Parliamentary Assembly
Assemblée parlementaire
https://pace.coe.int

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Doc. 11478
04 January 2008

Video surveillance of public areas

Report
Committee on Legal Affairs and Human Rights
Rapporteur: Mr Yuri SHARANDIN, Russian Federation

Summary

Video surveillance is an increasingly widespread phenomenon in public places. Rapidly evolving technology and a growing feeling of insecurity in the general population have gradually increased public acceptance of video surveillance as a useful tool in the context of crime prevention and detection.

Although the use of new technologies is increasingly efficient in protecting public order and security in Europe, the fact remains that video surveillance may impinge on human rights.

Legal, procedural and technical guarantees must be in place in order to enable video surveillance to be carried out in full compliance with the European Convention on Human Rights, as interpreted by the European Court of Human Rights.

The report notes the existence of certain technical means which can limit the impingement on human rights during video surveillance. Member states should systematically make use of these technical possibilities.

The report concludes that member states should consider adopting unified signs (pictograms) relating to video surveillance and considers that the Council of Europe should continue its work on the issue of video surveillance in the future.

Contents **Page**

A. Draft resolution

1. The Parliamentary Assembly notes that video surveillance is an increasingly widespread phenomenon in public places.

2. Rapidly evolving technology and a growing feeling of insecurity in the general population have gradually increased public acceptance of video surveillance as a useful tool in the context of crime prevention and detection.

3. The Assembly notes that the use of video surveillance as such is no longer called into question. Modern technology makes it possible to carry out high quality video surveillance (CCTV) without intruding into the private lives of citizens. The spectre of "Big Brother" no longer seems to inspire the fears it used to.

4. Indeed, video surveillance has found its place in daily life in a great number of cities in Council of Europe member states and has, on several occasions, proved to be an effective tool. The Assembly is aware of the positive role played by video surveillance systems in resolving criminal cases before the courts, for example in the case of the bomb attacks of 21 July 2005 in the London Underground, and also more recently in helping to prevent car bombing attempts in London and Glasgow.

5. Whilst welcoming the increasingly efficient use of new technologies to protect public order and security in Europe, the Assembly remains concerned by the fact that video surveillance may impinge on human rights such as the protection of privacy and data protection. In the light of, in particular, Article 8 of the European Convention on Human Rights (the Convention) which guarantees the right to respect for private life, video surveillance should remain an exceptional measure prescribed by law and only in cases where it is necessary in a democratic society to protect the interests of national security or public safety, or for the prevention or detection of disorder or crime.

6. The collection, treatment and conservation of data obtained by video surveillance must be regulated by law in full compliance with the Convention, as interpreted by the European Court of Human Rights.

7. In this context, the Assembly recalls that several national and European legal instruments provide minimum guarantees for the protection of individual rights with regard to video surveillance and that these should be respected and fully implemented in all member states.

8. The Assembly is concerned by certain far-reaching aspects of seamless supervision offered by the technical possibilities inherent in CCTV systems. The use of such technical possibilities should be strictly regulated.

9. Considering that the existing equipment for video surveillance and software allows the use of a very strong (up to 30-50 times) zoom and resolution of the image, the Assembly strongly encourages Council of Europe member states to adopt legislation laying down limits for the installation of such equipment with reference to each specific place.

10. The Assembly also stresses that existing CCTV equipment and software allows for "privacy zones" (windows of apartments, etc.) to be automatically excluded from video observation. The Assembly considers that this practice serves not only to protect the private life of individuals but also to protect the employees of CCTV centres from seeing anything which lies outside their competence. In Council of Europe member states, such "privacy zones" should be defined by law and excluded from video surveillance by using such specialised software.

11. Images from CCTV cameras are currently stored in a digital format and the software allows the image to be encoded. This excludes access by third parties to the information stored and protects it from unauthorised access and modification. Encoding can render the information valid for criminal investigations. In Council of Europe member states, the practice of encoding of video data images should be imposed by law.

12. Everyone living in or passing through the range of video surveillance has the right to know about it and to gain access to all the images of himself. Council of Europe member states should protect this right by law.

13. Furthermore, the Assembly stresses that co-operation between government bodies and non-governmental entities is vital in the sphere of video surveillance and encourages member states to enhance this co-operation. The governments are obliged to co-operate with NGOs which should have the right to control the volume and form of video surveillance.

14. The Assembly is concerned to note that national laws are far from homogeneous in this area and therefore formally calls on the Council of Europe member states:

14.1. to apply the guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance adopted by the Council of Europe's European Committee on Legal Cooperation (CDCJ) in May 2003 and to ensure that they are adhered to as systematically as possible;

14.2. to lay down by law technical restrictions for installation limits of the equipment with reference to each place under surveillance;

14.3. to define "privacy zones" to be excluded from video surveillance by law, imposing the use of special software;

14.4. to provide in their legislation for the practice of encoding video data images;

14.5. to provide access to a legal remedy in cases of alleged abuse related to video surveillance.

15. The Assembly finds it necessary that a unified sign, and an accompanying unified written notice, are adopted as soon as possible and used by the member states.

16. Finally, the Assembly – considering that further reflection is needed in the field of video surveillance – encourages the European Commission for Democracy through Law (the Venice Commission) to develop further its consideration of this subject in order to lay down guidelines to balance the public interests involved against the human rights and freedoms of individuals in a democratic society.

17. Taking into consideration current events and the constant technical progress in the field of video surveillance, the Assembly underlines the need to continue the work on the issue of video surveillance in the future.

