often video surveillance is only a part of a whole package of safety measures. In his critique, Tilley even gathers nine aspects which can lead to inadequate measurement (1998: 150-151).

Finally, standard evaluations referring solely to crime statistics are questionable, because they operate with certain presumptions. They presume first, that the technology does really work and second, that crime prevention is the only intention of the employment of CCTV. Contrary to those critics and promoters of CCTV who take the functioning of the CCTV technology for granted, a rigorous assessment of CCTV requires that the functionality of the technology itself be first put in question.

After the first open street system has been installed in 1985 in South-England Bournemouth, criminologists as Tilley, Ditton and Short started in the 1990s to re-think existing evaluations methods. Meanwhile many other researchers have adopted their critical perspectives to evaluate CCTV (see the different contributions on British evaluations in Norris et al. 1998 and in Painter/Tilley 1999). The overwhelming majority of high quality evaluations have been carried out in Britain so far. In other European countries CCTV evaluations are underway with only preliminary findings published so far (e.g. Flight & van Heerwaarden 2003).

A comparison of two systems in two adjacent Scottish cities showed that CCTV does not have the same effects regardless of where it is installed. While in Airdrie CCTV showed a crime-reducing effect, in Glasgow crime even increased. (Ditton/Short 1998) The effects of a successful employment at the one site cannot be generalised to another. „We conclude“, state Ditton and Short (1999: 217) "open-street CCTV can ‚work‘ in limited ways, but it is not a universal panacea. It works in different ways in different situations and future evaluation might choose wisely to concentrate on ‚how‘ rather than ‚if“.



In their overviews of evaluations Phillips (1999) as well as Colemann and Norris (2000) have underlined that up to now it was not possible to compile consistent results about the employment of CCTV as an instrument of combating crime. Next to the success stories there are examples of mixed as well of negative effectiveness. The findings of the evaluations of the crime impacts of CCTV are disparate and not easy to summarise. Welsh and Farrington conclude on the basis of their meta-analysis of 18 CCTV evaluations from Britain and North America:

“CCTV had a significant desirable effect on crime, although the overall reduction in crime was a very small four per cent.” (Welsh & Farrington 2002: 41)

However, half of the reviewed studies show evidence of a desirable effect of CCTV on crime, while the other nine studies show no evidence of any desirable effect. In detail, mixed results were found for the crime prevention effectiveness of CCTV across three settings, i.e. city centre and public housing setting, CCTV in public transportation systems, and CCTV in car parks. Five evaluations of CCTV in the first setting showed small but significant effects on crime, while CCTV had no effect on crime in four other evaluations. A similar picture emerged for CCTV in public transportation systems. Two evaluations found a desirable effect, one found no effect, and one even found an undesirable effect on crime. For CCTV in car parks they found a “statistically significant reduction in crime of about 41 per cent”, but cautiously add that in all these cases other crime prevention measures were in operation at the same time (2002: 42). In terms of types of crime affected, Armitage summarises in her review of current CCTV evaluations that “CCTV appears to have no effect on violent crimes, a significant effect on vehicle crimes and it is most effective when used in car parks” (2002: 4).

In their fundamental critique of evaluation research, Pawson and Tilley have introduced the importance of context into evaluation matrixes and evaluation research into the direction of more complex social studies. The authors outline their examination with the argument that most evaluations so far have been not 'realistic'. The reason for that lays in the silent "epistemological assumptions about causation and their lack of fit with the nature of social programs" (1997: 30). It has to be highlighted, as Pawson and Tilley pointed out, that most evaluations are based on a rationalistic sight of reality which ignores the diverse contextual conditioning as a whole in which a social program takes part. Instead, such concepts construct a casual relationship between a program and an outcome but in the end the outcomes are assertions without any substance. The causal aspect is constructed. "The bottom line, as they say, is to show that it really was the program which was responsible for changing the subjects' lot" (1997: 31).

Correspondingly, these evaluations often describe outcomes, but they forget to ask why and how programs work in to achieve certain results. The consequence is to be confronted with inconsistent results without knowing - or more than that - without wanting to know the reasons. They are blind to the circumstances within the assumed

(causal) relationship between program and outcome, what is familiar as the black box problem. i.e. to leave unexamined or even to obscure the inner mechanism of a research program as well as the whole evaluating approach including his pre-assumptions. One refers to a causal model that reduces the diverse process in operation to the question whether a program can be seen as a "success" or not.

Major academic books on CCTV (Norris, Moran and Armstrong 1998; Norris and Armstrong 1999, McCahill 2002) have shown the ambivalence of its employment. While mostly advocates and critics believe that visual surveillance technology works, these studies explain that CCTV has to be seen in broader social and political contexts and that every optimistically belief in the effectiveness of the technology is pure fantasy. In his book, *The Surveillance Web*, for example, McCahill (2002) has shown how visual surveillance systems (in shopping malls, workplaces, and high-rise housing schemes) are shaped by the organisational, occupational and individual concerns of those responsible for setting up and monitoring the systems.

### ***CCTV and public opinion***

Armitage also points out that CCTV appears to have a life cycle contingent upon the maintenance of publicity and even reports that in many cases the effects of CCTV upon crime began before surveillance cameras actually became operational. Thus it becomes clear that when studying how CCTV works, public awareness and opinion are as important as the actual organisation and practice of surveillance, which leads us to the second major strand of research.

Besides the bunch of opinion polls on CCTV that have been ordered by local media or self-interested practitioners in many European countries<sup>1</sup>, studies explicitly committed to scientific standards are known from Britain (for an excellent summary see: Phillips 1999), Germany (Reuband 2001, Klocke et.al. 2001, Hölscher 2003) Finland (Koskela & Touminen 2003), the Netherlands (Flight & van Heerwaarden 2003) and Switzerland (Klauser 2004a, 2004b). Though methods and sample structure are unknown, we also include a Gallup Poll survey ordered by the Danish Crime Prevention Council (2000) in our summary of the recent findings, as it is the only survey from Denmark covering more aspects of CCTV from which findings are available in English. Though it is likely that other studies have been done in other countries, the only international comparison that we know above this is the small qualitative study on video surveillance and women's perception of safety in Helsinki and Edinburgh provided by Koskela (1999).

---

<sup>1</sup> The findings of these surveys are mostly limited to a simple pro vs. contra CCTV decision. Further details are not available. Thus it seems likely that the question is either raised by professional market research in telephone interviews between questions for the next Sunday vote decision and the favourite soft drink, or by ad-hoc surveys of journalists who approach – armed with microphones and perhaps TV cameras – the visitors of a pedestrian area for an afternoon. Having said this, we see no need to further discuss these data.

Though most of these studies address similar issues their value for a European comparison is limited because of their very different methodological approaches. Ditton (1999) and others reminds us that the methods chosen have a significant impact on the results of research on public attitudes towards CCTV. Different sampling strategies might bias the representation of certain social groups. Personal interviews in street surveys might represent those who actually use the street, while postal interviews of randomly selected respondents might represent the socio-demographic structure of the local residents. As "older women are less likely to resist CCTV than younger men", as Ditton puts it brutally (1999: 222), a significant higher support is likely to be found in studies which employ the latter sampling strategy. Honess and Charman show a gender difference according to the method: While in street surveys males were more critical towards surveillance, it were women who expressed the most concerns in group discussions (quoted in Koskela 1999: 5). Moreover, Ditton (1999: 226) found a 35% difference in public support of CCTV as influenced by questionnaire design. Contextualising questions either pro or contra CCTV before asking for the acceptability of CCTV had a highly significant impact on the results.

Having said this, we cautiously summarise the findings of previous studies as following: A majority of respondents to surveys throughout Europe is supportive when asked for their attitude towards CCTV either in general or in the open streets. However, when asked for more details, people draw a clear line and oppose CCTV in 'personal spaces' though it might happen that they get used to it after a while. Between one tenth and more than one third of respondents indicated concerns on the grounds of civil liberties. Variations in support and opposition between the surveys might to some degree be explained by different methodologies and sampling strategies. However, peoples' attitudes towards CCTV were shown to be contingent on local culture and personal values. Though CCTV schemes are among others often justified by the claim to make people feel safer, the surveys so far indicate that its effects on the fear of crime are marginal. Rather it seems that believe in the general crime effects of CCTV, trust in its benevolent usage and desire for order makes people likely to support CCTV. That many respondents are hardly informed about the locations under surveillance or the actual functions of particular CCTV systems suggests that surveillance cameras are seen as a symbol of social order rather than a means to increase individual safety. However, even the supportive majority demand clear regulations of CCTV in particular of its use by private operators.

### ***CCTV and the Panopticon***

As David Lyon has pointed out, the sociological response to the general issue of surveillance has been dominated by images of the Panopticon (Lyon 1994). This has been especially true of CCTV surveillance which naturally invites comparisons with Jeremy Bentham's proposal, written in 1787, for an architectural system of social discipline, applicable to prisons, factories, workhouses and asylums. Bentham's

architectural design "has been one of the most powerful metaphors in locating the theoretical and social significance of CCTV in contemporary society." (Norris 2003: 249)

The design of the panopticon illustrates the mechanism of surveillance. It consists of a circular prison building including a central watchtower. It enables a single officer to control a multitude of prisoners. Its impressive clearness makes it an evident model for contemporary trends of surveillance. In form of modern CCTV systems – as for example in shopping malls – the panopticon suppose to celebrate its renaissance: The view of the camera's eye is expected to be felt by the subjects regardless of the operation or even the existence of a CCTV system. It is hardly surprising, then, given the parallels that can be drawn with CCTV, that many theorists have been drawn to both Foucault's concept of the Panopticon and his analysis of its disciplinary potential (see Davis 1990; Fyfe and Banister 1996; Reeve 1998). As Fyfe and Bannister (1994) note, CCTV, like the Panopticon, facilitates the power of the watchers over the watched not only by enabling swift intervention to displays of non-conformity but also through the promotion of habituated anticipatory conformity. By approaching the question if European cities are "on the threshold to urban panopticon" the URBANEYE project appeals to it, too.

However, just taking the diversity of current forms of CCTV systems into account, it is obvious that the panopticon approach, stressing parallels to the industrial age of the 19th century, is highly questionable in regard to current social developments towards a post-industrial society based on mobility and information flows. Lyon considers: "Whatever one may learn from Jeremy Bentham's Panopticon or George Orwell's totalitarian telescreen technology, it is not clear if these are entirely helpful ways of understanding surveillance today." (Lyon 2002: 4). Thus McCahill states that one has to go "beyond Foucault" (McCahill 1999). Given the challenges of globalisation and the new patterns of living in a highly individualised society the panopticon has to be re-examined, combined with other discourses and models. Re-reading Foucault Norris has lately extended the understanding of it. He pointed out that in the end the panopticon is "far more than an architectural form of visualization". It implies at its "heart" already "the collection of individualized codified information". As the deviant is segregated from society, the panopticon is "exclusionary" as well as "inclusionary". It provides a "rationale for social classification" (Norris 2003: 251).

### ***CCTV and risk***

A further strand is to interpret the increasing use of CCTV in the context of the contemporary shift towards a risk society (Beck 1986). Thus, a changing perception of security can be observed all over the world. New sources of insecurities are located in terrorism, drug trade, growing social inequalities, transnational migration or the vulnerability of information and communication infrastructure. In this context CCTV is understood as a response to risks. The multifunctional potential of it makes it a management tool for all kinds of dangers and possible hazards, such as traffic jams, fire,

tunnel accidents, crime, terrorists attacks etc. In this respect a shift from reactive to proactive policing can be considered. Moreover, it has been pointed out, that the management of risks is not only addressed to state agencies as the police but increasingly to a mixture of institutions and organisations within the security branch. In combination with neo-liberal political programmes and strategies risk management becomes more and more a responsibility of corporate and individual regulation. (McCahill 1999: 54) An installation of a CCTV system leads meanwhile probably in many countries of Europe to price deductions in insurance. The suicide plane attacks of September 11th have certainly roused a world-wide concern for issues of risk and increased the sense of insecurity. It is likely it has intensified the public acceptance for the further installation of CCTV throughout the world.

### ***CCTV and the city***

A further perspective of understanding the increasing use of CCTV is the current trend of commodification urban space. Its increasing employment is described as part of a broader transformation of contemporary cities throughout Europe. Within the reconstruction of the old industrial to the new post-fordist city, which is characterised not by a mixture of functions, but first by the management of leisure and consumption, CCTV is understood as a tool of economic restructuring space. Parallel to architectural revitalisation, declined city centres, e.g. around central stations, shall be "won back" through its employment. It is argued, that the aim is to create a 'commode' space for tourists and consumers. In times of scarce urban financial resources a new emerging understanding of urbanism is suspected to immolate public space for pure economic interest. Reeve considers: "The danger is that this largely insidious move towards a particular and commercially driven conception of what public space is for may lead to management and even policing practices which reduce the social richness of public space and thereby reduces its potential to be genuinely civilising and civic" (Reeve 1999: 73).

Turning away from the idea of urbanism in terms of social difference it is assumed that public space is transformed to homogenised zones. But the purpose of commodification is not just the creation of pleasing and comfortable atmospheres. Within the entrepreneurial city, it is said, that the managing of urban space means to classify people according to their economic purchasing power. According to this visual surveillance could become a tool of social exclusion. It is argued, that people could be sorted out by operators if their appearance and behaviour is not in accordance with the commercial utilisation of space. Hence would follow, the commodification of urban space implies its segmentation according to certain social affiliations, which are negotiated not publicly, but determined by commercial interests. In line with that, it is also seen that the commodification of urban space correlates secondly with an inner commodification of behaviour of those who want to belong to the favoured space. A certain behaviour and appearance is asked for in order to participate on the playground of leisure and

consumption. Within this context the surveillance potential of CCTV turns out to be one of "social sorting" (Lyon 2003).

### **3.2 Legal framework and public debate**

The aim of work package 2 was to give a general overview of CCTV in Europe in terms of its legislation and the public debate. Therefore technical handbooks, academic literature, policy documents and legislation, such as basic rights, data protection, codes of criminal procedures and police laws in seven European countries were surveyed. Moreover, it a discourse analysis of the current debate on the basis of selected articles was carried out.

#### ***Methodology***

In work package 2 each of the six partners (plus the Spanish subcontractor) carried out research according to the categories of comparison as agreed upon at the two-days kick-off meeting in Berlin at the end of September 2001.

In brief these categories include general background information providing the national context of CCTV and an overview of the history as well as facts and figures (market, estimated number of systems etc.) on CCTV for each country. Moreover, each partner was requested to outline the legal context framing CCTV, in particular data protection legislation and police acts. To fulfil these tasks all partners carried out a textual interpretation of relevant literature, media reports and legislation. In addition, some partners interviewed key stakeholders such as data protections officers, criminologists and law enforcement practitioners.

The analysis of the current debate was carried out by a content analysis of three or four newspapers per partner for a period between November 2000 and November 2001. Some research teams carried out an additional mini-analysis of the period following September 11 in order to study if and how the discourse on CCTV changed. Electronic full-text-archives of these newspapers were searched for relevant key words such as CCTV, video surveillance or surveillance cameras. All found articles were coded according to a list of typical contexts, the topic of texts, the orientation towards CCTV, discussed intentions, locations and named targeted groups. Finally, these data were analysed computer aided. This task served as preparation for the written report which outlines typical contexts of CCTV, fields of contestation and advocacy coalitions in this emerging policy field.

#### ***Legal regulation of CCTV***

Modes of legal regulation of CCTV vary greatly across Europe. Its employment is regulated by federal and state data protection acts, by police laws and codes of criminal procedure, by specific laws on video surveillance and furthermore special regulations for

locations such as banks or sport stadiums. Also copyrights provisions touch the usage of CCTV. In some countries strict regulation exists in regard to private CCTV systems. In other countries mainly public systems are legally regulated. However, the findings demonstrate that although the spread of video-surveillance was partly determined by the lack of regulation in some countries, it is not simply the case that legal regulation has limited the rise of CCTV. Since the law has served to stem the growth of CCTV in some contexts, due also to specific facts of the individual political systems, one has to keep in mind that the law also served to legalise existing practises of surveillance.

At the European level CCTV is mainly regulated in the context of privacy and data protection: in particular by Article 8 of the European Human Rights Convention, the European Convention on the Automated Processing of Personal Data of the Council of Europe and the Data Protection Directive (95/46/EC) of the European Union. Especially the latter, which is binding for all member states of the Union, has influenced the national regulation of CCTV during the last years throughout Europe. Passed in 1995 it came into force in October 1998 with the aim to harmonise European data protection legislation. Although it is not in the EU, but nonetheless affiliated with the Union through the Agreement on the European Economic Area (EEA) of 1992, also Norway has replaced its privacy legislation in line with the EU-Directive. Similar, the accession state Hungary revised its 1992 Privacy Law in June 1999. Mainly the directive has led to a lot of similarities among the countries in regard to central definitions of terms like "personal data" or "sensitive data", "data subject" or "data controller", "data collecting" or "data processing". Signifying the political pressure towards the European national governments to update their provisions in respect of new technologies it has led to first more or less direct regulations of video surveillance in the countries.

**Table 1: National provisions especially addressing CCTV<sup>2</sup>**

Denmark	<p>Consolidation Act No. 76 of 1 February 2000 on the ban of video surveillance. This act generally prohibits private entities from monitoring public streets, roads, squares or any similar area used for common travel. There are however, certain exceptions to this prohibition.</p> <p>DPA´s decision of 3 June 2002 concerning video surveillance by a large supermarket chain and live transmission from a pub on the Internet.</p> <p>DPA´s decision of 1 July 2003 stating that video surveillance conducted in privately run public transportation must be proportionate and in adherence with the rules of the Danish Data Protection Act.</p> <p>DPA´s decision of 13 November imposing certain limitations on video surveillance conducted by public authorities.</p>
Germany	<p>Section 6b of the Federal Data Protection Act that governs the deployment of CCTV by private entities and federal authorities other than the police and secret services.</p> <p>Further regulations on video surveillance by state authorities other than the police and secret services in the Data Protection Acts of the 16 German states.</p> <p>Sections 26 and 27 of the Federal Border Police Act.</p> <p>Further regulation on video surveillance by the state police forces in the Police Acts of the 16 states.</p>
Hungary	DPA´s recommendation of 20 December 2000 on how to implement the Data Protection Act.
Norway	Chapter VII in the Personal Data Act No. 31 of 14 April 2000.
Spain	<p>Ley organica No. 4/1997 on video surveillance by security agencies in public areas.</p> <p>Real Decreto No. 596/1999 implementing Act No. 4/1997.</p>
United Kingdom	<p>Section 163 of the Criminal Justice and Public Order Act 1994 that regulates local authority powers to provide CCTV.</p> <p>CCTV Code of Practice 2000 of the Information Commissioner which clarifies the more general provisions of the Data Protection Act 1998 (currently under revision).</p>

<sup>2</sup> This is not a comprehensive list of national provision that apply to CCTV: Other provisions applying to CCTV are found in codes of criminal procedures, assembly acts, sports acts, certain police acts, human rights acts, copyright provisions or case studies.



As a general rule, different acts govern the employment of CCTV for purposes of public safety and the prevention of disorder or crime on the one hand and to all other areas on the other. The former employment is regulated by specific laws as police acts or codes of criminal procedure. The latter use is mostly regulated within the framework of the data protection legislation. Some countries such as Spain have explicit laws for CCTV-surveillance by the police in the public realm. In Denmark the 'Law on the ban against TV-surveillance', which came into force on July 1st 1982 forbids the private use of CCTV in public areas. In other countries such as Germany explicit sections on CCTV by non-police actors can be found in the data protection acts. From case to case this variety causes major differences, for example, in regard to the demand of transparency as required by data protection regulations. In Great Britain there is no explicit CCTV law and there is also no explicit regulation of video surveillance in the British Data Protection Act. But meanwhile there is a "Code of Practice" issued by the British Information Commissioner that sets a framework on how the Data Protection Act of 1998 should be put into practice in regard to CCTV. As this code does not have any independent legal character it is unknown how effective it is. Nevertheless, besides this formal diversity of legal regulations there are different regulatory tools such as the registration of systems as it is known from France, Norway and Sweden or the notification in order to guarantee transparency. But if and how they meet the purpose to protect the universal human right to privacy has still to be evaluated.

### ***Public debates***

One of the main findings is that legal regulation in its own is not sufficient to reconcile video surveillance with the necessary preservation of the human right to privacy. The comparison shows that also the public discourse has its regulative effect, even when this is more indirect. While there is a high standard of regulation in Norway caused by the legally binding duty to register CCTV systems, the public awareness is rather low. In Denmark a stronger public debate is verifiable due to the engagement of the Danish Crime Prevention Council. The extent to which CCTV is an issue in the public debate differs from country to country. If there has been one at all, in the UK the public debate has passed its peak long ago. Events like the abduction of the two year old James Bulger in 1993 chronicled by security cameras in the UK promoted public awareness which however was supportive and not critical. According to our sample of four newspapers (two national and two regional newspapers) most stories still can be found in Britain. This is again not due to a critical debate, but indicates the fact that in England CCTV is a matter of everyday life. In Norway and Austria its use just becomes a topic of public interest while in Germany a debate is recognisable to some degree, which is however limited to open-street CCTV. It is polarised between advocates of the surveillance technology, often convinced of policies of law-and-order, data protectors and civil rights activists.

All news stories and events can be set in a wide range of discursive frameworks. The question is which discourse is prioritised and in whose interest does it operate? It was the aim of a newspaper analysis to study dominant orientations, typical policy actors and their positions and perceptions in order to identify major discourse strategies. The crucial question has been at what point of public perception video surveillance becomes an issue. In all countries where there is some critical debate on CCTV, it is noticeable that they refer to different realms. In Denmark it is the private use of cameras within the public that causes concerns. In Germany it is the use of CCTV by the police, and in Great Britain the use of cameras to enforce speed restrictions on the roads. In contrast to other countries CCTV in Britain is not contested as a crime prevention measure. The variations can be explained by cultural and historical differences. Beyond this, one can conclude, that the sensibility for surveillance measures is contingent upon cultural and individual norms and values. A thesis for further research could be: The closer the surveillance is to pester not only the others but oneself, the less enthusiastic one is about it. Depending on age, sex, profession etc. there are a lot of different perceptions about the benefits of CCTV. A prostitute might welcome the gaze while the suitor might probably feel disturbed.

In addition it has to be mentioned, that although the rise of CCTV in Europe proves the growing demand and opinion polls often indicate a high public acceptance, its rapid proliferation has caused public resistance in many countries. Established organisations raising the issue such as Privacy International which initiated the "Big Brother Awards" exist besides loose networks such as the UK CCTV Surveillance Regulation Campaign or the Surveillance Camera Players engaged in entertaining bored controllers by short performances in front of the cameras.

### **3.3 Locations and actors of CCTV**

The objective of the work package has been twofold. On the one hand side the aim was to give a general overview of the employment of CCTV of the capitals of the participating countries, on the other to map locations of CCTV systems in a selected urban area in order to identify owners and operators, intentions and core features in particular. The aim was to give an overview on video surveillance for each capital of the participating countries, Berlin, Budapest, Copenhagen, London, Oslo and Vienna. Given the thousands of surveillance cameras the ambition was to unveil the actors and intentions behind these myriad inscrutable gazes. What are the differences of the employment of CCTV among these cities? What are common trends across Europe? Also in preparation of the case studies of individual systems in the next work-package the idea was to get a better understanding of the daily reality of video-surveillance in the six capitals. Moreover out of this data it was possible to derive a first proposal for a typology of CCTV systems.

### ***Methodology***

Data on CCTV were collected in each capital at three levels. At the urban macro-level a set of "major urban infrastructure" such as public transport, airports, railway stations and motorways was selected for each capital in order to give an overview of CCTV networks. By media research, semi-structured interviews with security managers and police officers the data was ascertained. Also e-mail and telephone inquiries at press offices of relevant authorities and institutions and visits of CCTV control rooms helped to complete the research. At the micro- and meso-level of a selected high street and the neighbouring area in a multi-functional central district the national research teams carried out a "door-to-door survey" of CCTV in public accessible premises and institutions such as small shops, chain stores, cinemas, post offices, schools, hospitals etc. Thus, the team collected data for 1365 public accessible premises and institutions in the selected high streets. In addition at the meso-level, each national team collated data of 31 types of institutions in the district in which the high street is situated. Thus, the consortium collected and analysed two data sets (high street / 31 institutions) for each surveyed city. The analysis of these data sets served as the empirical basis for the identification of common patterns and differences in coverage, legality and technical sophistication of CCTV systems in a variety of national and/or institutional settings.

For each location with a system respondents, such as owners or managers, were solicited to answer a questionnaire regarding core features of the individual systems. It included 20 questions on organisational and technological aspects such as:

- Who owns the system and who operates it?
- Is there any notice on the system?
- What is the monitor-camera ratio of the system?
- Is the system monitored by observers in real time?
- Are the images recorded?

As part already of the results, one has to state, that especially in Berlin and Budapest there was mistrust against the subject itself and the questionnaire in particular. A lot of people requested here refused the information right from the beginning. Therefore in a lot of cases only an on-site observation was possible. Nevertheless, the analysis of both data sets has served as the empirical basis for the identification of common patterns and differences in the coverage, legality and technical sophistication of CCTV systems in a variety of national and/or institutional settings. Thus, it was the basis for the cross-national typology.

### ***CCTV in major urban infrastructure***

Independent of the national context we find networks of visual surveillance in almost any setting that we treated as "major urban infrastructure" and other key sites of the seven

capitals, such as airports and national government buildings. The major exception is open street CCTV which does not exist in Copenhagen and Vienna and was only found in the outskirts of Madrid and Berlin.<sup>3</sup>

**Table 2: CCTV in major urban infrastructure**

	Berlin	Budapest	Copenhag.	London	Madrid	Oslo	Vienna
Open street CCTV	A few systems within the larger urban agglomeration	Yes	No	Yes	A few systems within the larger urban agglomeration	Yes	No
Public transport	Yes	Yes	Yes	Yes	N.A.	Yes	Yes
Major Motorways	Yes	Yes	N.A.	Yes	Yes	Yes	Yes
Train stations	Yes	N.A.	Yes	Yes	Yes	Yes	No
Airports	Yes	Yes	Yes	Yes	N.A.	Yes	Yes
National Government buildings	Yes	N.A.	N.A.	Yes	Yes	Yes	Yes

It is evident that there are buildings in each capital that are seen as high risk locations. Governmental, ministerial buildings and airports deploy a CCTV system. For these institutional settings surveillance cameras are state of the art. Another strand of CCTV employment is transport. Roads and motorways, Railway stations, undergrounds and urban railways, busses and trams and also taxis are often equipped with cameras. For example in all cities of the survey the underground or urban railway network is capable of a system. From city to city they are used for diverse tasks such as train clearance, train driver assistance, passenger information and emergency services. In addition, in Berlin and Oslo (as trial) also a number of vehicles are equipped with cameras to deter vandalism.

In contrast, in Berlin, Copenhagen and Vienna open-street systems do not exist. Berlin is one of the last four German states where the employment of CCTV is still legally not authorised, even there are strong efforts since years by the conservative party to permit the use at crime hot spots. If seen as a larger urban agglomeration rather than as an administrative unit, there exist three small open-street CCTV systems in the outskirts of

<sup>3</sup> Another exception is the non-existence of CCTV in Viennese train stations.

Berlin: Beyond the borders of the city in the neighbouring state Brandenburg the police started systems in Bernau, Erkner and Potsdam in winter 2001/2002. In Vienna there are just two sites, one at the 'Stephansplatz', the city centre (since 1999), and one on the Kärntnerstraße / Opernring (since 1989/1990), the central high street, where cameras are installed. However, the Police of Vienna does not use them for permanent observation but for the monitoring of events such as the annual demonstration against the opera ball (König 2001: 44).

London is currently the unrivalled world capital for CCTV in public streets and places. Norris and Armstrong estimate that in a single day a citizen of London could expect to be "filmed by over three hundred cameras on over thirty separate CCTV systems" (1999: 42). It is 'guesstimated' that about 4 million cameras monitor the UK, whereas 40.000 are used for open-street CCTV. In respect to open-street CCTV in London more than 1.000 cameras trace and track the routines of the everyday life of its approximately 7.2 million residents. 22 of the 32 boroughs deploy an own system. The CCTV system of the Borough of Newham integrates an intelligent system that is equipped with a facial recognition device.

Next to London Budapest is the URBANEYE sample with the most systems. The first open-street system in Budapest including five cameras was installed in the 5th district in 1997. In 1999 the municipal assembly of Budapest funded the installation of CCTV in further six districts with an amount of 16 million Forint (app. 66.390 Euro). In 2000 again 10 districts received 31.8 million Forints (app. 132.000 Euro). In April 2002 there are in Budapest 14 larger open-street CCTV schemes with about 200 cameras. 7 more are planned. Between 5 and 90 digital cameras per system monitor the areas. Compared to those the only system of Oslo is rather small. It consists of six cameras operated by the police in the area around the railway station.

### ***CCTV in selected high streets***

The findings of the high street sample show the following: From all 1365 cases 29% have a CCTV system and 4% deploy dummy cameras or pretend by a sign that CCTV is in operation. Thus in one third of all sites there is in a sense a surveillance measure.