B. Draft recommendation

1. The Parliamentary Assembly refers to its Resolution … (2008) on video surveillance of public areas.

2. Considering the work undertaken under the authority of the Committee of Ministers, and especially of the European Committee on Legal Co-operation (CDCJ), which led to the elaboration of the guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance of 2003 – and convinced that this subject merits more thorough analysis – the Assembly recommends that the Committee of Ministers organise a conference on the subject of video surveillance. Such a conference should involve, *inter alia*, persons possessing expertise on video surveillance, both in the public and private sectors, as well as representatives of civil society.

C. Explanatory memorandum, by Mr Yuri Sharandin

1. Introduction

1. In September 2003, the Committee on Legal Affairs and Human Rights had referred to it a motion for a recommendation that had been presented by Mr Bindig and others[1] calling for a precise assessment of the implications of video surveillance and its impact on crime rates in member states.

2. On 27 April 2004, the Committee on Legal Affairs and Human Rights appointed Ms Maria Eduarda Azevedo (Portugal, EPP/CD) its rapporteur on this issue to succeed Mr Ignasi Guardans, who was leaving the Parliamentary Assembly.

3. On 23 May 2005, the Committee on Legal Affairs and Human Rights appointed Mr Yuri Sharandin (Russian Federation, EDG) its rapporteur on this issue.

4. The term video surveillance refers to the technical and electronic systems that enable the remote monitoring of property and people using video cameras (closed circuit television, or CCTV). This technology was developed in response to the growing public feeling of insecurity in a context of rising crime and the authorities' desire to boost crime prevention and crack down on offenders. The present situation of resurgent terrorism in Europe can only lead to a further increase in the public's feeling of insecurity and is scarcely calculated to foster a reversal of the trend.

5. The issue raised is bound to lead to conflicting arguments and comments, which is to be expected whenever a technological innovation affects individual freedoms and privacy. Some people will obviously cite the need for strict respect for the individual's rights, dignity and private life in order to condemn the potential misuse of this technology and the Utopia of total security, even raising the Orwellian spectre of Big Brother. Others, on the other hand, will advocate the necessary limitation of these individual rights and freedoms, claiming that this is in the general public interest and that there is a need to ensure public security and protect public order.

6. In the end, the committee will have to answer the specific question of what social benefits video surveillance provides. We need to establish whether the use of this technology meets the needs of our societies and whether the laws and regulations currently in force guarantee a fair balance between respect for human rights and public freedoms and the limitation of these rights on the basis of the proportionality principle.

7. The Council of Europe has been active on this issue, especially by adopting guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (report adopted by the European Committee on Legal Co-operation (CDCJ) in May 2003).

8. In order to prepare this report, the Committee on Legal Affairs and Human Rights held an exchange of views with Mr Paul Wille, Belgian Senator and member of the Assembly on 3 October 2006. Mr Wille gave details of the legislative process concerning video surveillance in Belgium, where draft legislation was currently being debated.

9. Following this exchange of views, the committee decided to request the opinion of the European Commission for Democracy through Law (Venice Commission) on "the extent to which video surveillance is compatible with basic human rights". The committee raised in particular the question of defining at what moment does normal observation of people in public places (by authorities, by institutions, by citizens) become a legal and political problem, in particular because of the use of observation cameras, sometimes in a network.

10. The Venice Commission adopted its opinion at its 70th plenary session (16-17 March 2007) on the basis of comments by Mr Pieter Van Dijk, Mr Vojin Dimitrijevic and Mr Giovanni Buttarelli.[2]

11. This opinion has been completed by a second one on video surveillance by private operators in the public and private spheres and by public authorities in the private sphere and human rights protection, adopted at its 71st plenary session (1-2 June 2007).[3]

---

1. Doc. 9869.
2. Opinion on video surveillance in public places by public authorities and the protection of human rights ("Venice Commission Opinion No. 1"), CDL-AD(2007)014; available at www.venice.coe.int/docs/2007/CDL-AD(2007)014-e.asp.

2. A widespread technology

12. The first video surveillance systems appeared in the 1950s and their development was boosted by the invention in 1956 of the video cassette. Their use by private individuals became widespread in the following three decades as a means of monitoring private premises, whether or not they were accessible to the public, and made it possible to check on the movements of people in the vicinity of, at the entrances to, and inside buildings, such as luxury-goods shops, shopping centres, banks, residential buildings, etc. Their use was extended to the surveillance of workplaces and leisure, cultural and sports centres. Today, citizens are fully familiar with these surveillance systems, which are all the more accepted as they respond to the demands of a public anxious to preserve its security and peace of mind.

13. It is thought that the United Kingdom alone – ironically, Orwell's homeland – has 4 million surveillance cameras, thus accounting for 10% of those in use worldwide. This figure has quadrupled in three years. Some 85% of the United Kingdom's local authorities are equipped with video surveillance networks. It is estimated that about 10 million video cassettes are recorded each day. A British citizen is said to be filmed five hundred times a week on average and a Londoner three hundred times a day!

14. A study carried out in the context of the European Commission's "Urbaneye" project[4] and published in the spring of 2004 reveals that 90% of British people questioned were in favour of these systems (compared with 48% of the Germans and 24% of the Austrians questioned). Some 47% of Londoners, compared with 4% of the inhabitants of Vienna, think that video surveillance protects them from crime.

15. Like surveys or opinion polls, which reveal differences of perception according to the country concerned, the question of the degree to which these systems are accepted or tolerated has a highly cultural dimension. In addition, it is not certain that the population has the same tolerance of video surveillance when it is employed in a private place as it does in the case of a public place.

16. A survey carried out in France in 1996 revealed that social acceptability varies according to the application. Only 9% of those questioned considered the presence of cameras in car parks and shops a breach of their privacy, whereas 51% thought that the broadcasting, without their knowledge, of a picture taken in a public place constituted a serious invasion of privacy. By contrast, the majority of the population in the United Kingdom are prepared to make more concessions regarding fundamental rights in order to improve security.

17. From the 1980s onwards, and especially in the 1990s, video surveillance ceased to be limited to private or semiprivate areas and began to become widespread in public places. More and more public bodies are resorting to the installation of video surveillance systems to monitor public places and buildings: administrative buildings, national defence installations, prisons, museums, schools, universities, stations, airports and hospitals, as well as national borders.

18. However, it is mainly in the area of public transport and the regulation of road traffic that video surveillance systems have undergone rapid development. The Brussels ring road has been equipped with cameras since 1993. Cameras are also installed in the main tunnels through the Alps and in tunnels in Spain and the Scandinavian countries. However, while video surveillance makes it possible to regulate traffic and ensure the security of main roads and major junctions it also enables drivers who commit traffic violations to be identified. In London, where cameras began to be installed in 1974, the establishment in 2003 of a scheme for charging motorists to enter the central area was accompanied by the installation of some 700 cameras for checking vehicle number plates.

19. Several countries have also installed surveillance systems on their public transport: 5 000 cameras monitor all the tracks, platforms and corridors in the Paris metro. The underground railway networks of Amsterdam, Stockholm, Bucharest, Brussels and Vienna, in particular, are also equipped with video surveillance. In Switzerland, the Federal Railways installed a video surveillance system in 2003 to monitor their railway installations and trains. Frankfurt airport is equipped with 2 000 cameras. More than 40 German stations also have video surveillance systems.

---

3. Opinion on video surveillance by private operators in the public and private spheres and by public authorities in the private sphere and human rights protection, CDL-AD(2007)027; available at www.venice.coe.int/docs/2007/CDL-AD(2007)027-e.asp. The rapporteur considers that this does not fall within the mandate of this report but that this issue will need further consider- ation by the Assembly.

4. This comparative study co-ordinated by the Zentrum Technik und Gesellschaft (Technische Universität Berlin) on the use of video surveillance in places accessible to the public in Europe was carried out between September 2001 and February 2004 in the following countries: Austria, Denmark, Germany, Hungary, Norway, Spain and the United Kingdom, including in their capital cities.

20. In France, the decision taken in 2003 to install a system of digital surveillance cameras at the entrances and in the immediate vicinity of about 90 secondary schools in the Paris suburbs caused an outcry. Yet more than 100 schools in the United Kingdom are equipped with a system, as are the schools in three Danish towns. The universities of Cologne, Edinburgh, Dundee, Cardiff, Porto and Eindhoven, for example, also possess video surveillance facilities.

21. Video surveillance is also likely to be employed in courtrooms, since the United Kingdom is considering installing cameras in some of the country's appeal courts.

3. Does video surveillance help to make combating crime more effective?

22. The installation of surveillance cameras in public places is the public authorities' response to the citizens' feeling of insecurity and their demand for better crime prevention and law enforcement. The proliferation of these systems meets security requirements, such as combating the upsurge in theft, physical violence, vandalism, burglaries, drug dealing, prostitution, etc.

23. It is clear that video surveillance mainly has law enforcement applications and serves as a means of visually identifying individuals.

24. Is technology the key to the security of public places? The conclusions of most studies on the impact of video surveillance on crime are in fact conflicting.

25. It is true that numerous examples show that video surveillance is to some extent effective in combating crime, and a surveillance camera can enable criminals and minor offenders to be identified and arrested.

26. The use of CCTV has been impressively effective in helping to apprehend the persons who attempted a car bomb attack in central London at the end of June 2007. Previously, video surveillance had proved itself to be of outmost importance in establishing responsibility for a terrorist attack, since CCTV video featuring the six men accused of plotting the bomb in the London subway in July 2005 (in which 25 people died and 700 were injured) had been used in their trial. Also, on 21 July 2005, the police revealed an attempt to detonate bombs in the London subway by four other terrorist bombers. The four men were arrested after videos of the suspects were released.

27. Everyone will also remember the tragic assassination of Anna Lindh, the Swedish Foreign Minister, in a Stockholm department store, in September 2003. Video surveillance made it possible to identify and arrest her murderer. A more recent crime case is the murder of Joe Van Holsbeeck in Brussels in April 2006. The 17-year-old was stabbed to death at the busy Brussels Central train station. This case highlighted the police use of video surveillance cameras to identify and reconstruct the offenders' movements before and after Holsbeeck was attacked.

28. A number of figures from a French survey conducted in 1998 show that in the case of bank branches with video surveillance 50% of thieves are identified and arrested within two years. On the Paris metro, 83% of incidents are detected by surveillance cameras and the number of people taken in for questioning has increased by 36%. Similarly, in a British town of 10 000 inhabitants, where six cameras monitor the town centre, the number of offences fell from 137 in 1991 to 37 in 1992. In Monaco, which has cameras everywhere, the crime rate is three times lower than that of the neighbouring French *département* of Alpes-Maritimes.

29. The Venice Commission also notes that, considering that technology has dramatically improved, "in comparison with human observance, video surveillance is by far more effective under several accounts". But the Venice Commission also concludes that video surveillance might be more intrusive with regard to human rights than human observation.[5]This is the consequence, in particular, of the possibility of storage and easy electronic transmission of the images, which does not exist in the case of human observation.

30. Other studies show that video surveillance is ineffective in combating crime. For example, video surveillance in the Paris metro has been no help at all in the fight against terrorism. The municipality of Levallois-Perret is a noteworthy example of the ineffectiveness of video surveillance: its streets are monitored more than almost any others in France but there has nevertheless been a significant increase in crime.

---

5. See Venice Commission Opinion No. 1, paragraphs 17 and 21. Some examples are mentioned like, *inter alia*, night vision, zoom and automatic tracking capacities, voice recognition and even intelligent systems able to detect fake beards or moustaches.