As expected, the extent of CCTV surveillance is most advanced in London (40%), followed by the Scandinavian capitals Oslo (39%) and Copenhagen (33%). With 28% Budapest comes close to the cross-European average. The extent is less advanced in Berlin (21%) and Vienna (18%). However, these figures need to be handled with caution. The selected high streets in Oslo and Copenhagen are the central boulevards of these capitals. In particular the Oslo boulevard was reported to belong to the most densely surveyed areas in Norway. In contrast, a study carried out in another Berlin high street showed that 19 out of 52 publicly accessible spaces in this area deploy CCTV cameras, i.e. 36.5%. Given this, we assume that the national figures of this data set do

hardly represent the national extent of CCTV. But we believe that the data give us a taste of the extent, legality and sophistication of CCTV in urban Europe.

When ordering the data by institutions rather than nations they show as following.

**Table 3: CCTV at high streets ordered by institutions**

Institution	Total N = 100%	CCTV Systems	Dummy systems
(Metro) station	7	7 cases 100.0%	0 cases 0.0%
National government building	1	1 100.0%	0 0.0%
Bank	70	58 82.9%	0 0.0%
Post office	5	4 80.0%	0 0.0%
Hotel	10	6 60.0%	0 0.0%
Shopping mall	8	4 50.0%	0 0.0%
Public toilet	2	1 50.0%	0 0.0%
Museum	2	1 50.0%	0 0.0%
Chain store / Large retailer	317	127 40.1%	16 5.0%
Prescribing pharmacy	11	4 36.4%	0 0.0%
Restaurant	88	24 27.3%	0 0.0%
Pub / Bar / Café	100	24 24.0%	2 2.0%
Other local authorities	5	1 20.0%	0 0.0%
Small shop / Corner store / Grocery	581	102 17.6%	31 5.3%
Cinema / Theatre	9	1 11.1%	0 0.0%
Public School	1	0 0.0%	0 0.0%
Police station	1	0 0.0%	0 0.0%
College / University	2	0 0.0%	0 0.0%
Religious centre	6	0 0.0%	1 16.7%
Others	123	24 24.0%	1 0.8%
<b>Total</b>	<b>1349</b>	<b>389 28.8%</b>	<b>51 3.8%</b>

The existence of systems varied between different institutions. CCTV is most likely to be found in metro stations as mentioned above. Transport locations in general seem to be a focal point for CCTV. Not only has the history of CCTV underlined this, but also the fact that the first open-street system in Norway and most of the public systems in Germany are located nearby stations. Most of the systems of our sample are private ones. 74% were found in small shops, chain stores, and banks. However, only 18% of all small

shops, 40% of chain stores or large retailers and 83% of all banks use a system. It is very likely to be filmed at every financial institute, banks and post offices. One may assume that in those locations the camera implies also a symbolic value. The money at these places is safe. Striking is, that only 50% (4 out of 8 cases in our sample) of all shopping malls – often thought to be prototypes of controlled urban space – deploy surveillance cameras.

Another matter of interest has been the legality of the systems. In Norway and Germany an adequate warning is legally obligatory to indicate the existence of video-surveillance. In both cases the legislation demands that the conducting of a CCTV scheme and the authority in charge of it has to be made visible by appropriate means. The mentioned British “Codes of Practice” goes even one step beyond. According to the interpretation of the Data Commissioner the demand on notification of the British Data Protection Law requires a number of information in respect to CCTV. In order to fulfil a “fairly and lawfully processing of personal data” people must be aware of the measure and therefore an adequate signage of the conducting of CCTV is requested. All systems should provide details about the identity of the data controller and the stated purposes.

**Table 4: Signage of CCTV systems at the high street level**

	CCTV systems	Missing cases	Valid cases (N = 100%)	Signage		No signage	
Berlin	25 cases	0	25	8 cases	32.0%	17 cases	68.0%
Budapest	60	21	39	7	17.9%	32	82.1%
Copenhagen	75	2	73	38	52.1%	35	47.9%
London	85	5	80	42	52.5%	38	47.5%
Oslo	78	0	78	62	79.5%	16	20.5%
Vienna	66	36	30	3	10.0%	27	90.0%
Total	389	64	325	160	49.2%	165	50.8%

The data suggest enormous differences of signage practices among the six capitals. However, taking the results of the survey into account, slightly more than 50% of all inspected systems were not notified by signs at all. Many systems operate in a illegal or at least in a grey legal area as they do not satisfy the demand on notification. One must assume that the idea of notification is either unknown or not taken serious and therefore ignored. One might argue – as the Federal Government of Germany did when asked for the notification practice at federal buildings that are under video surveillance – that the clear visibility of a camera is a notification. However, the employment of CCTV is an

intransparent phenomenon as in most cases it is not identifiable by whom, how, and for what purposes the system is used for.

This intransparency is also underlined by the response rate of the survey. 43% of the premises operating CCTV denied detailed information, in particular in Budapest (87%), in Berlin (72%) and Vienna (55%).

**Table 5: Response rate**

	Premises with CCTV (N = 100%)	Respondents who answered the question for ownership of CCTV	Answer rejected (Secrecy indicator)
Berlin	25	7 28.0%	18 72.0%
Budapest	60	8 13.3%	52 86.7%
Copenhagen	75	58 77.3%	17 22.7%
London	85	63 74.1%	22 25.9%
Oslo	78	57 73.1%	21 26.9%
Vienna	66	30 45.5%	36 54.5%
Total	389	223 57.3%	166 42.7%

Another item of the survey has been the organisation and technological sophistication of CCTV systems. 74% of the systems are monitored by observers who, however, often have to fulfil other tasks (90%). Thus, the effectiveness of CCTV in imposing a panoptical gaze is likely to be very limited. Given this it is not surprising that 76% of the systems record the images.

Over half of the systems in the overall sample are small isolated systems with very little technological sophistication. 53% of the systems are equipped with not more than 3 cameras, just 11% with more than 10 cameras.

**Table 6: Sizes of CCTV systems at the high street level**

Sizes of the CCTV systems	Number of cases	Percentage
Less than 5 cameras	176	66.9%
5-9 cameras	58	22.1%
10-19 cameras	25	9.5%
20-49 cameras	3	1.1%
50 and more cameras	1	0.4%
Total	263	100.0%



But the study shows that for larger systems there is a trend to integrate these by the implementation of new technologies and also by the rationalisation of management and organisation of surveillance practices. 1/3 of all systems employ a linkage to other systems. 50% of all systems with more than 10 cameras are linked to others by either switching images (33%) or some kind of communication link (46%). In contrast, just 8% of all the small systems with less than 4 cameras are able to switch images and only 23% use a communication link. Hence follows the likeliness that a big system (>10 cameras) uses a device to switch images is four times higher than for small systems (<4 cameras), and that it uses a communication link twice as high.

When comparing the rise of video-surveillance in individual countries, it is obvious that its diffusion is very unequal, and it is apparent that different countries in Europe are following different paths. The public awareness and also the academic knowledge about the development of CCTV varies highly from country to country. The extent of CCTV in public space in the individual countries seems to be dependent on different factors: the socio-economic contexts, the political constellations and their dealing with urban problems such as crime and also legal traditions.

Obviously there are some significant similarities between the UK and Hungary in regard to the perceptions of benefits and the implementation strategies of open-street CCTV. Both countries have undergone a more rapid socio-economic transformation process in the last decades than all other countries. With the economic crisis of the 1970s unemployment increased in Britain, poverty became visible, and rising crime rates alarmed politicians. New strategies of control such as "zero tolerance" or "community policing" emerged in the changing political climate of the 1980s, which combined "economic liberalism, reduced public expenditure and an emphasis on individual moral responsibility, with populist law and order politics." (Coleman and Norris: 2000: 149) The focus in crime prevention shifted from the offender and his social background to the offence and its proactive management. In this context CCTV was seen as an adequate tool of such proactive strategy of social control. In Hungary after the fall of the iron curtain the economy of the country collapsed with the consequences of immense fiscal problems, decreasing incomes and increasing crime rates. Confronted with public demands to combat crime and the sudden need to position Budapest in international urban competition CCTV appeared as a promising 'silver bullet' of the west against the 'evils' of a new era. In addition, in both countries, the lack of explicit legal regulation enabled the rise of open-street CCTV.

To conclude, while the extent of open-street CCTV differs extremely throughout Europe, it is spreading in the semi-public and private realms in similar ways and likewise dimensions. Moreover, according to the results of the URBANEYE project show that the rise of CCTV is following two trends.

### ***Typology of surveillance***

In an attempt to organise the diversity of video surveillance in a more systematic approach we finally developed a cross-national typology of CCTV:

This typology locates individual systems between vision (the capacity to make those under surveillance visible to an observer) and visibility (the capacity to induce the feeling of being under the gaze of the camera). Moreover, the "activity" of a CCTV system – understood as socio-technical system – in terms of recording footage and potential intervention is considered. Derived from these dimensions we finally outlined 16 levels of "surveillance intensity" that indicate degrees of asymmetry in power and violation of privacy.

Matching the collected data with this typology shows that a majority of CCTV systems aims to prevent deviant behaviour by symbolic but more or less incompetent deterrence rather than permanent and exhaustive surveillance combined with intervention. These systems are hardly able to make those under surveillance visible to an observer because of irregular monitoring, informational overkill, or even because of deploying dummy cameras.

However, most systems record footage and staff is supposed to react to events caught on camera. Therefore our data indicate that many systems operate beyond the critical edge of moderate surveillance in which power relations between the observers and the observed are rather balanced. For reasons of proportionality these forms of surveillance either need to serve a clear defined and legitimate purpose or power balance need to be restored by enhancing the transparency of surveillance operations.

### **3.4 CCTV systems and practices**

WP 4 aimed to study selected CCTV networks in six countries as socio-technical systems. The structure of such systems consists of different technical and non-technical resources and rules. Resources are the workplace including all technologies and functions, the staff and their mentality. The rules are shaped by the interrelation and internal negotiation of the discursive consciousness of "what to do" and the practical consciousness of "how to do it," as well as their adequacy in everyday practice. Both the systems' structure in terms of technical functions and spatial configuration of control and the systems' practices in terms of management and everyday observation were analysed in order to compare the styles of employment in the participating countries. Studying the patterns of observation the practice of CCTV the idea had been to identify groups and styles of behaviour targeted by video surveillance. By doing this, the project aimed to examine whether CCTV is an adequate instrument to counter disruptive behaviour and maintain social discipline thus helping to guarantee social cohesion in Europe, or whether it only serves partial interests biased against fringe groups thus being an instrument of social exclusion and discrimination.

## ***Methodology***

Though initially each local team of URBANEYE was supposed to study two comparable CCTV systems in detail, the manifold obstacles which we were confronted with in the field compelled the team to choose a different and rather pragmatic approach. As it was already clear after work package 2 that getting access to the field as planned would be very difficult, the agreement was made to study only one CCTV system in a shopping mall in detail, and to carry out more superficial “flashlight observations” in a public transport CCTV network, a CCTV system used for facility management in a publicly accessible “intelligent building” and – if in operation – in an open street CCTV system. However, again the local teams had to modify the plan because they were confronted with many obstacles in practice. In particular getting access to CCTV control rooms of shopping malls for participant observation was not possible in all countries. However, each team who was confronted with such obstacles found ways to substitute the task. They either decided to carry out their observations in another kind of CCTV system or to study more shopping mall systems for a shorter period of time.

In order to describe the technical and social organisation of the CCTV systems the teams interviewed managers and CCTV operators according to a common semi-structured interview guide. The interview guide addresses issues such as the risk assessment that guided the technical design of the systems, the rules and organisation of work, and the attitudes of the operators towards their workplace and their field of observation.

Studying the control room routines and surveillance practices by participant observation, the researchers collected both qualitative data by writing down field notes and quantitative data by keeping an observation schedule with logs on targeted surveillances, the reasons for targeting, who initiated the targeting, the type of suspicion, the characteristics of targeted persons, deployment, arrests and information about the shift. A targeted surveillance was defined as any incident where an operator took control of the cameras by zooming in on and/or tracking individual persons or artefacts for 30 seconds and more.

Eventually the research that was done by each partner was as following.

- The *Berlin Institute for Social Research* (BIS) carried out 10 case studies. CCTV systems in one railway station, an airport, six shopping malls, a soccer stadium and an urban entertainment centre were studied in more or less detail. Therefore 17 semi-structured interviews with managers and operators of CCTV systems were conducted. Eight flashlight observations and 40 hours observation of control room work were carried out. Despite their efforts it was impossible for the BIS researchers to get access to CCTV control rooms for more than two days for participant observation. Thus, they carried out a socio-geographic survey of 62 Berlin shopping malls and their surveillance regimes. In addition, three heuristic experiments in order

to investigate the awareness of control room staff to events not in line with the house rules of selected shopping malls have been done.

- The *Budapest University of Technology and Economics* (BUTE) was also unable to get access to control rooms of shopping malls. Moreover, the management of privately owned CCTV systems in Budapest was very reluctant to allow access in general. However, eventually the BUTE researchers were able to carry out two case studies in an open-street CCTV system operated by the Hungarian police and a CCTV network at a main national bus station. In total they conducted 18 semi-structured interviews and 240 hours of participant observation.
- The *University of Hull* (U-Hull) studied four cases of CCTV networks in London: a public network, a system in a mainline railway station and systems in two shopping malls. This was done by 23 semi-structured interviews with managers and CCTV operators, three flashlight observations and a 120-hours-observation in one South London shopping mall.
- The *Norwegian University of Science and Technology* (NTNU) carried out case studies of 14 CCTV systems in the Norwegian capital Oslo and the Danish capital Copenhagen: four shopping mall systems, one open street system operated by the police, two networks in public transport, two traffic management systems, one airport system, and video surveillance systems in an exclusive commercial complex, in a cultural institution, in a department store, and in public toilets in Copenhagen. Therefore the NTNU researchers carried out 25 interviews, conducted six flashlight observations and observed the work of control room staff for 124 hours.
- Finally, the *Interdisciplinary Centre for Comparative Research in the Social Sciences* (ICCR) studied 10 cases of CCTV systems in Vienna: two banks, one football stadium, one business area, two department stores, two shopping malls, one traffic management centre and one public transport network. In total, the ICCR researcher carried out four flashlight observations and 10 interviews.

**Table 7: Studied CCTV systems**

CCTV in	Berlin	Budapest	Copenhagen & Oslo	London	Vienna	Total
Shopping malls	6 (2*)	-	4 (1*)	2 (1*)	2	14 (4*)
Public transport	1	1*	2 (1*)	1	1	6 (2*)
Open street	-	1*	1*	1	-	3 (2*)
Traffic management	-	-	2	-	1	3
Airports	1	-	1	-	-	2
Other	2	-	4*	-	6	12 (4*)
Total	10 (2*)	2*	14 (5*)	4 (1*)	10	40 (12*)

An asterix\* indicates systems that were studied by more than a "flashlight observation", i.e. by participant observation of at least one hour and interviews with managers and control room staff.