31. It is therefore not possible to draw any definitive conclusions regarding the effectiveness of such a system. In fact, one expert on the subject, Professor Jason Ditton, the Director of the Scottish Centre for Criminology in Glasgow, maintains there is nothing to prove that video surveillance has any impact on the crime rate. The studies carried out in the 1990s by the Scottish Centre for Criminology tend to play down the impact of video surveillance on the crime rate and the citizens' security reflex.[6]

32. At the 23rd International Conference of Privacy and Data Protection Commissioners in 2001, mention was made of the automatic facial recognition system that forms part of a video surveillance scheme[7] set up in the London Borough of Newham. The town has been equipped since 1998 with a closed circuit video surveillance system coupled with a technology that enables the police to be alerted when a person contained in its files passes in front of one of these cameras. When the system was installed in 1997, 75% of the 250 000 inhabitants were living in fear of being attacked. This figure was reduced to 67% in 1998 and subsequently continued to decline. In early 1998, a survey conducted by the local authorities revealed that 67% of those questioned were in favour of the system. This figure even rose to 93% by the end of 1999 (the questionnaire took care to ask the respondents to express their opinion by taking into consideration the possible consequences of the system on human rights, civil rights and privacy). The face comparison system is based on police files on persons already convicted for crimes and involved in criminal activities in the last twelve weeks. Individual files are examined by the police at least every twelve weeks. The images of the faces scanned are not preserved unless they correspond "without any doubt" to a person on file in the database. The public is informed about all the areas covered by the system. The result is a 34% reduction in crime since 1997.

33. The same technology linking a video surveillance system to a facial recognition system was also tried out in the United States by the City of Tampa in Florida in January 2001 on the occasion of the Super Bowl (the final of the American football championship). This experiment was criticised by the American Civil Liberties Union (ACLU), which concluded in a study[8] that this technology was not reliable enough to justify its installation, which threatens privacy in a number of ways. This system made it possible on several occasions to indicate the presence of the terrorist Carlos in a crowd, but he was in fact at that time in France serving a prison sentence. This raises the question of whether this automatic facial recognition system is sufficiently reliable.

4. Public security or social control?

34. For several years now, people have been speaking out against the dangers of using security as a pretext. Video surveillance puts a new complexion on the problem of striking a necessary balance between the prevention of breaches of public order and the exercise of individual freedoms, freedom of movement and the right to privacy. The widespread routine use of video surveillance makes it possible to monitor an ever broader population without people always being aware of this. In its very principle, if security is set against freedom, video surveillance poses a risk of interference with the citizens' daily lives and of violation of their right to respect for their privacy. There is also the problem of the conditions for gathering, using and disseminating the information and data collected on individuals (in the form of pictures and sound) through video surveillance. Video surveillance enables people to be identified directly (facial recognition) or indirectly (via their vehicle, their clothing, etc.). It makes it possible to multiply the amount of information available on their behaviour, movements and activities. The gathering of such data permits the full-scale tracking of individuals.

---

6. The conclusions of these studies show that the crime rate declined in the year following the introduction of video surveillance in Glasgow (570 000 inhabi- tants) in November 1994 but did so much less than in other towns and cities not equipped with video surveillance. This finding could be put down more to the overall trend towards a reduction in crime in the country as a whole. On the basis of adjusted data, the crime rate in Glasgow had in fact risen by 9%. At the same time, opinion polls showed that video surveillance had no impact on the feeling of insecurity in the population. In 1995, the 32 video surveillance cam- eras enabled 209 arrests to be made in Glasgow, which corresponded to just 5% of the crimes committed in the city centre that year. On the other hand, after the installation in 1992 of 12 cameras in Airdrie (36 000 inhabitants), there was a decline in the crime rate and a rise in the number of people identified.

7. Such a system permits:
   individuals to be identified by comparing their faces with those stored in a database;
   the identity of individuals to be verified by comparing a declared identity with those linked to the faces stored;
   individuals to be monitored by enabling the image of an individual to be followed in video footage;
   individuals to be kept under surveillance by enabling the identity of a per- son to be established in real time video footage from a list of faces.

8. "Drawing a blank: the failure of facial recognition technology in Tampa, Florida", January 2002.

35. According to two Belgian lawyers who have written a report on video surveillance in Belgium, video surveillance threatens privacy in two ways: where it takes place secretly, it results in the gleaning of information on certain forms of behaviour or attitudes that the person concerned might not have wanted to be disclosed; when its presence is known to the persons concerned, video surveillance encourages them to adopt certain forms of behaviour or attitudes that differ to a greater or lesser extent from those they would actually demonstrate in the absence of surveillance. This latter finding must be related to the phenomenon of the displacement of crime from the streets and neighbourhoods equipped with cameras to those without them. To some extent, this calls into question the effectiveness of video surveillance in combating crime.

36. The Venice Commission comes to the same conclusion that "in principle, before entering a public sphere, a person will adjust his/her appearance and demeanour to the possibility of being seen by others". However, it recalls that even if the degree of privacy necessarily decreases in a public area, it does not mean that individuals are deprived "of their rights and freedoms including those related to their own private sphere and images".[9]

37. Cameras are becoming better and better and can monitor a 360-degree field of vision. Equipped with zoom lenses, they are, for example, capable of reading a newspaper from a distance of more than 100 metres or a vehicle number plate from 300 metres. Some contain detectors that issue a warning in the case of an incident or indications of abnormality in their field of vision, such as suspect smoke or a sudden movement. It has been claimed that the cameras in London's Oxford Street were able to identify the size of the shoes of the passers-by.