To summarise, the URBANEYE team studied 40 CCTV systems in a wide range of institutional settings. In total, 93 semi-structured interviews (á 30-90 minutes) with managers and operators of CCTV systems were conducted. Flashlight observations were realised in 17 cases. Observations lasting at least an hour were done in twelve cases with a total of 524 observation hours. Thus, eleven CCTV systems were only studied by interviewing staff. In addition, the BIS team carried out three heuristic experiments testing control room staff reactions to undesirable events in shopping malls and realised a socio-geographic survey of 62 shopping malls and their surveillance regimes in Berlin.

### ***Systems***

CCTV systems are characterised by potential multifunctionality and formal diversity. One cannot make any generalisation about the extent, nature and impact of CCTV surveillance from the mere existence of a system. The practice in terms of management and everyday observation clearly depends on the structure of technical functions, of the work organisation and the spatial configuration of the observed space. This findings leads to the following hypotheses:

1. While the general rise of CCTV within a country depends upon national differences such as legal regulations, the surveillance practice of a CCTV system depends upon the institutional context of operation and the space under surveillance.
2. The institutional context is not only of relevance for basic features of CCTV but also for the in-depth analysis and comparison of CCTV in action.

CCTV systems have diverse levels of technological sophistication, operating procedures and staffing policies, and they can be deployed for various purposes: law enforcement, information and service to the public, general safety or a combination of all. According to the institutional setting we differentiate three sorts of CCTV systems for analysis

**Table 8: The sample**

City	CCTV in shopping malls	CCTV in public transport	Open street CCTV
Berlin	two Berlin shopping malls		
Budapest		a coach station in Budapest	an open street CCTV system in Budapest
London	a shopping mall in South London	a London mainline railway station	a London borough public CCTV network
Oslo	A shopping mall in Oslo	a major public transport centre in Oslo	the open street CCTV system in Oslo
Vienn		the underground network in Vienna	

**Shopping mall systems:** In the academic literature shopping malls are often described as a kind of prototype of a controlled urban space (e.g. Wehrheim 2002). Thus, we expected to find CCTV in shopping malls as an ubiquitous instrument to enforce discipline and exclude unwanted individuals in order to maintain the commercial image and provide a convenient atmosphere for consumption. However, the collected data show the necessity to modify these assumptions about the function of CCTV to "purify space".

In regard of their infrastructures shopping malls can be understood as high-tech dispositions which are equipped with a lot of different sorts of technologies, such as escalators and elevators for transport, smoke detectors and fire alarms for accident prevention. Within this conglomerate CCTV is only one technology among others. The crucial question is how CCTV is actually used in a particular spatial regime of a mall. The case studies provide evidence for both the proactive use and exclusion on the one hand and the more or less passive but symbolic existence of CCTV systems.

**Public transport systems:** In this sector CCTV is operated as a multifunctional tool for the management of all kinds of risks. A central purpose is the prevention of accidents. Cameras are used for the supervision of traffic conditions, crowd management, control of technical instruments, communication with passengers via service and emergency points, control and co-ordination of employees and finally the deterring and detecting crime. However, this does not exclude functions of social control. Passengers as well as employees within the transport area are observed for different reasons. Moreover, the surveillance capacity is increasing with the expansion of digital systems and their integration with intelligent scene monitoring, and the opacity of the actual purposes for which CCTV is used is growing with the linkage of systems to third parties such as the police or fire departments. In addition, several theorists have noted that the rise of CCTV is closely related with the privatisation and commodification of urban space (Reeve: 1998). Though being still places of transit, stations of all kinds tend to become more and

more places of sojourn and consumption. Thus the desire for a “feel-good atmosphere” in which “flawed consumers” have no space also drive CCTV operations in public transport.

House rules are often an essential part of this risk management regime, and CCTV is used to support the enforcement of these rules. The less regulated the operation of these CCTV systems is the more likely is the practice of surveillance to be governed by personal attitudes. This might be part of the logic of the new surveillance as the observation task is very impersonal and keeps the operators at distance. However, where the spaces of transit have also become spaces of consumption it might occur that house rules aim to exclude unwanted individuals, such as buskers or beggars. Under these circumstances discriminatory targeting practices might be in complete accordance with the purposes of the system. An operator of the Budapest coach station, for example, reported that there is no interest in individuals, but in keeping the area “clean”.

**Open street systems:** The universally declared purpose of open street CCTV is to reduce crime and the fear of crime. While “crime prevention” is on top of the list of arguments of those who demand and support open street, it is apparent that the use of footage for criminal investigation is of at least equal importance in daily practice. Open street CCTV systems in Europe differ significantly in seize, technological sophistication, organisation etc. These features seem to be very much determined by the legal framework: While issues such as the selection of the monitored space, storage times for footage or the operating agencies are, for example, rather clearly defined in Germany by the state police acts, they are more or less unregulated in Britain. As a consequence the “German model” of open street CCTV is a rather small system focussing on “crime hot spots” that is usually operated by the police and closely integrated with the deployment forces. In contrast, many British systems are operated by local councils, cover extensive areas and are often only loosely integrated with the deployment forces.

### ***Practices***

However, even if the institutional contexts and the spaces under surveillance are comparable, beyond this the practices of surveillance are contingent upon a large variety of further factors. The socio-technological organisation of surveillance is crucial for the practice of surveillance. Thus besides the official policy of a CCTV system it are the functionality of cameras, recording capacities, ergonomic design of control rooms, management, the organisation and scope of work, the integration of observers and deployment forces and last but not least the individual skills and attitudes of CCTV operators that count. Studying the practices has shown that the use of CCTV systems is depending on the individual working ethos of the personnel. The attitudes shape the operational procedures. Attitudes towards the technology and the management regime determine the personal engagement of observers. The mere presence of a system in a shopping mall does not mean that it is permanently used in a well organised and efficient manner.

The objectives publicly claimed by the management of several shopping malls – crime prevention and the like – could not be achieved because the everyday practice presents other tasks to the operators. The workplace, the personnel, their multiple tasks, their qualifications support more a reactive use of video surveillance than a proactive targeted observation of individuals, even if the equipment would allow for that. It is doubtful that the publicly stated objectives are the same as the internal ones. We must assume that those objectives are a part of an “impression (management) scenery” (Goffman 1990), while video systems are meant and used for other purposes involved with core business process of the mall. The case of the South London mall shows a lack of proactive use of the CCTV system partly due to the high level conflict that produced divided and disillusioned work force. The disillusionment amongst the guards was reflected in their use, or rather non-use of the CCTV system.

As targeting, interpreting and reacting to a scene from a distance according to a specific purpose is a difficult task, in particular accountable management and an adequate operator training are important for an effective and responsible functioning of a CCTV system. In all the studied systems there is some kind of training, but it is hard to say how intense training really is. Often it is only a kind of house training that can be based on former skills or in combination with some further programmes as police training. All in all there are no standards for training, nor in terms of the content nor in terms of its temporal extent. The training is often self organised and is carried out by ‘coaches’ that work already for the system. These are full-time employees with extensive knowledge of it.

Finally, our research suggested that the sensory limitations of video screens and the distance between the observers and the observed encourage the application of categorical suspicion based on a narrow range of readily observable traits rather than the application of behavioural suspicion. CCTV operators might tend to target whole categories of the public seen as likely criminals or nuisances. Operators mostly describe situations where they can see “immediately” if there is a threat or not. “They come in with big empty bags, this is already suspicious, then they clear shelves in ‘Douglas’ [perfumery] or ‘Kd’ [drugstore]. They are four, two for the lookout, two to go into the store and to do the job. We have to catch them when they are trying to escape.” In that case, the video recording serves as safeguard for the security personnel.

But if this occurs and which consequences it entails also varies according to structural factors such as the fit between mandated activities and available time, the relationship of the operators and those in the field and the function of monitored space. In particular the growth of CCTV in semi-private spaces such as shopping malls bring with it an increasing emphasis on exclusion as dominant strategy of social control as it is reported from Oslo and London. Mall exclusionary practices are shaped by the discretionary powers of private security officers. On this site, most ejections from the mall were reserved for ‘known troublecausers’ and ‘shoplifters’.



### **3.5 The social effects of CCTV**

The objective of work package 5 was to analyse and compare the social implications of CCTV. Thus, it was studied how people experience CCTV and with what effects by a comparative quantitative street survey of 1,000 citizens in Berlin, Budapest, London, Oslo and Vienna. In addition, around 30 respondents were interviewed in-depth.

#### ***Methodology***

The URBANEYE team agreed to carry out standardised interviews with around 200 citizens per surveyed city in the course of 2003. The questionnaires used in the different countries were carefully translated versions of an English questionnaire. This questionnaire was a four pages questionnaire including questions about street-using behaviour, the knowledge, imaginations, attitudes and experiences regarding CCTV in urban space and some socio-demographic background data.

Most respondents were selected by a street survey in different locations across the capitals of five countries. Preferable people should be interviewed in the vicinity of shopping malls as CCTV in this type of urban space was the main focus of the previous work package. However, due to practical reasons it was not possible to complete the sample in all cases solely near shopping malls. Depending upon the particular local situation some researchers had to move to other places in order to complete the sample in time. Thus, some completed their sample in inner-city transportation centres and high streets. The interviews themselves took 15-25 minutes. In total 1,001 persons were interviewed between June 1 and October 24, 2003. As those who avoided giving an interview were not counted, we have no data about the refusal rate. The size of the sample was approximately similar in all countries. However, in London only 180 respondents were interviewed while it were 218 in Oslo. The quota recruitment structure ensured a rather good balance in terms of gender and education. In terms of age those aged between 15 and 39 years are overrepresented on cost of the elderly in comparison to the demographic age distribution. In terms of time the majority of respondents were afternoon visitors while only one tenth of those interviewed were evening visitors.

Given the pragmatic approach to data collection that was necessary in order to complete the work in time and the structure of the sample, we need to stress that our findings are in formal methodological terms neither strictly representative nor comparable. However, we talked to a broad range of people with very different backgrounds in terms of age, profession, education or political affiliation. Thus we can claim that we have taken the pulse of public opinion, knowledge of and experience with video surveillance" – at least the pulse we have found present at central urban areas under surveillance. Moreover, our analysis and interpretation of the data is informed by a comprehensive review of previous research on public opinions on and the social implications of CCTV.

**Table 9: The survey sample**

<b>N (% per country)</b>	<b>Berlin</b>	<b>Budapest</b>	<b>London</b>	<b>Oslo</b>	<b>Vienna</b>	<b>Total</b>
8 am - 2 pm shift	72 (35.5%)	63 (31.5%)	79 (43.9%)	57 (26.1%)	104 (52.0%)	375 (37.%)
2 pm - 7 pm shift	100 (49.3%)	71 (35.5%)	98 (54.4%)	141 (64.7%)	95 (47.5%)	505 (50.4%)
7 pm - 10 pm shift	31 (15.3%)	66 (33.0%)	1 (0.6%)	20 (9.2%)	1 (0.5%)	116 (11.6%)
Missing values			2 (1.1%)			2 (0.2%)
Male	101 (49.8%)	100 (50.0%)	106 (58.9%)	115 (52.8%)	103 (51.5%)	525 (52.4%)
Female	102 (50.2%)	100 (50.0%)	74 (41.1%)	103 (47.2%)	97 (48.5%)	476 (47.6%)
Aged 15-19	15 (7.4%)	17 (8.5%)	33 (18.3%)	54 (24.8%)	28 (14.0%)	147 (14.7%)
Aged 20-39	69 (34.0%)	67 (33.5%)	105 (58.3%)	75 (34.4%)	87 (43.5%)	403 (40.3%)
Aged 40-59	69 (34.0%)	68 (34.0%)	29 (16.1%)	51 (23.4%)	77 (38.5%)	294 (29.4%)
Aged 60+	50 (24.6%)	48 (24.0%)	13 (7.2%)	38 (17.4%)	8 (4.0%)	157 (15.7%)
School pupils	6 (3.0%)	4 (2.0%)	8 (4.4%)	22 (10.1%)	15 (7.5%)	55 (5.5%)
Elementary school graduates	82 (40.4%)	34 (17.0%)	35 (19.4%)	45 (20.6%)	52 (26.0%)	248 (24.8%)
High school graduates	34 (16.7%)	95 (47.5%)	39 (21.7%)	66 (30.3%)	83 (41.5%)	317 (31.7%)
College graduates	80 (39.4%)	67 (33.5%)	98 (54.4%)	80 (36.7%)	50 (25.0%)	375 (37.5%)
Missing values	1 (0.5%)			5 (2.3%)		6 (0.6%)
<b>Total</b>	<b>203</b>	<b>200</b>	<b>180</b>	<b>218</b>	<b>200</b>	<b>1,001</b>

Additional qualitative data were collected by researchers of three local teams (Berlin Institute of Social Research, Budapest University of Technology and Economics, Norwegian University of Science and Technology). They recruited respondents of the quantitative survey, school children, marginalised people such as drug users and informants from their wider social networks for individual in-depth interviews or group interviews. In total, 33 respondents were interviewed, 18 males and 15 females. 6 of them were school children, 14 middle aged and 13 aged 50 years and older. The in-depth interviews focused not only on experiencing CCTV but also included questions for mental maps, the use of urban space and fear and safety. Usually the interviews took between 60 and 90 minutes but some took two hours and more. All interviews were tape-recorded and transcribed.

The comparison based in particular on the quantitative data that were merged after some modifications of the national data sets and then analysed computer-aided. Though much more analysis could be done (i.e. multiple regression analyses) the analysis was mainly limited to descriptive statistics such as cross-tabulating because of the tight schedule.

### ***Acceptance***

Confirming previous studies that have surveyed public opinions on CCTV in Britain, Germany, Finland, Denmark or Switzerland, we found a majority of respondents being supportive of CCTV in all five capital cities. However, national differences in the acceptance of CCTV are significantly with Britons being most supportive and Austrians and Germans being rather sceptical. Moreover, people draw a clear line *where* they accept CCTV. Most people support CCTV in banks or transportation facilities while they oppose it in intimate spaces such as changing rooms. In international comparison the most different attitudes were found towards open street CCTV. which is seen as a "good thing" by 90% of the respondents in London and by only 25% in Vienna.

To study the attitudes we asked the respondents to answer the question if they find CCTV a "good", "bad" or "neutral" thing in 12 different settings, such as open streets, shops, station platforms, taxis or changing rooms.

**Table 10: Attitudes towards CCTV at...**

	<b>Good</b>	<b>Neutral</b>	<b>Bad</b>
Bank counters	91.9%	3.8%	4.3%
Subway / railway platforms	86.7%	9.3%	4.0%
High street shops	82.9%	10.2%	6.8%
Shopping mall walkways	62.5%	23.4%	14.1%
Along motorways	62.6%	21.9%	15.5%
Open high streets	56.1%	21.5%	22.3%
Taxi passenger seats	46.6%	24.9%	28.5%
Hospital wards	42.7%	28.6%	28.6%
Outside entrance to homes	36.1%	27.1%	36.8%
Public toilet washrooms	22.2%	17.5%	60.3%
Sports centre changing room	13.8%	17.8%	68.4%
Clothing store fitting room	13.0%	13.6%	73.4%

As we see, a majority of respondents is positive towards CCTV at banks, station platforms, shops, shopping malls, along motorways and in open streets. In contrast, a majority is negative towards CCTV in public toilet washrooms, changing and fitting rooms. While the character of the spaces where CCTV is clearly opposed can be easily described as intimate, it is not easy to get hold of a common denominator of the locations where CCTV is supported. Some might be seen as monofunctional or less "social" and thus frightening spaces, such as station platforms. For other locations people might accept the interest of property owners to protect their assets. Or they simply recognise the "power of facts" when they support CCTV at banks or in stations.

In attempt to reduce the complexity we summarised the attitudes towards CCTV in different settings and coded for a "supportive" attitude when positive answers for the attitudes towards CCTV in our twelve settings outnumbered the negative. The general attitude towards CCTV was coded as "ambivalent" when the positive and negative answers were balanced.

**Table 11: General attitudes towards CCTV**

	supportive	ambivalent	critical	Total
Berlin	112 (56.0%)	10 (5.0%)	78 (39.0%)	200
Budapest	136 (70.1%)	16 (8.2%)	42 (21.6%)	194
London	167 (94.4%)	3 (1.7%)	7 (4.0%)	177
Oslo	149 (73.4%)	14 (6.9%)	40 (19.7%)	203
Vienna	91 (45.5%)	26 (13.0%)	83 (41.5%)	200
aged 15-19	94 (66.7%)	7 (5.0%)	40 (28.4%)	141
aged 20-39	235 (63.7%)	26 (6.5%)	118 (29.7%)	397
aged 40-59	196 (67.6%)	27 (9.3%)	67 (23.1%)	290
aged 60+	112 (76.7%)	9 (6.2%)	25 (17.1%)	146
Total	655 (67.2%)	69 (7.1%)	250 (25.7%)	974 (27 missing)

As the table above shows the majority of respondents is supportive of CCTV in general. However, in Vienna we only found a relative majority being positive on video surveillance at the majority of our 12 settings. Here and in Berlin more than one third of the respondents were critical about CCTV. In contrast, in London an overwhelming majority of 94% found CCTV at more settings a "good thing" than a "bad thing". While a clear majority in all countries is supportive of CCTV at banks and station platforms, it is opposed by a clear majority in all countries in intimate spaces such as sports changing rooms and clothing store fitting rooms.

Culturally the most different was the acceptance of public area CCTV, which was welcomed by 90% in London and only by 25% in Vienna. Interestingly Londoners were not being most supportive of CCTV for all settings. The Viennese, for example, though often rather sceptical, were being most supportive for CCTV along motorways. This might be explained by the fact that CCTV in Austria was mainly discussed in the context of Alps tunnel safety. People in Oslo were most supportive for CCTV in taxi passenger seats; maybe because CCTV was recently discussed after assaults against taxi drivers. As these examples show, attitudes towards CCTV are not only culturally shaped but are also contingent on local and temporal contexts. If the differences in the general attitudes towards CCTV are a result of the different extents of diffusion as found in work package

3, or if the different extents are determined by the different attitudes remains a question for further research.

### ***Attitudes***

In addition, the respondents were asked for their agreement or disagreement with five statements in favour of CCTV and five critical statements on CCTV (see Table 12). Two thirds of the respondents agreed with the statement that "who has nothing to hide, has nothing to fear of CCTV", but more than 53% believe that "CCTV footage can be easily misused" and around 40% believe that "CCTV invades privacy". Moreover, most respondents seem not to be convinced that CCTV is an effective tool for crime control. More than 50% agreed with the statement that "CCTV displaces crime" and 56% doubted that "CCTV protects against serious crime".

In European comparison, the most optimistically about CCTV were respondents in London: More than two third of the interviewed Londoners would "welcome in their street" and almost half of them would "feel safer with CCTV everywhere". In particular the believe in the crime effects of CCTV seems to explain this support: 47% believed CCTV to "protect against serious crime".

In contrast, the most sceptical were respondents in Vienna: Less than 10% of the interviewed Austrians agreed with the statements "I would welcome CCTV in my street" or "I would feel safer with CCTV everywhere". As Londoners support might be explained by their trust in CCTV's effectiveness, so can the scepticism of the Viennese: Only 4% of the respondents believe CCTV to "protect against serious crime".

**Table 12: Agreement with statement on CCTV**

	Berlin	Budapest	London	Oslo	Vienna	Total
Nothing to hide, nothing to fear	70.0%	77.6%	75.0%	67.1%	43.0%	66.4%
Footage can be easily misused	65.7%	31.3%	55.0%	41.8%	73.0%	53.2%
CCTV displaces crime	55.2%	55.2%	40.6%	35.8%	65.5%	50.5%
Hidden cams are OK	37.4%	72.1%	67.2%	41.3%	6.0%	44.3%
CCTV invades privacy	49.3%	37.8%	41.1%	42.9%	35.5%	41.4%
Cameras are a poor substitute for police officers	65.5%	22.4%	44.4%	44.5%	19.5%	39.3%
I would welcome CCTV in my street	28.6%	29.4%	68.5%	17.5%	3.5%	28.5%
I would feel safer with CCTV everywhere	29.2%	22.4%	45.6%	28.4%	3.5%	25.4%
Unfair use by discriminatory targeting	39.1%	17.4%	29.1%	22.8%	13.5%	24.3%
CCTV protects against serious crime	23.8%	14.9%	46.6%	27.1%	4.0%	22.8%

In terms of socio-demographic rather than national background, gender turned out to be of minor importance as predictor for peoples' attitudes towards CCTV. Thus we conclude that women's safety feeling is not increased significantly when being under surveillance and thus their opinions on CCTV do hardly differ from those of men.

In contrast, age was found to be most likely to influence the opinion on CCTV. As a general rule younger people were much more likely to be found opposing CCTV and doubting its benefits than the elderly. Though these differences between the generations are often explained by different levels of vulnerability previous studies suggest that it is a general desire for social order rather than individual fear of crime which makes people likely to support CCTV (e.g. Ditton 2000, Reuband 2001). In this context we interestingly found teenagers most likely to be disciplined: Almost one third of the respondents aged under 20 thought that CCTV affects their behaviour while only 14% of those aged 60 and older thought so.

Although people do not know much about CCTV, its growing presence in urban space has become part of their consciousness – they are feeling the gaze rather than seeing the eye: 75% of the respondents believed the survey area to be under CCTV surveillance but

only 36% of them were able to point to the next camera. Moreover, many people tend to overestimate the technological potential of surveillance: 36% of the respondents believed all or most of the surveillance cameras in their city to be capable of taking close-up images of faces, and 29% thought all or most CCTV systems to be able to automatically recognise individuals or licence plates. Thus, in contrast to our results of work package 3 in which we found the reality of CCTV to be dominated by small, isolated and technologically poor systems, people see CCTV as a powerful technology of social control.

### ***Trust and regulation***

In terms of trust, a majority of respondents prefer the police to operate an open street CCTV system. Moreover, regulation matters for most of them.

**Table 13: Regulations seen as "very important"**

	Berlin	Budapest	London	Oslo	Vienna	Total
Restricted access for the media	93.0%	66.2%	87.7%	82.0%	75.0%	80.9%
Restricted access for commercial interests	97.0%	56.7%	69.8%	82.3%	90.5%	79.5%
Inspection	93.0%	83.6%	90.3%	90.6%	13.0%	73.8%
Registration and licensing of CCTV systems	85.0%	64.2%	86.9%	90.1%	21.5%	69.2%
Access to (image) data	53.2%	39.8%	57.7%	67.8%	90.5%	61.9%
Signage	45.0%	54.2%	64.4%	55.6%	47.0%	53.0%
Limited storage times of footage	65.7%	22.4%	34.7%	43.8%	26.0%	38.5%
Restricted access for the police	20.9%	56.2%	14.6%	29.1%	26.5%	29.9%

In particular to restrict access to footage for the media and commercial interests was of uttermost importance for most respondents. Inspection, registration and licensing was also seen as very important by more than two third of the respondents. Interestingly signage and limitations to footage storage times were of secondary relevance. To restrict access to footage for the police was seen as very important by less than a third of the overall respondents.

In international comparison, people shared a very similar view on the importance to restrict access to footage for media. Culturally most different were the opinions on regulation for the issues inspection and registration, in particular because these are given low priority by respondents in Vienna. Interestingly, a majority of respondents in Budapest found it "very important" to restrict access to footage for the police which



might reflect some distrust in state surveillance inherited from the socialist period. However, when asked for the most trusted operator of CCTV, the police was also the first choice of respondents in Budapest: 57% of the respondents said that they would "feel most comfortable" if an open street CCTV system would be operated by the police.

### **3.6 The policy implications of CCTV**

The core of work package 6 was a workshop with around 30 experts. It was held at the European Academy in Berlin December 9<sup>th</sup> and 10<sup>th</sup> 2003 and has to be seen a key dissemination event of the whole project. However, its aim was twofold. Firstly the findings of the URBANEYE project ought to be presented and discussed with the invitees. Many of them are directly involved in the praxis of surveillance. It was intended to check the relevance of the results and to clarify discrepancies with the experts' experiences. In the end the group included politicians, policemen and risk managers, legal experts, data protectionists and civil rights activists, technologists and members of relevant interests groups. This assemblage of different professional perspectives could guarantee a strong variety of feedback. Given that they came from 8 different countries (including Austria, Canada, Denmark, Germany, Great Britain, Hungary, Netherlands and Norway) and the speed of the proliferation of CCTV differs from country to country this was even intensified and also an international exchange encouraged.

Moreover, as the overall objective of the URBANEYE project is to outline strategies for regulation on the basis of our analysis of the employment and social and political impact of Closed-Circuit Television (CCTV) in Europe it was secondly aimed to enquire the experts' opinions and assessments regarding the political impacts of CCTV. The try was to formulate first directions for policy recommendations. For this reason it was again the aim to confront different national, professional and political perspectives of the stakeholders. It has been quite astonishing that despite the different expert views on the use CCTV there were many consensuses in terms of the necessity of regulating the use, but also in terms of the difficulties to find *the* appropriate tools therefore.

#### ***Workshop Procedure***

Next to the lively feedback on the presentation of the URBANEYE results both days of the workshop addressed a large variety of topics related to surveillance and CCTV in particular. Including the presentation of results the workshop procedure comprised five major parts.

1. Presentation of URBANEYE Results + Feedback
2. On the first day the experts discussed in four parallel panels the following main topics in accordance with their professional backgrounds:
  - CCTV as instrument of risk management

- CCTV and policing
  - the state of the art and future perspectives of the technological development
  - CCTV and civil rights.
3. On the second day participants from mixed policy fields were asked to criticise in three work groups scenarios of CCTV systems. These fictive settings were previously written on the basis of the URBANEYE field work. The idea was to give the experts the chance to state problems in terms of system's legality, practicability, efficiency etc and to come up with suggestions for the regulation of these surveillance settings. The results of both days were presented at the end of the session.
  4. In between Prof. David Lyon from Queens University of Canada held a key-note speech on "Assessing Surveillance". After defining surveillance in general Lyon outlined major trends of CCTV. In line with many commentators he pointed out that the future of CCTV is digital and that there is a general development towards linkages of databases. Moreover in quest of policy he stressed that there is no single solution for regulating CCTV in its new forms. Instead these new technologies ask for complex responses. Legal regulations are often of limited use, Lyon says. Also the referring on concepts such as privacy and human rights are problematic since there is a clearly trend recognizable that national security and policing may be exempt from data protection regimes. As a starting point Lyon proposes to conceptualize guidelines, best practices and education programs for personal. A large problem sees Lyon in respect to ethics.
  5. At the end of the workshop a set of policy recommendations proposed by a member of the URBANEYE working group was introduced controversially discussed.

### ***Understanding CCTV. Experts' Perspectives***

The following paragraphs summarize the discussions of the workshop's first day. In four parallel sessions the experts discussed the use of CCTV in terms of (1) risk, (2) policing, (3) trends in technology and (4) civil rights.

#### ***Risk and CCTV***

In the context of a rising sense of insecurities in our societies the aim of the panel was to discuss CCTV as a tool of risk management. The try was to get a closer insight into the decision processes within this particular context on the one and on the other hand to gain a more realistic evaluation of what CCTV can really do. A short introduction opened up the discussion.

Modern societies demonstrate a growing concern for uncertainty, fear and risk. Throughout Europe video surveillance is currently seen as one very useful instrument to remedy various risks in all kinds of urban and institutional settings. But local and social

contexts of hazardous situations are often neglected within the decision making process of strategies. Evaluations of CCTV therefore often have shown ambivalent results. It cannot be taken for granted that dangerous situations, hazards or crimes, will be avoided by the employment of the measure. In fact the safety promise of a camera's eye can turn out to be a risk itself as certain forms of social control and solidly action could be displaced by the use of the technology.

Moreover the employment of CCTV is often less transparent and accountable to the public than it should be. But risk management implies a balance between the level of socially accepted risks and the benefits of a decision to manage these. In democratic societies setting this level of socially acceptable risk is not possible without public participation. This makes the public acceptance often part of a risk strategy. Even though the perception of CCTV seems to be quite positive towards the benefits of its employment, realistic evaluations contest the validity of this as intentions are often not clearly defined and perceptible.

The following issues were addressed and discussed:

**Strategies of risk management and CCTV:** In which contexts is CCTV deployed as technology of risk management? How do different stakeholders in risk management value CCTV?

- The risks to be managed by CCTV are danger, feelings of insecurity, crime and the fear of crime. Moreover, an important purpose of CCTV is to revitalise and "reclaim" declining urban spaces.

**Efficiency of CCTV:** How effective is CCTV? What are the costs of CCTV?

- The lack of comparable data is a problem for the evaluation of installed CCTV systems.

**The risks of CCTV:** What are the social costs of it? What risks implies human mediation of technology? How effective is risk management in terms of ensuring quality of life and guaranteeing basic rights?