38. The technologies of video surveillance systems are converging more and more with other technologies, which is giving rise to new concerns about the protection of privacy and data. These technologies include, *inter alia*, sound recordings, high capacity wireless information networks used for the transmission of images, automatic facial recognition systems integrated into computer databases that can identify people or follow their movements, and devices that make it possible to "see" through clothes and walls, such as thermal recognition or infrared systems. The transmission of images via the public telephone networks can enable images and sound to be received worldwide across national borders.

39. The recorded information can be precisely analysed. It is possible to install fully automatic identification systems based on zoom and digital imaging technologies and linked to other digital databases. For example, in the British City of Bradford video surveillance is linked to an automatic number plate recognition system (ANPR) that enables data to be provided automatically for the police files at the rate of 3 000 registration numbers recorded per hour by each camera. The Home Office is considering extending the use of this technology and equipping police cars with it.

40. Technological developments in the field of video surveillance – ANPR, automatic facial recognition, etc. – raise even more questions. How and by means of what procedure is the database of suspects fed with information? What is a suspect? When is a suspect deleted from the database? Indeed, as rightly pointed out by the Venice Commission, "in general, it is not the monitoring as such which is the most problematic, but the recording of the data and their processing …".[10]In this context, the protection of personal data is concerned, and the Venice Commission recalls that it falls within the scope of private life within the meaning of Article 8, ECHR.[11]

41. The use of video surveillance cameras also poses a risk of discrimination. Studies have shown that staff responsible for viewing the CCTV screens tend to focus more readily on certain population categories. The automatic facial recognition process, which is based on the image of the face, increases even more the fear of serious abuses connected with an individual's physiognomy or signs of poverty or deviant behaviour.

42. Video surveillance may give rise to numerous abuses that are always hard to prevent. Surveillance systems can easily be used for other than their declared purposes, for example the introduction of a social control: cameras installed in a shop to prevent theft are often used to monitor the staff; and department stores use them to produce studies on consumer behaviour. On an even more serious level, video surveillance can be a means of imposing political controls: the cameras installed at Beijing's Tiananmen Square served to identify and arrest regime opponents in June 1989.

---

9. See Venice Commission Opinion No. 1, paragraph 25. In this respect, the Venice Commission rightly underlines that the European Court of Human Rights has held in its case *P.G. and J.H. v. the United Kingdom* of 6 February 2001 that there is a zone of interaction of a person with others, even in a pub- lic context, which may fall within the scope of "private life".
10. See Venice Commission Opinion No. 1, paragraph 29.
11. Ibid., paragraph 41.

A specific case: webcams

43. Finally, it is also necessary to consider the use of video surveillance in public places by private individuals rather than public bodies to keep an eye on public areas. The proliferation of live images shot by video cameras (webcams) and made available on the Internet poses similar problems concerning respect for privacy and conformity with the data protection regulations. However, the problem arises not only with regard to the processing of the data but above all to their dissemination and to an individual's right to his or her own image and the protection of his or her personality.

44. Webcams are generally installed in public places, often at tourist spots. They can either provide a fixed image or change their viewing angle, and they can be equipped with a zoom lens. The images they shoot can be accessed worldwide and are processed, recorded, printed and transmitted without being subject to any controls. In order that these cameras are used in conformity with the law, they should be installed and configured in such a way that no one can be identified; otherwise, those filmed must consent to being filmed. But, is this always the case? Depending on the position and the technical quality of the camera, it is possible to recognise a person filmed, and that person is unaware that he or she is being filmed and that the pictures will be received all over the world via the Internet.

45. It is therefore not certain that existing data protection and privacy legislation will be sufficient to guarantee human rights in these specific cases.

5. Preventing abuses by laying down a legal framework based on respect for a number of principles

46. European citizens are not totally defenceless against these potential or actual abuses. There are legal instruments available. At the national level, first of all, very few states have opted to introduce specific legislation concerning the electronic surveillance of private or public places. On the other hand, a number of member states have enacted legal and constitutional provisions that are applicable in this area, especially provisions that guarantee respect for privacy and human dignity or others concerning the protection of personal data. At the supranational level, several international instruments, in particular those of the Council of Europe, cover the same areas. However, the question arises whether these instruments are sufficient to provide proper protection for the citizens who are "watched".

5.1. Instruments of European law

47. Video surveillance activities involving the processing of personal data fall within the scope of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, of 1981 (ETS No. 108).[12]

48. The convention is the first binding international instrument aimed at strengthening the legal protection of individuals against the unauthorised use of automatic processing of personal data concerning them. It applies to both the public and the private sectors and establishes a number of general principles concerning the collection, processing and communication of personal data via the new information technologies. These principles are in particular the lawful and honest collection and automatic processing of data that are recorded for particular legitimate purposes and are not used for ends incompatible with these purposes or preserved beyond the period necessary. The convention prohibits the processing of "sensitive" data relating to a person's racial origin, political opinions, health, religion, sex life, criminal convictions, etc., in the absence of guarantees provided by domestic law. It also guarantees the right of the persons concerned to ascertain what information is stored on them and, if appropriate, to demand that any necessary corrections be made.

49. This convention has been completed by an Additional Protocol (ETS No. 181) regarding supervisory authorities and transborder data flow, which entered into force on 1 July 2004.

50. In order to adapt the general principles set out in the convention to the specific demands of society's various areas of activity, several additional recommendations have been adopted by the Committee of Ministers of the Council of Europe. Mention might be made of Recommendation No. R (87) 15 on the use of personal data in the police sector, Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies, and Recommendation No. R (99) 5 on the protection of privacy on the Internet.

12. See the stand of signatures and ratifications under http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=11/19/2007&CL=ENG (as of 19 November 2008, 38 member states have ratified it, and 5 have signed it).