- CCTV might also cause risks. The geographical, tactical or methodological displacement or crime might, for instance, become a problem. A loss of motivation and moral courage by the individual citizen in monitored places is another potential risk of CCTV. Social instruments of control might become displaced by an allegedly "technological fix". Moreover, it could happen that self-control decreases and thus needs to be permanently enforced by instruments of control. The reduction of frontline policing and remote policing pose risks to the crucial police-society-relations. Trust and confidence in the work of police may decrease, and a general culture of suspicion could emerge. Risks to privacy are certainly another issue. To conclude, all technological innovations have caused risks due to a dynamic that is hardly controllable.

**Improvement of risk management:** How can we contribute to the design of safety solutions which are in line with local social context? Are there urban situations where CCTV as a risk management tool can not be replaced? Is there scope for citizen-friendly risk-management and surveillance?

- Standardisation could improve the risk management, e.g. in terms of evaluation. But no evaluation standards exist. However, the Campell collaboration ([www.campbellcollaboration.org](http://www.campbellcollaboration.org)) at least suggests some standards and guidelines.

### ***CCTV and Policing***

The deployment of video surveillance cameras has become an innovation in a broad range of policing activities: the usage of surveillance images as evidence in court; documentation of interrogation procedures; covert surveillance in criminal investigations, monitoring of traffic flows for both management and control purposes; temporary and mobile observation of crowds at demonstrations and mass events to deter and detect public order offences; and last but not least the permanent operation of open street CCTV for combating street crime. Moreover, video surveillance is a common mean in private initiatives for self-protection and outsourced security services. These become increasingly integrated with public policing either by the provision of images as evidence or by the social or technical connection of individual systems that generate visual information.

CCTV is seen as a useful instrument for investigative assistance, evidence gathering, ensuring police procedures, efficient deployment of the scarce resource police, and finally proactive crime prevention. However, as the rationales of policing shape the form and function of visual surveillance technologies, the utilisation of such technologies by law enforcement agencies and private security services might have an impact on their own rationales, organisations and practices as well. Thus, advanced surveillance technologies may contribute to an unanticipated or even unintended transformation of policing.

**Modes of operation:** For what purposes do the police use CCTV and how?

- Police use of CCTV throughout Europe is characterised by wide variations. Public area systems are, for instance, controlled by the state police forces in some nations while predominantly controlled by local authorities in other nations. The legal and political contexts differ. Police forces may use CCTV either in a more proactive way while others prefer a reactive use. Thus, any form of regulation needs to take account of particular national context.
- move towards digitalisation poses problems in forms of downloading information, i.e. the compression of image data which reduces quality

**Change of police practices:** In what ways does CCTV affect policing practices? How is discretion of police officers affected under the gaze of surveillance cameras?

- The move from analogue systems towards digitalisation poses problems for crime investigation and criminal procedure in particular when it comes to downloading the information. Then the sheer data quantity and the reduction in footage quality because of image data compression might hinder criminal justice.
- In contrast to the emphasis on crime prevention, a trend is the shift to post-incident activity based on retrospective searching.
- Another trend is that problems of information overload are answered by mobile CCTV units which strategically target hot spots.
- The British experience shows that training of operators is often very inadequate and it is difficult to ensure that compliance with Code of Practice is monitored and enforced. This is not only a problem for privacy issues but also for criminal justice as evidence might get lost or devalued when, for instance, footage is not adequately archived.

**Change of police organisation:** What does the introduction of CCTV mean for deployment strategies, staff structures and the public presence of police? How are command chains and hierarchies and decision-making affected by space transcending visual surveillance technologies?

**Blurring of boundaries:** How dependent do the police become on private interests if relying on or linking with non-public CCTV infrastructures?

- The increasing integration of CCTV systems in the context of public-private-partnerships is a serious challenge for privacy issues, in particular when it goes out of the state's hands

#### **Miscellaneous**

- As a point with general European relevance it was highlighted, that the lesson of the United Kingdom is that regulation would be best in place before the rapid expansion of CCTV.

#### ***CCTV and the future: Emerging technical and organisational trends***

As video surveillance has become a routine feature of urban landscapes, we are seeing the camera's surveillance capacity enhanced through the exploitation of digital technologies. Increasingly we are seeing cameras coupled to computers to utilize the image recognition potential of newly developed algorithms. In the UK we have seen applications that include automatic license plate recognition; automatic facial recognition, behavioural and incident recognition.

With the progress of network architectures systems do become increasingly integrated. In some contexts monitoring is centralised as a reaction towards the substantial costs of observation by staff. Moreover, wireless applications and broadband data transfer enhance the mobility and flexibility of camera deployment. Digital recording and new data compression methods increase storage capacity and reduce efforts to be spent on retrospective searching of footage.

On the other hand cryptography and intelligent image processing provide new means against the manipulation or abuse of personal data. For instance, watermarking and encryption of video signatures might certify the content integrity, or limited image data such as only those of people involved in specific actions might be transmitted.

In the context of these emergent developments in the workshop we are interested in examining, in the European context, how these new technologies are likely to be developed and deployed. The workshop will, therefore, explore three key themes:

**Trends in the technology:** Where is the technology now? Where will it be in the next five years and in the next to ten years? What are the technological prospects for algorithmic surveillance, the standardisation and integration of systems or new means of data protection?

- The future is digital at least for the larger systems found in railway stations etc.
- The digitalisation is a precursor for intelligent image processing and evaluation
- CCTV will be opened up by Internet Protocol and networked cameras. This means an increase in access to cameras, an increase in the mobility of data and the use of handheld applications. Moreover, it poses new threats by an increase in the vulnerability of image data storage and the integrity of data.
- With the advent of digitalisation not the cameras are critical but the databases do become. Their content, the circle of persons and agencies who have access and algorithms for the retrieval of data is crucial.

**Trends in commercially available products:** What systems are available now? What systems are likely to be available in the future? Where do the commercial companies see the expanding markets?

- Facial recognition will not be operational in the open streets but in specific and controlled environments, e.g. for access control at airports, at casinos etc.
- In broader contexts behavioural recognition might become more important as the demand for automated alarms or scene evaluation increases because of information overload and staff costs.

**Implications of these trends:** What are the implications for public and private policing of an increasing integration of systems and the use of automated systems? How adequate is

data protection legislation for dealing with new developments? Are there policy strategies to enforce the development?

- It poses new threats by an increase in the vulnerability of image data storage, the integrity of data.
- New possibilities for data protection arise by so-called privacy enhancing technologies (PET) such as encryption of footage, an electronically guaranteed four-eye-principle, automatic protocols of camera use, blinding out of particular field of vision by so-called privacy zones etc.
- CCTV is not only a matter of the rules but of controlling mechanisms such as inspections, licensing and transparency.

### ***Civil Rights***

Critics argue that CCTV is as a threat to civil rights and democratic values. For instance, its disciplining potential is seen as a threat to privacy and autonomy. Non-criminals could be forced to change their daily routines and modify their behaviour according to certain norms determined by the practice of video surveillance. Others warn that free access to public spaces might be affected by the employment of CCTV. Moreover, it is argued that – in face of the blurring of boundaries between public and private space – the distribution of power between public authorities and private security services is transforming and thus, the power to monitor people. New forms of policing and the expansion of potential applications for CCTV as for example automated license plate recognition raise the question how the growth of surveillance technologies in general and CCTV in particular can be regulated in accordance to achieved civil rights standards. With respect to their protection not only the actual state of video surveillance has to be taken into account. Also the future technological development that likely opens new forms of data exchange, might require new pro-active regulations regarding the collecting, storing and transmitting of images and information.

At the moment these concerns are addressed by different strategies, e.g. duties for the public registration of systems or the notification of surveillance. Whether these instruments are sufficient not only for today but also for tomorrow shall be discussed in the workshop.

**Defining the threats:** What civil and human rights are concerned by the employment of CCTV? Who are the stakeholders in the field (industries, business communities, NGOs, lawmakers, administrations, etc.)

- Not the cameras are the problem but the processing of personal data.
- It was contested whether CCTV affects the social behaviour of non-criminal citizens and whether anticipatory conformity that could undermine the democratic basis of our societies is thus to be feared.

**Modes of regulation:** What forms of regulation do exist (legal terms, ethical codes, etc.)? What is the purpose, what is the final effect of them: limitation or legal authorisation of CCTV? How and by whom can legal frameworks be enforced? Do we need a sort of experimental regulation in order to cope with the technological development of the security sector?

- For an evaluation of CCTV from a civil rights perspective the guiding principles are autonomy, privacy, and informational self-determination.
- Moreover, a clear definition of public, private and semi-public space is necessary for an evaluation as clear regulations for these types of spaces exist.
- When assessing CCTV from a civil rights perspective it is important to balance different interests (and rights). This is a particular critical issue in the case of workplace surveillance and labour law.

**Lacks of regulation:** What issues need further regulations, what type of regulation could be envisaged for the future development of CCTV technology? On what level should the regulations be decided (European level, national level)?

- Increased awareness for the developments is needed by stakeholders, and a European consensus on the regulation of CCTV is desirable.

**Alternative forms of regulation:** Are other forms than legal frameworks necessary to regulate CCTV accurately in terms of civil rights? If yes, what should be done to convince practitioners of the necessity of regulation? Are there models, e.g. data protection through technology?

- A common vision of the experts was no surveillance of public space by private organisation. (A comment by a British participant was that the realisation of this vision would be impossible in the United Kingdom. As a better vision accountable management was proposed.)
- In public space CCTV-free zones should exist which allow to avoid the gaze of the cameras.

### ***Towards policy recommendations***

By assessing the political impacts of video surveillance and formulating policy recommendations for suitable employment and management of CCTV the idea is to help decision-making processes at various levels. Communal and regional bodies shall be assisted in deciding on the suitability of the installation of costly CCTV networks to tackle crime and urban violence. National governments and the European Union ought to be helped to develop directive principles for the employment of CCTV in order to guarantee both the safety and the freedom of their citizens. For the final discussion a



member of the URBANEYE working group presented a set of policy recommendation. Eight issues were pointed out and finally discussed.

### **1. Training**

- All operators will require professional accreditation of 6 months duration. It will involve written or legal and competency-based assessment
- It will be illegal by the year 2008 to operate a CCTV system unless accredited.

### **2. Organisation**

- CCTV managers must be professionally accredited
- They should be made legally responsible for compliance with human rights, data protection and associated codes

Discussion: Here, it was mentioned that there is already a high turnover of operators. In the UK monitoring costs are at a crucial state! Moreover, a six months operator training is seen as too long. One also should distinguish the training efforts between small and big systems. Another expert mentioned that one week training is sufficient, but an accountable management is most important.

### **3. Technology**

- All digital systems must undergo a privacy security audit which demonstrates how privacy enhancing technologies have been incorporated into the system.

### **4. Licensing**

- All systems must be licensed by the newly formed video surveillance licensing agency.

### **5. Registration**

- Initial Registration will cost 500+ Euro and 300 Euro thereafter.
- Licensing fee will pay for auditing and inspection.

Discussion:

It was added that the regulation of CCTV demands definitions: What is a CCTV system since the borders between private and public space are more and more blurring. Here again one has to distinguish between small and big systems. Some systems need to be licensed, others should only be notified.

Privacy should maintain as a pillar of assessing the utility. In terms of access to data bases it needs to balance state security and privacy rights. But from a policing perspective access rights are crucial. It stays to question where the limits are. Exceptions should only be allowed in extreme cases. They could be possible by court decisions. Another participant pointed out in this context that access rights shall be a benefit and should not infringe rights of other data subjects.

## 6. Evaluation

- Routine and random Inspection/Evaluation to ensure
- Human rights complaints
- Data protection
- Fitness for purpose

## 7. Transparency

- Subject access rights must be guaranteed and audited if visual images are linked to named individuals on databases
- Subjects must be informed of their inclusion and have a right to access their information

## 8. Scope

- There should be a presumption against video surveillance in public and semi-public space
- It must be justified in relation to appropriateness and the available alternatives
- In specific places (intimate publicly accessible places) the concept of a surveillance-free zone should be implemented.

### ***Final Discussion***

It was said, that breach of this will require special and exceptional authorisation. Furthermore, there should be a big knowledge exchange between technology developers and other stakeholders in order to check and consider other PET options.

It was pointed out that many of the recommendations, e.g. transparency, are already implemented in the European Data Protection Directive and video surveillance is to be considered to fall under its scope.

When something becomes evidence should it become subject of other rules than CCTV data protection? If a crime is identified all data should be handed over to the police and are then subject of police act rules. But today every powerful police force in Britain is equipped with systems linked to several data bases (insurance, intelligence etc.). Therefore it needs control of powerful systems by stronger rules.

It also has to be questions what are the sanctions and consequences of violating rules.

## 4 Conclusions and policy implications

For more than 40 years we witness the proliferation of video surveillance systems in public and private, but publicly accessible spaces throughout Europe. Driven by socio-economic transformation and technological progress the process of diffusion accelerated since the late 1970s. However, the rise of CCTV became a policy issue only since the 1990s as police forces or local authorities in a growing number of European nations utilised cameras for the permanent and intense surveillance of public urban areas in an attempt to control crime. The debate is focusing on how to balance public safety and national security on the one hand and individual privacy on the other.

### 4.1 CCTV: A European issue?

Given the mobility of both citizens and their data between member states of the Council of Europe and within the Common Market, the issue is meanwhile not only discussed among local or national policy-makers: As image data might fall under the scope of European legal instruments, several European organisations and stakeholders have addressed the rise of CCTV in recent years. These legal instruments are:

- the Council of Europe's Convention on Human Rights and Fundamental Freedoms, in particular Article 8 (the right to privacy),
- the Council's Convention No. 108/1981 on the Automated Processing of Personal Data,
- the Data Protection Directive 95/46/EC of the European Union,
- and the Charta of Fundamental Rights of the European Union, in particular Article 7 (right to privacy) and Article 8 (protection of personal data).

In winter 1997/98 the Manchester-based Omega Foundation issued an interim report on technologies of political control to the Scientific and Technological Options Assessment panel (STOA) of the European Parliament (Wright 1998). The report highlights the dramatic changes in the art of visual surveillance by the increasing capacity to store and process images, and therefore recommends to develop common and consistent codes of practices for CCTV systems, explicit criteria for who should be targeted for surveillance and how collected data should be handled:

Two follow-up reports for the STOA again considered the impacts of video surveillance. A report on crowd control technologies warns that to fulfil the desire for an effective deployment of CCTV "would mean putting the whole of society under continuous surveillance which would be assuming a continuing benign level of political stability which rarely exist in the long term, not even in Europe." The report, however, mentions that intelligent CCTV systems could play a powerful role in "preventing public disorder occurring at fixed locations [...] where there are inevitably considerable public safety

considerations" (Omega Foundation 2000: viii). Another report on prison technologies even suggests that the "European Union should be seen as a democratic leader in video surveillance," and the "European Parliament should ensure urgently that a debate takes place on the introduction of videosurveillance within Member States, as much within as outside jails." (Mampaey/Renaud 2000: 51)

Perhaps in response to such recommendations members of the European Parliament announced to bring the issue on the agenda of committees and the plenary. Jo Leinen, for instance, then socialist member of the European Parliament and its Commission on Constitutional Affairs noted in 2001: "When travelling, people are filmed by video devices in their host countries and thus, their fundamental rights are infringed." Thus Leinen demanded CCTV to be a "top issue". Moreover, he criticised that it had not been on the agenda when discussing the European Charter of Fundamental Rights proclaimed by the European Council in December 2000 in Nice (Frankfurter Rundschau, 26.1.2001).