51. There is no European Union legal instrument on video surveillance as such. The video surveillance of public places is only partially covered by Directive 95/46 of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, since this directive explicitly excludes certain video surveillance activities – the very activities that interest us here[13]– from its scope.

52. Community citizens nevertheless enjoy the guarantees provided by this directive. All the countries of the Union apart from France have transformed Directive 95/46/EC into national law. It has been supplemented by Directives 97/66/EC and 2002/58/EC on privacy and electronic communications. There is still no case law of the Court of Justice of the European Communities (ECJ) on the subject of video surveillance, but the Court recognises the application of the proportionality principle and the need for an overriding public interest to impose a restriction on a fundamental right.

5.2. Member states' legislation

53. Few countries have provisions in their law that specifically regulate the use of video surveillance, let alone video surveillance in public places. However, the member states' legal systems are not entirely without any rules in this area since legislation on the protection of privacy, the recording and use of information and personal data, the secrecy or confidentiality of sensitive information, etc., may be applied to video surveillance activities and provide a basis for citizen guarantees.

54. Spain is one of the few countries to have adopted legislation on the video surveillance of public areas. In particular, this law provides for machinery for authorising its installation by public legal entities. A high level of integration of the video surveillance systems (CCTV) with the national emergency and security services has been achieved in this country.

55. In 2006 the Integrated Centre of Safety and Security Services (Centro Integrado de Seguridad y Emergencias) was opened in Madrid. The representatives of police, first aid, fire protection and other services successfully operate under one roof at this centre. The crisis centre for emergency interventions can be deployed there in minutes.

56. The experience of Spain has shown the extreme efficiency of such centres. The integrated municipal safety system in Madrid is recognised as the best in Europe.

57. In Spain the practice of the CCTV image output on monitors accessible for the public installed for example in the underground and at railway stations is used. This system allows citizens to be involved in the process of video observation and serves as an original reminder that the situation in such places is under surveillance. In the opinion of psychologists such openness, along with the special unified signs (pictograms approved by the special law of Spain), serves to reduce the intensity and favourably influences the general conditions for crime prevention in public places under video surveillance.

58. In Belgium a new law regulating the installation and use of video surveillance cameras was proposed by Senator Stefaan Norielde in April 2006.

59. In Great Britain about 5 million CCTV cameras will be in use in the near future. It is widely known that the average citizen of London becomes the object of video surveillance 300 times a day. Some 1 060 CCTV cameras are in operation in Westminster alone.

60. In order to maximise the potential of the national video surveillance network, a National CCTV strategy project is under construction. British experts came to the conclusion that without a strategy, it is likely CCTV in public areas in the United Kingdom will remain uncoordinated, disparate, of questionable quality, less effective and poorly targeted. Furthermore, in the absence of a strategy, it is unlikely that the Treasury will agree to further public funding. This being the case, there is a danger that the current infrastructure will deteriorate and society will lose the opportunity to maximise the effectiveness of CCTV and integrate future technologies that could greatly assist policing.

61. In France, video surveillance is specifically regulated. The installation of video surveillance systems on public thoroughfares and in places or establishments open to the public is governed by the law of 21 January 1995 and the decree of 17 January 1996. The law provides that systems may only be installed in public

13. Paragraph 16: "Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this direc- tive if it is carried out for the purposes of public security, defence, national security or in the course of state activities relating to the area of criminal law or of other activities which do not come within the scope of Community law".

places for specific purposes (the protection of public buildings and installations, the control of road traffic, the detection of traffic violations and the prevention of breaches of the security of individuals and property). The installation of such systems is subject to prior authorisation. The video surveillance systems must not enable pictures to be seen of the interior of residential buildings or their entrances. The law also provides for a public right to information, for a right for individuals to access video recordings concerning them and for the destruction of recordings within a maximum period of one month (except in the case of an expedited police investigation or a judicial investigation).

62. General laws on data protection are in force in several member states either following the ratification of ETS No. 108 or the transformation of Directive 95/46/EC into national law. This is the case in Albania, Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom, as well as Azerbaijan, Bosnia and Herzegovina, Malta, Monaco, San Marino, Serbia and Montenegro, and "the former Yugoslav Republic of Macedonia", although these latter states are not parties to ETS No. 108.

63. In 33 member states, it is the constitution that establishes the fundamental principle of the right to privacy or data protection. Data protection is a basic right laid down in the Portuguese Constitution of 1976, Article 35 of which provides the citizen with very comprehensive guarantees (right of access to personal information, right to obtain and correct information, etc.).

64. In addition, a majority of member states have set up an independent regulatory and supervisory authority to ensure compliance with the principles laid down in their legislation.[14]

5.3. Case law of the European Court of Human Rights[15]

65. Video surveillance falls within the scope of Article 8 of the European Convention on Human Rights (the right to respect for private life – "Everyone has the right to respect for his private and family life, his home and his correspondence"). The Court has defined in its case law the limits to the exercise of this right, especially with regard to the extent to which the public authorities might be entitled to interfere. A public authority may only interfere with the exercise of the right to privacy if this interference is provided for by the law and constitutes a measure that, in a democratic society, is necessary for the defence of a number of legitimate objectives. In a judgment (*M.S. v. Sweden* of 27 August 1997), the Court "reiterate[d] that the protection of personal data … is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention".

66. In its *Peck v. the United Kingdom* judgment of 28 January 2003, the Court found itself required for the first time to consider the problem of an invasion of privacy by video surveillance. In the case in issue, the applicant had been filmed trying to commit suicide by a local authority's remote surveillance camera, which had led to police intervention. The pictures had been used by the town council for a press feature and on a national television channel to promote the prevention of crime, but without masking the applicant's identity. The Court ruled that the disclosure of footage filmed by a surveillance camera infringed the applicant's right to privacy without there being any relevant or sufficient reasons to justify this and held that there had been a violation of Article 8 of the Convention.