However, the first European organisation to address the rise of video surveillance was the Council of Europe as being committed to the protection of human rights in its 43 member states. In December 2000 the Council launched an expert report on (video) surveillance written by Giovanni Buttarelli, the Secretary General of the Italian Data Protection Authority. He reminded of the fear "that modern society may inadvertently tend to replace or supplement control with the incitement to self-control and the repression of impulses". Thus he suggested to consider "the extent to which surveillance causes a breach of privacy", and to evaluate "the effects resulting from the widespread use of surveillance as regards citizens' freedom of movement and behaviour."

Also at the Council of Europe an inter-party group of parliamentarians took action in the Parliamentary Assembly of the Council in March 2001. Ten MPs from the Czech Republic, Finland, Germany, Sweden and Switzerland presented their "Motion for a recommendation on video surveillance of public areas". They argued that the Parliamentary Assembly should recommend that the Council of Ministers call upon the member states to initiate the assessment of video surveillance, create provisions of law counteracting its uncontrolled spread, guarantee its transparent and democratic use and define the ways in which this kind of data is to be recorded, stored and used. (Doc. 9008 of the Parliamentary Assembly). Almost the same motion (Doc. 9869) was presented again in July 2003. A report is currently under preparation in the Committee on Legal Affairs and Human Rights.

At the European Union, the Article 29 Working Party, an independent advisory body on data protection and privacy adopted an "Opinion on the processing of personal data by means of video surveillance" in February 2004. This document was meant to draw "attention to the wide scope of criteria for the assessment of lawfulness and appropriateness" that are relevant when applying the European Data Protection Directive to CCTV (Article 29 Data Protection Working Party 2004: 5).

However, just as these initiatives show the demand to evaluate CCTV from a general viewpoint, they indicate the complexity of the task. Although the operation of a CCTV system might fall under the scope of European legal instruments, it is contingent on the context, purpose and technological details of deployment if it actually does, and if yes, which legal instruments are relevant. The European Data Protection Directive, for instance, does only cover first pillar activities and thus explicitly excludes all kinds of data processing in the context of public safety, national security and criminal justice. These fields are covered by the Convention on Automated Processing of Personal Data but the collection of image data by a CCTV system does not necessarily entail an "automated processing". Moreover, the meaning of the crucial terms "personal data", "processing" or "privacy" is contested, as well as the relevance of other fundamental freedoms such as the freedom of movement, assembly or communication. At present international courts only provide rudimentary guidance if and under what conditions these terms and concepts can be applied to video surveillance.

Having made these introductory remarks, we will now review our main findings in order to discuss their implications for both policy and research.

#### **4.2 Comparison: Common trends and national differences**

As we have shown CCTV has become an essential part of urban life across Europe. Surveillance cameras monitor banks, petrol stations, chain stores, transportation centres, public and private office buildings, shopping malls, universities, schools, hospitals, museums, sports arenas, residential areas, etc. In our survey of more than 1,400 publicly accessible locations in six capital cities we found in summer 2002 nearly one third of all premises and institutions operating a CCTV system. This figure is certainly only a "snapshot" and all evidence collected since then suggest that the extent of technologically mediated visual surveillance is growing continuously. The choice to be not caught on camera is becoming increasingly limited.

However, the extent of CCTV differs from country to country. Our findings suggest that its diffusion (and to some degree its technological sophistication) in semi-public space is most advanced in Britain, where we found 40% of the studied publicly accessible locations under surveillance. The extent of CCTV is least developed in Austria, where in 18% of these locations cameras were in operation. Nonetheless, the mere existence of a CCTV system in semi-public space is determined by the institutional rather than the national context: While religious centres, cemeteries, and educational institutions are most unlikely to be under surveillance, typical locations of CCTV are places of transit such as metro systems, train stations or airports. Moreover, the operation of a CCTV system is common at national government buildings, embassies, money institutions, museums, hospitals and petrol stations. Thus urban dwellers cannot avoid being videoed

during ordinary but often indispensable daily routines such as travelling by public transport or drawing cash money.

In contrast to the gradual variations in the diffusion of CCTV in semi-public spaces, it is the extent of permanent and intense surveillance of the open streets that differs most significantly across Europe: For Britain it is estimated that around 40,000 cameras monitor public areas in more than 500 cities. In France around 300 towns are reported to operate more or less extensive CCTV networks monitoring public areas, and in the Netherlands one fifth of the municipalities run a system. In contrast, open street CCTV is only in operation in around 20 German cities, and in Denmark no such system exists. Moreover, extensive surveillance and large networks with more than 50 cameras are reported for cities in Britain, France, Hungary, Italy or Monaco, it is the surveillance of limited but strategic locations (in particular the vicinity of main railway stations) that it is the model in Austria, Germany, Norway or Spain.

Having said this, it becomes clear that the rise of CCTV, though propelled by common structural factors that are at work across Europe, is highly contingent on national and local contexts.

In all studied countries policy makers, institutional stakeholders and private entrepreneurs are engaged in a quest for new directions of managerial practices and social control. Among the common structural factors behind the proliferation of video surveillance are "rational" strategies of risk management that favour allegedly inexpensive "technological fixes" and the privatisation of risk. Moreover, emergent paradigms of crime control that emphasise prevention and a decentralised reliance on citizens to mobilise the law and to control themselves and others drive the diffusion of video surveillance. Last but not least the exchange of ideas and experiences within the context of European police co-operation impel the adoption of open street CCTV as instrument of policing.

Nonetheless, the degree to which these ideas and practices have gained ground in the individual countries differ significantly as well as the types of risk that are addressed with priority or the extent to which CCTV is accepted as a saviour. Thus, the deployment of CCTV is often discussed in the context of terrorism or urban unrest, for example, in Britain and to some degree in Spain or Germany. In contrary, it is the context of tunnel safety in which CCTV mainly discussed in mountainous countries such as Austria and Norway. Surely, also in these countries the focus of debate shifted in the aftermath of September 11.

In particular in discourses on open street CCTV, "street crime" and the "reclamation of declining town centres" are common topics found in almost all countries. However, the extent to which these topics mobilise public and political support differs notably. Interestingly, the countries where open street CCTV was found most widespread and accepted, i.e. Britain and Hungary, are the countries which have undergone the most dramatic socio-economic changes during recent decades as a result of Thatcherism

respectively post-socialist transformation. Thus, one might assume that the crisis of social order lead to a "culture of suspicion" that propelled the rise of open street CCTV; and as economic restructuring is picking up pace in nations with traditionally strong welfare states, we found open street CCTV also rising in countries as Germany, France and perhaps Austria. If this "culture of suspicion", as consequence of social crisis, is promoted by an extraordinary increase in crime, decreasing social cohesion or the general loss of accustomed orientation (or all together), remains a question for further research.

But even if a general culture of suspicion and "rational" risk management provides a fertile ground for the extension of CCTV, this may be shaped by cultural attitudes, historical experiences, organisational interests and certainly legal regulations and institutional frameworks. Different notions and expectations of privacy – in terms of cultural attitudes or legal provisions – might limit or permit the diffusion of CCTV in particular spaces. In Britain, for example, the right to privacy was traditionally understood (and was without any national legal basis until the Human Rights Act 2000) in terms of locations rather than persons: While "the home is the castle" there was "no right to privacy in the public". Thus it might come as no surprise that open street CCTV is most advanced in Britain. In contrast, in Germany the right to informational self-determination as derived from the German quasi-constitution, develops a concept of informational privacy, i.e. the freedom to reveal or hide personal data. As CCTV, if meant to collect personal data, is seen in the German context as infringements of a constitutional right per se, its installation in semi-public, such as railway stations or public transport, and public areas caused controversial debate. Also in other countries the deployment of surveillance cameras in public areas is among the most contested fields. In Denmark, for example, a specific law prohibits the targeting of public space by private cameras. However, we found legal provisions also preparing the extension of CCTV when legalising certain practices. In Norway, for instance, the explicit regulation of CCTV by the Personal Data Act seems to have stopped any subsequent debate. Though semi-public spaces in Oslo were found very likely to be under surveillance, people in Oslo were hardly found in opposition of CCTV.

Moreover, it is interesting that open street CCTV is most advanced in countries where the majority of systems are operated by local authorities but supported by a clear and developed policy of the central government, as, for example, in Britain, France and the Netherlands. It seems that surveillance by local, limited government is favoured. Perhaps local government is believed to be more accountable to the people than, for instance, a "distant" German police force which is responsible to the state government. An additional factor contributing to the very different levels of CCTV's diffusion in the open streets might be the reluctance of the police themselves to adopt open street CCTV because of inner-organisational resistance. In Germany, for example, the officers of criminal investigation branches are very supportive of open street CCTV, while a major trade union of policemen representing also the views of common beat officers and civil

employees is rather sceptical, probably because of worries about potential staff reductions.

However, the strongest conclusion we can reach is how little we know that would permit a detailed comparison contrasting European countries, functional areas or local settings. Thus further research is needed to study and understand the filters that shape the diffusion of CCTV as a technology of new surveillance.

But despite all these complex national differences and our uncertainties about how the diffusion of CCTV is shaped in general or in certain types of urban space in particular, we found some common characteristics and trends that we consider worth to mention.

First, the reality of CCTV is dominated by small, technologically rather simple and isolated systems in all studied countries. Its use has become widely accepted and normal. Taking into account that one third of all premises on European capitals high streets the hypothesis of Stephan Graham that CCTV has become the "fifth utility" of urban infrastructure seems to be justified (Graham 1999). As a number of writers have pointed out, many of the programmes of practical action which flow from strategies of "risk management" are shifted "*beyond* the state apparatus, to the organisations, institutions and individuals in civil society" (Garland, 1996). One may argue that the increasing number of small and isolated systems follow the common emphasis on individual responsibility for managing risk as one can hear it today throughout all parts of the political spectrum.

Second, there is tendency that in particular larger systems are being linked to each other by technical and social means, and thus larger "surveillance webs" are emerging. Not only indoor alarm systems of banks or museums get connected to private security services or the police, but also CCTV systems of railway stations or shopping malls. Formal and informal exchange of information connects different networks and as a consequence the boundaries between the public and private sphere becomes blurred. During our research we found almost two third of the systems with 10 or more cameras being integrated with other agencies by either dedicated communication links or the technical capability to transfer image data. In his study on the operation of CCTV across a whole domain of an English city McCahill (2002) argues that in the end not only a separate and discrete system has to be taken into consideration in order to understand the impact of visual surveillance systems, but at least for the British case meanwhile a whole "surveillance web." McCahill argues: "A combination of public and private CCTV systems linked with pager systems, panic alarms, radio links and mobile and fixed telephone networks is facilitating the development of surveillance webs which weave unseen through the fabric of contemporary cities." (McCahill 2002: 99) In Germany, for example, the police in the city of Hannover might use the around 200 cameras of the public transportation corporation Üstra. In railway stations, the private security company of the German Railway Company and the Federal Border Police exchange information in



the context of a so-called security partnership. Moreover, some politicians already considered the integration of private security cameras into a comprehensive "architecture of security". New developments in network technologies and the rise of so-called internet protocol cameras might accelerate this trend. In contrast to cameras and signage of a single system, "surveillance webs" are invisible. Thus they remain among a serious challenge for regulation. They, in particular, resist in the end demands for transparency. The cross-linking might multiply the purposes of systems and in the end it might become impossible for citizens to discern the real intentions of a surveillance measure.

The third major common trend is digitization of systems. The CCTV industry trade magazine, *CCTV Today*, titled in July 2001 "the future is digital". For the development of video surveillance this trend represents a paradigmatic shift. Not the camera but the invisible technology behind becomes the core of this new generation of CCTV surveillance. As Norris has argued, at digital video systems the image itself becomes the source of information and can be used for all kinds of purposes; from whether forecast to anticipation of traffic congestion or acts of crime and terrorism. However, digitization also means a change in practices. For examples, it might cause a loss of information as it often entails a compression of information. But it also enables retrospective as well as forward-looking automated searching when more and more algorithms allow the combination of information in order to predict the future. From a social point of view digitization has certainly fundamental implication of the future of social control. Its tremendous enforcement of surveillance capacity clearly asks for regulation and also will need further research. However, the digitization process also carries some possibilities to regulate CCTV by technology itself. In terms of privacy the shift allows to integrate certain privacy enhancing technologies and also other regulating technologies that prevent misuses.

### **4.3 Purposes, organisation and practices of CCTV surveillance**

Though debates on CCTV concentrate on crime, surveillance cameras are deployed for a variety of risk management purposes such as tunnel safety, the prevention and detection of traffic congestion, fire or accidents, and deviant behaviour such as unauthorised access, so-called "anti-social behaviour" and crime. Thus the collection of personal data is very likely to occur but not all CCTV systems do necessarily collect personal data.

Although the improvement of services (16%) and the fire safety (5%) were also among the publicly declared purposes of CCTV systems that were found in our 2002 survey, most CCTV systems (86%) were declared to be tools to prevent and detect theft. Many (39%) were also declared to serve the prevention and detection of violence against persons. However, the potential of expandable mutability characterises the use of CCTV because – once in place – other forms of use might occur. CCTV systems that were

installed to deter shop theft might become instruments to monitor the performance of employees or toys that fulfil voyeuristic purposes.

Our data suggest that the majority of CCTV systems aim to prevent deviant behaviour by symbolic but more or less incompetent deterrence because cameras are highly visible but those under surveillance are hardly visible for an observer due to irregular monitoring, informational overkill or even the deployment of dummy cameras. However, more than three fourth (78%) of the CCTV systems do record footage on a permanent basis.

Though the dominant practice is symbolic deterrence rather than active surveillance suggest that the control potential of CCTV in general is often overestimated, technologically mediated visual surveillance is an opaque phenomenon: CCTV surveillance in one out of two systems (51%) found in our survey was not notified by signage. While in Norway only 20% of the systems were lacking signage, in Hungary and Austria more than 80% were doing so. And even if CCTV surveillance was notified the identity of the responsible data controller and contact information was often missing. Moreover, in 43% of the cases our request to answer the simple question on who is the owner of the system was rejected. The secrecy of CCTV was worst in Austria, Germany and Hungary where in between 55% and 87% of the cases an interview was rejected, while the rate in the two Scandinavian countries and Britain was only around one fourth. However, most managers of larger systems – in particular those of (semi)public bodies such as public transport, museums or open street CCTV systems – were responding to our survey, and thus indicated their commitment to a certain degree of transparency.

Ours and others research in CCTV control rooms suggest that the sensory limitations of the video screens and the distance between the observers and the observed encourage the application of categorical suspicion based on a narrow range of readily observable traits rather than the application of behavioural suspicion. Thus operators might tend to target whole categories of the public seen as likely criminals or nuisances. However, if this occurs and which consequences it entails varies according to structural factors such as the fit between mandated activities and available time, the relationship of CCTV operators and those in the field, and the function of monitored space. In particular the growth of CCTV in semi-private spaces might bring with it an increasing emphasis on exclusion as dominant strategy of social control, for which we have found examples in different settings in at least three countries.

To conclude, one cannot make any generalisations about the extent, nature and impact of CCTV surveillance from the mere existence of a system. CCTV systems are deployed for various purposes, have diverse levels of technological sophistication, operating procedures and staffing policies. The operation and impacts have to be understood as the outcome of the interplay between technological, organisational and cultural factors. The combination of all these different factors determines if a system is fit for its purpose

or if it becomes more or less ineffective due to “surveillance slack” and “linkage blindness”, as represented, for example, by bored and unmotivated operators or conflicts between the control room personnel and on-site staff. But the combination of these factors might also cause a transgression of mandated activities and an abuse of power.

#### **4.4 Policy implications and recommendations**

The use of video surveillance is representing a peculiar social technique with exceptional consequences which barely seem to be met by common data protection laws. In contrast to many other forms of data processing that require the informed consent of the data subject, video surveillance allows to collect, store and process personal data covertly and without interaction between the controller and the data subject. The only way to opt out of this form of data processing is to avoid locations under surveillance. Clearly the right of the data subjects to object to being filmed as laid down in Article 14 of the European Data Protection Directive cannot be applied effectively. Moreover, the more or less opaque character of the collection, storage and processing of personal data by the means of video surveillance threatens to undermine the ability of the observed to make an informed and autonomous decision on the acceptance or avoidance of such data processing by video surveillance. The mere existence of a camera – even if notified – does hardly tell the relevant details. Whether it is a dummy camera, a system not collecting personal data, a single camera system without storage capacity, or a camera of a large and sophisticated system additionally linked to third parties remains unknown to the citizens.

Thus, we see the relation of information that the observers hold on the observed and vice versa – which in fact is an asymmetric relation of power – as crucial for the systematic assessment and regulation of video surveillance.

Having said this, we would like to point out the following issues.

- Since data controllers cannot assume informed consent of the data subjects per se the employment of video surveillance in public and publicly accessible space should only be allowed for a limited set of clearly defined purposes. Art. 6b and Art. 7 of Directive 95/46/EC should help to prevent both the exhaustive spread of video surveillance systems and the expandable mutability that characterises their use at the moment.
- As an additional safeguard against the exhaustive spread and disproportional deployment of CCTV a system of registration and licensing should be considered for at least larger networks of visual surveillance. Registration should help citizens and public authorities to review the current extent of surveillance and its development over time.

- To inform a licensing system and the assessment of the proportionality of video surveillance systems, professional but independent evaluations of their effectiveness in terms of declared purposes and other possible impacts and consequences, especially with respect to the basic prerequisites of open and democratic societies are necessary.
- Pictures in a way seem to be more open to interpretation by the individual controller. Therefore the regulatory approach must also address problems of this "openness" as these also seem to undermine the principle of purpose specification. In order to ensure both compliance with Art. 6b and Art. 7 of the Directive and the proportionality of video surveillance (which is a socio-technical rather than simply a technical device) the operators of video surveillance systems, in particular control room staff, should be guided, trained and managed in an appropriate manner. This may serve as to limit the possible discriminating use and misleading conclusions drawn from picture materials.
- An appropriate guidance should be provided by a common and consistent set of codes of practices. Regular inspections or audits should ensure the implementation of these codes of practices and guarantee an adequate complaints system. CCTV managers should be professionally accredited and made legally responsible for compliance with the relevant legal provisions.
- Moreover, the implementation of technical safeguards, known as privacy enhancing technologies, such as encryption of data, the four-eye-principle, automated protocols or so-called "privacy zones" should be considered.
- Transparency should be enhanced as a balance weight against the asymmetric relationship of vision between the data controllers and the data subjects. In line with Art. 10 and Art. 11 data subjects should not only be informed about the operation of video surveillance, the identity of the data controller and its purpose but also about core features of systems such as storage of footage or possible linkages to third parties.
- Given the definition of personal data as "any information relating to an identified or identifiable natural person" by Art. 2 it should be clarified if and how the oral exchange of information drawn from the processing of image data is touched by the Directive. Such practices are evident for technical and social networks of video surveillance systems and their operators for instance within police-private-partnerships. If not addressed, this problem could easily lead to an arbitrary practice of networks informally exchanging information referring to identifiable persons.

Finally, we wish to address the following issues going beyond the scope of the Directive but which, however, are closely related to it.

- Privatisation and securitisation are not just catchword. Although the Directive does not apply to video surveillance carried out by public crime control and national

security authorities, we observe – as mentioned above – that the lines between the work and the specific tasks of these public bodies and other private data controllers where the Directive is wholly applicable are increasingly blurring. Thus, these hybrid areas of surveillance activities need increased attention and eventually regulation. We recommend therefore to promote an understanding of the Data Protection Directive which strengthens its decisive meaning and impact as the common aquis also within the remaining third and second pillar of the European Union. The current discussion of a growing "European space of freedom, security and rule of law" (Constitutional Convention draft papers) should consequently be enriched by stressing the legal achievements of the EU in its first pillar activities.

## 5 References

- Article 29 Data Protection Working Party (2004): *Opinion 4/2004 on the processing of personal data by means of video surveillance*, 11750/02/EN, WP 89, adopted on 11 February, 2004: [www.europa.eu.int/comm/internal\\_market/privacy/docs/wpdocs/2004/wp89\\_en.pdf](http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp89_en.pdf).
- Armitage, Rachel (2002): *To CCTV or not to CCTV? A review of current research into the effectiveness of CCTV systems in reducing crime*, London: NACRO <http://www.nacro.org.uk/data/briefings/nacro-2002062800-csps.pdf>.
- Beck, U. (1986): *Risikogesellschaft. Auf dem Weg in eine andere Moderne*, Frankfurt/Main, Suhrkamp.
- Buttarelli, Giovanni (2000): *Protection of personal data with regard to surveillance. Report for the Project Group in Data Protection of the Council of Europe*: [www.legal.coe.int/dataprotection/Default.asp?fd=reports&fn=RapButtarelliE.htm](http://www.legal.coe.int/dataprotection/Default.asp?fd=reports&fn=RapButtarelliE.htm).
- Coleman, C. and C. Norris (2001): *Introducing criminology*, Cullompton: Willan Publishing.
- Danish Crime Prevention Council (2000): *CCTV surveillance. Between prevention and privacy. A booklet for debate from The Danish Crime Prevention Council on attitudes to and experience with CCTV surveillance*, Copenhagen.
- Davis, M. (1990): *City of quartz. Excavating the future of Los Angeles*, London: Verso.
- Ditton, Jason (1999): "Public support for town centre CCTV schemes: myth or reality?" in: *Surveillance, Closed-Circuit Television and social control*, ed. by Clive Norris, Jade Moran & Gary Armstrong, Aldershot: Ashgate, pp. 221-228.
- Ditton, Jason & Emma Short (1999): "Yes, it works, no, it doesn't. Comparing the effects of open-street CCTV in two adjacent Scottish town centres", in: *Surveillance of public space. CCTV, street lightning and crime prevention* (Crime Prevention Studies Vol. 10), ed. by Kate Painter & Nick Tilley, New York. Criminal Justice Press, pp. 201-223.
- Ditton, Jason (2000): "Crime and the city. Public attitudes towards open-street CCTV in Glasgow", in: *British Journal of Criminology*, Vol. 40, pp. 92-709.
- European Opinion Research Group (2003): *Special Eurobarometer 196. Data Protection*, [http://europa.eu.int/comm/public\\_opinion/archives/ebs/ebs\\_196\\_data\\_protection.pdf](http://europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_data_protection.pdf).
- Flight, Sander & Yvonne van Heerwaarden (2003): *Evaluatie cameratoezicht Amsterdam. Effectmeting August Albéplein, Belgiëplein en Kraaiennest*, Amsterdam: DSP Groep. <http://www.amsterdam.nl/contents/pages/00002790/eindrapportdspevaluatie.pdf>.
- Foucault, Michel (1977): *Discipline and punish. The birth of the prison*, London: Penguin.
- Fyfe, N. R. and J. Bannister (1996). "City watching. Closed circuit television surveillance in public spaces", in: *Area* 28(1), pp. 37-46.
- Gandy, O. (1989). "The surveillance society. Information, technology and bureaucratic social control", in: *Journal of Communication* 39(3), pp. 61-76.

- Garland, D. (1996): "The Limits of the Sovereign State. Strategies of Crime Control in Contemporary Society", in: *The British Journal of Criminology*, Vol. 36, No. 4, Autumn, pp. 445-471.
- Graham, Stephan (1999). "Towards the fifth utility? On the extension and normalisation of CCTV", in: *Surveillance, Closed Circuit Television and social control*, ed. by C. Norris, J. Moran and G. Armstrong. Aldershot, Ashgate, pp. 89-112.
- Hempel, Leon & Eric Töpfer (2001): *Inception Report*, Urbaneye working paper No. 1, [www.urbaneye.net/results/ue\\_wp1.pdf](http://www.urbaneye.net/results/ue_wp1.pdf).
- Hölscher, Michael (2003): "Sicherheitsgefühl und Überwachung. Eine empirische Studie zu Einstellungen der Bürger zur Videoüberwachung und ihrer Erklärung", in: *Kriminologisches Journal*, No. 35, pp. 42-56.
- Klauser, Francisco (2004a): "Die Entwicklung einer 'Sicherheitsstadt', in: *digma. Zeitschrift für Datenschutz und Informationssicherheit*, 2004/1, pp. 24-29.
- Klauser, Francisco (2004b): "Die Veränderung der urbanen Territorialität infolge der Videoüberwachung des öffentlichen Raums. Ein Vergleich unterschiedlicher räumlicher Funktionsweisen der Videoüberwachung", in: *Geographica Helvetica. Schweizerische Zeitschrift für Geographie*, No. 2/2004, pp. 106-118.
- Klocke, Gabriele & Group of Scholars (2001): "Das Hintertürchen des Nichtwissens. Was Regensburger BürgerInnen über die Videoüberwachung in ihrer Stadt wissen und denken", in: *Bürgerrechte & Polizei / CILIP*, No. 69, 2/2001, <http://www.cilip.de/ausgabe/69/video.htm>.
- Koskela, Hille (1999): "'Safe to be afraid': Video surveillance and women's perception of safety", in: *Fear, control and space. Geographies of gender, fear of violence and video surveillance*, ed. by Hille Koskela, Helsinki: University of Helsinki.
- Koskela, Hille & Martti Tuominen (2003): "*Kakspiipunen juttu*" *Tutkimus helsinkiläisten suhtautumisesta kameravalvontaan*, Helsinki: Jultkaisija Utgivare Publisher (City of Helsinki Urban Facts Research Series 2003/3).
- Lyon, D. (1994): *The electronic eye. The rise of surveillance society*. Minneapolis, University of Minnesota Press.
- Lyon, D. (2001): *Surveillance society. Monitoring everyday life*. Buckingham, Philadelphia, Open University Press.
- Lyon, D. (2002): "Surveillance studies. Understanding visibility, mobility and the phenetic fix", in: *Surveillance & Society*, No. 1, Vol. 1, pp.1-7.
- Lyon, D. (ed.) (2003). *Surveillance as social sorting. Privacy, risk, and digital discrimination*. New York, Routledge.
- Mampaey, Luc and Renaud, Jean-Philippe (2000): *Prison technologies. (An appraisal for technologies for political control). Final study*, Working Document PE 289 666, STOA programme of the European Parliament, Luxembourg
- McCahill, M. (1999). „Beyond Foucault. Towards a contemporary theory of surveillance“, in: *Surveillance, Closed Circuit Television and social control*, ed. by C. Norris, J. Moran and G. Armstrong. Aldershot, Ashgate, pp. 41-65.

- McCahill, Mike (2002): *The Surveillance Web. The rise of visual surveillance in an English city*, Cullompton: Willan Publishing.
- Norris, Clive & Gary Armstrong (1999): *The maximum surveillance society. The rise of CCTV*, Oxford: Berg.
- Norris, Clive, Jade Moran & Gary Armstrong (1999): *Surveillance, Closed Circuit Television and social control*, Aldershot: Ashgate.
- Norris, C. (2003): "From personal to digital. CCTV, the panopticon, and the technological mediation of suspicion and social control", in: *Surveillance as social sorting. Privacy, risk and digital discrimination*, ed. by D. Lyon. London, New York, Routledge: 249-281.
- Omega Foundation (2000): *Crowd control technologies. (An appraisal for technologies for political control). Final study*, Working Document PE 168 394, STOA programme of the European Parliament, Luxembourg
- Painter, K. and N. Tilley, Eds. (1999). *Surveillance of public space. CCTV, street lightning and crime prevention*. Crime Prevention Studies. Monsey, New York, Criminal Justice Press.
- Pawson, Ray und Nick Tilley (1997): *Realistic evaluation*, London: Sage.
- Phillips, Coretta (1999): "A review of CCTV evaluations. Crime reduction effects and attitudes towards its use", in: *Surveillance of public space. CCTV, street lightning and crime prevention*, ed. by K. Painter and N. Tilley. Monsey, New York: Criminal Justice Press, pp. 123-156.
- Reuband, Karl-Heinz (2001): "Videoüberwachung. Was die Bürger von der Überwachung halten", in: *Neue Kriminalpolitik*, Vol. 13, No. 2, pp. 5-9
- Reeve, A. (1999). „*The panopticism of shopping. CCTV and leisure consumption*“, in: *Surveillance, Closed Circuit Television and social control*. C. Norris, J. Moran and G. Armstrong. Aldershot, Ashgate: 69-87.
- Short, Emma und Jason Ditton (1998): Seen and now heard. Talking to the targets of open street CCTV, in: *British Journal of Criminology*, Vol. 38, No. 3, pp. 404-429.
- Welsh, Brendon C. & David P. Farrington (2002): *Crime prevention effects of CCTV. A systematic review*, Home Office Research Study 252, August 2002, <http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf>.
- Wright, Steve (1998): *An appraisal of technologies of political control (consultation version)*. Luxembourg: STOA programme of the European Parliament.