67. For the Court, "the monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life". However, video surveillance must comply with the criteria of strict conformity with the

---

14. Büro der Datenschutzkommission und des Datenschutzrates in Austria, Commission de la Protection de la vie privée in Belgium, Personal Data Protection Commission in Bulgaria, Bureau for the Protection of Personal Data in the Czech Republic, Office of the Personal Data Protection Commissioner in Cyprus, Datatilsynet in Denmark, Data Protection Inspectorate in Estonia, Office of the Data Protection Ombudsman in Finland, Commission nationale de l'informatique et des libertés in France, Der Bundesbeauftragte für den Datenschutz in Germany, Data Protection Commission in Greece, Data Protection Commissioner in Hungary, Persónuvernd in Iceland, Data Protection Commissioner in Ireland, Garante per la protezione dei dati personali in Italy, State Data Protection Inspectorate in Latvia, State Data Protection Inspectorate in Lithuania, Liechstensteinische Landesverwaltung Stabstelle für Datenschutz in Liechtenstein, Commission nationale de la protection des données in Luxembourg, the Office of the Commissioner for Data Protection in Malta, College Bescherming Persoonsgegevens in the Netherlands, Datatylsinet in Norway, Office of the General Inspector of Data Protection in Poland, Commissão Nacional de Protecção de Dados in Portugal, Commissioner for Personal Data Protection in Slovakia, Agencia de Protección de Datos in Spain, Datainspektionen in Sweden, Préposé fédéral à la protection des données in Switzerland, Information Commissioner in the United Kingdom, etc.

15. For complementary information, the rapporteur draws the attention of the reader to paragraphs 26-33 and to paragraphs 49-67 of Opinion No. 1 of the Venice Commission.

law, legitimacy and proportionality set out in Article 8, paragraph 2, of the Convention. The Court considered that "the relevant moment was viewed to an extent which far exceeded any exposure to a passer-by or to security observation … and to a degree surpassing that which the applicant could possibly have foreseen when he walked in Brentwood on 20 August 1995". Consequently, the Court concluded that there had indeed been a serious infringement of the applicant's privacy, stating that "the disclosures (of the images) were not accompanied by sufficient safeguards to prevent disclosure inconsistent with the guarantees of respect for the applicant's private life contained in Article 8".

68. It should be noted that this is not the only case of video surveillance involving the United Kingdom. In *Martin v. the United Kingdom* (Application No. 63608/00), the applicant, Janette Martin, a resident of Nottingham, complained about a breach of Articles 8 (right to respect for family life) and 14 (ban on discrimination) of the Convention with regard to the decision of her city council to place her home under video surveillance, without her knowledge, following complaints by her neighbours concerning her and her children's behaviour. The case ended in a friendly settlement.

5.4. The need to press for sufficient guarantees in the member states' domestic law

69. Given the increasing development of video surveillance technologies, it would be desirable to press for the harmonisation of member states' legislation in this area. This legislation should be clearly based on the principles and guarantees deriving from the Council of Europe's instruments, especially as regards the right to privacy and data protection.

70. In May 2003, the Council of Europe's European Committee on Legal Co-operation (CDCJ) adopted a report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (see appendix). It is important for the Parliamentary Assembly formally to call on the Council of Europe member states to apply these guiding principles and ensure that they are adhered to as systematically as possible.

71. National legislation should recognise the following minimum guarantees:

– the principle of strict compliance with the law: video surveillance may only be carried out if it is permitted by law, is justified by an overriding public or private interest and is accepted by the persons concerned;

– the principle of proportionality: video surveillance must be an appropriate and necessary means of achieving the aim pursued, namely security (and especially protection against attacks on property and/or individuals). It can only be adopted if other measures less likely to constitute an invasion of privacy prove insufficient or impracticable. A camera must be installed in such a way that it only captures images necessary for the surveillance proposed;

– the purpose or legitimacy principle: data may only be used in connection with protection against attacks on property and individuals. It cannot give rise to other uses (especially of a commercial nature). The communication of personal data recorded by a camera is prohibited in all cases apart from those provided for or authorised by the law;

– the principle of public information: the existence of a video surveillance system must be brought to the knowledge of the public; the person or body responsible for the video surveillance system must inform the persons entering into the surveillance camera's field of vision about the use of such a system by means of a written notice;

– the control principle: the persons directly concerned by the information gathered as well as the public regulatory authorities must be able to satisfy themselves that individual rights are respected by the users;

– the principle of the right of access to the data by the persons concerned: the persons concerned must be aware of the substance of the information that a file may contain about them;

– the principle of the right of the persons concerned to correct erroneous or inappropriate information;

– a right of appeal if one of the above principles is not complied with: any person concerned must be able to defend his or her rights in order to be able to check on the information relating to him or her when it is collected, processed and, if applicable, broadcast;

– a guarantee of data security: the person or body responsible for the video surveillance system must take appropriate measures to allow access to, and the preservation of, personal data in order to protect them from any unauthorised processing. The preservation and recording of data must be of limited duration.

6. Conclusions

72. Several national and European legal instruments provide minimum guarantees for the protection of individuals' rights with regard to video surveillance. According to current thinking, a European convention or a recommendation of the Committee of Ministers of the Council of Europe on video surveillance would not add very much to the existing instruments. However, as national laws are not homogeneous in this area, it is important for the Assembly formally to call on the Council of Europe member states to apply the guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance contained in the CDCJ's 2003 report and to ensure that they are adhered to as systematically as possible.

73. A unified sign (pictogram) in all member states for places under video surveillance should be adopted.

74. A unified written notice should accompany the sign (pictogram) with reference to the law.

75. The existing equipment for video surveillance (CCTV) and the software allows the use of a very strong (up to 30-50 times) zoom and resolution of the image. Council of Europe member countries should adopt legislation limiting the installation of the equipment with reference to specific places.

76. The existing CCTV equipment and the software allows for "privacy zones" (windows of apartments, etc.) to be automatically excluded from video observation. This practice serves not only to protect private life, but also to protect the employees of CCTV centres from seeing anything outside their competence. In the Council of Europe member countries "privacy zones" should by law be defined and excluded from video surveillance through the use of special software.

77. At the present time, images from CCTV cameras are stored in a digital format. The software allows the image to be encoded. Encoding excludes access of third parties to the stored information and protects it from unauthorised access and modification. It renders the information valid for criminal investigations. In Council of Europe member countries encoding of video data images should be imposed by law.

78. Everyone who is living within the range of video surveillance (CCTV) has the right to know about it. Therefore, Council of Europe member countries should guarantee this right by law.

79. Co-operation between government bodies and non-governmental entities is vital in the sphere of video surveillance.

80. In order to update its information on the subject matter, the Council of Europe should hold a conference to supplement its information on this subject; various experts could be invited:

– persons possessing expertise on video surveillance, both in the public and private sector;

– representatives of academic institutions and/or monitoring bodies that have recently carried out studies on such issues as the impact of video surveillance on crime rate and related privacy issues;

– representatives of specialist Council of Europe expert committees (CDCJ, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – T-PD);

– representatives of a national regulatory or supervisory authority for the protection of data or privacy;

– representatives of civil society (an association such as Privacy International).

Appendix – Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (2003) adopted by the European Committee on Legal Co-operation (CDCJ) at its 78th meeting (20-23 May 2003)[16]

Reporting committee: Committee on Legal Affairs and Human Rights.

Reference to committee: Doc. 9869 and Reference No. 2864 of 8 September 2003.

Draft resolution and draft recommendation unanimously adopted by the committee on 13 December 2007.

Members of the committee: Mr Dick Marty (Chairperson), Mr Erik **Jurgens**, Mr György **Frunda**, Mrs Herta Däubler-Gmelin (Vice-Chairpersons), Mr Miguel Arias, Mrs Aneliya **Atanasova**, Mr Abdülkadir **Ateş**, Mr Jaume Bartumeu Cassany, Mrs Meritxell Batet, Mrs Marie-Louise **Bemelmans-Videc**, Mrs Anna **Benaki**, Mr Luc **Van den Brande**, Mr Erol Aslan Cebeci, Mrs Pia Christmas-Møller, Mrs Ingrīda **Circene**, Mrs Alma Čolo, Mr Joe Costello (alternate: Mr Terry **Leyden**), Mrs Lydie **Err**, Mr Valeriy **Fedorov**, Mr Aniello Formisano, Mr Jean-Charles Gardetto, Mr József Gedei, Mr Valery Grebennikov, Mrs Carina Hägg, Mr Holger **Haibach**, Mrs Gultakin Hajiyeva, Mrs Karin Hakl, Mr Andres **Herkel**, Mr Serhiy **Holovaty**, Mr Michel Hunault (alternate: Mr Michel **Dreyfus-Schmidt**), Mr Rafael Huseynov, Mrs Fatme Ilyaz, Mr Kastriot Islami, Mr Željko Ivanji, Mrs Kateřina Jacques, Mr Karol Karski, Mr Hans Kaufmann, Mr András Kelemen, Mrs Kateřina Konečná, Mr Nikolay Kovalev (alternate: Mr Yuri **Sharandin**), Mr Eduard Kukan, Mrs Darja Lavtižar-Bebler, Mr Andrzej Lepper, Mrs Sabine **Leutheusser-Schnarrenberger**, Mr Humfrey **Malins**, Mr Andrija Mandić, Mr Pietro Marcenaro (alternate: Mr Andrea **Manzella**), Mr Alberto Martins (alternate: Mr Ricardo **Rodrigues**), Mr Andrew **McIntosh**, Mr Murat Mercan, Mrs Ilinka Mitreva, Mr Philippe **Monfils**, Mr João Bosco Mota Amaral, Mr Philippe **Nachbar**, Mrs Nino Nakashidzé, Mr Fritz Neugebauer, Mr Tomislav Nikolić, Mr Anastassios Papaligouras, Mr Ángel Pérez Martínez, Mr Claudio Podeschi, Mr Ivan Popescu, Mrs Maria Postoico, Mrs Marietta de **Pourbaix-Lundin**, Mr Christos **Pourgourides**, Mr John **Prescott**, Mr Jeffrey Pullicino Orlando, Mr Valeriy Pysarenko, Mrs Marie-Line **Reynaud**, Mr François Rochebloine (alternate: Mr Germinal **Peiro**), Mr Francesco Saverio Romano, Mr Paul Rowen (alternate: Mr Christopher **Chope**), Mr Armen Rustamyan (alternate: Mr Raffi **Hovannisian**), Mr Kimmo **Sasi**, Mr Ellert Schram, Mr Christoph Strässer, Mr Mihai Tudose, Mr Vasile Ioan Dănuţ **Ungureanu**, Mr Øyvind **Vaksdal**, Mr Egidijus Vareikis, Mrs Renate Wohlwend, Mr Marco Zacchera, Mr Krzysztof **Zaremba**, Mr Vladimir Zhirinovsky, Mr Miomir Žužul.

NB: The names of those members present at the meeting are printed in bold.

See 9th Sitting, 25 January 2008 (adoption of the draft resolution and draft recommendation); and Resolution 1604 and Recommendation 1830.

16. This document is available on the Council of Europe website, at the following address: www.coe.int.