



Strasbourg, 8 June 2007

Study no. 430 / 2007

CDL-AD(2007)027
Or. Engl.

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW
(VENICE COMMISSION)

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**

**Adopted by the Venice Commission
at its 71st Plenary Session
(Venice, 1-2 June 2007)**

on the basis of comments by

**Mr Pieter van DIJK (Member, Netherlands)
Mr Vojin DIMITRIJEVIC (Member, Serbia)**

I. Introduction

1. *The Venice Commission adopted at its 70th plenary session (16-17 March 2007) an “opinion on video surveillance in public places by public authorities and the protection of human rights” (CDL-AD(2007)014). This opinion was initiated by a request by the President of the Committee on Legal Affairs and Human Rights, Mr Dick Marty, in a letter, dated 10 October 2006, in which he requested the opinion of the Venice Commission on the question “The extent to which video surveillance is compatible with basic human rights” in the framework of the preparation of the report on “video surveillance at public places”.*
2. *Considering that an exclusive focus on the dangers of video surveillance activities performed by public authorities would miss the current development of video surveillance activities, the Venice Commission decided to expand its analysis to cover also video surveillance performed by private operators in the public and private spheres and video surveillance operated by public authorities in the private sphere.*
3. *Indeed, on the private level people are more and more using video surveillance supplies to keep an eye inside and outside their homes. The use of video surveillance facilities has soared over the years, whether home use like the so-called “nanny cams” or the more classical use of a camera mounted in a corner of the entrance of a house or a larger private property. Moreover, due to technological advances, declining costs of video surveillance equipment have resulted in an increase in its use among the public.*
4. *In addition, the Internet revolution has had a great impact on video surveillance. The Internet has enabled video surveillance to be instituted virtually anywhere and be watched from anywhere in the world. With satellites bouncing signals around the globe, it is now possible to watch anyone anywhere from a laptop. The “eye in the sky” has become a reality with digital streaming video, a remote system that enables people to monitor their site from anywhere in the world with Internet access, because the images are video-archived on a remote web server. The Internet and the spread of WiFi Wireless Fidelity have removed practically all boundaries for recording and viewing video pictures anywhere in the world.*
5. *The present study constitutes a further step in the Venice Commission's study of the issue of video surveillance and human rights, in which it purports to lay down guidelines for balancing public interests against human rights and freedoms of the individual in a democratic society.*
6. *Mr Pieter van Dijk and Mr Vojin Dimitrijevic were appointed as rapporteurs.*
7. *The present study, drawn up on the basis of their comments, was adopted by the Commission at its 71st Plenary Session (Venice, 1-2 June 2007).*

II. Scope of the present study

8. *The present study will focus on the observation of people by private operators in public and private areas and by public authorities in private areas by means of video surveillance tools, irrespective of the type of video tools used, whether they are connected to a network or not, and whether the data collected are registered or not. The study will confront these practices with current European Human Rights standards.*
9. *In order to determine the scope of the study, a definition will be given of the terms and concepts which will be used.*

Private operators

10. For the purposes of this study, the term “private operators” will cover individuals as well as private companies like private investigation companies, private bodies like casinos, banks or semi-public establishments, or any firm or company of the business world.

Public authorities

11. The term “public authorities” is used to mean national or local authorities in their preventing and protecting activities, among which those related to crime prosecution.

Public sphere

12. A “public area” is a place which can be, in principle, accessed by anyone freely and indiscriminately. Any person benefits freely from public areas. Public areas are governed by public law and controlled by public authorities, whose power to enforce the law and intervene are wider than within private property.

13. Examples of relevant public areas include: public parks; pedestrian streets in the city centres; outdoor public parking areas; residential neighbourhood streets; areas such as sports arenas and underground train stations.

14. Universities, hospitals, stadiums, post offices and schools are examples of “semi-public areas” to which, in principle, the rules of the public sphere apply as well.

Private sphere

15. The “private sphere” in a physical meaning is a place where access can be restricted by those who own this private sphere. Private spheres are not in principle open freely to the public and are not accessible indiscriminately. Rules governing private sphere are mainly those related to private law and more specifically to the right to privacy. The powers of public authorities over these areas are more restricted than over public areas.

16. The category of private places is not restricted to private homes, but also includes offices, shops, discos, cafes and restaurants, where the owner, user or licensee is accountable for what takes place there.

17. Universities, hospitals, stadiums, post offices and schools, which may be considered as semi-public areas, can also be considered as a private sphere in so far as the directors or managers have primary responsibility for what takes place there, while public authorities would be responsible for the prevention of disorder or crime.

18. For the purposes of this study, the private sphere will also include workplaces and the use of video surveillance in workplace premises, which raises legal issues concerning the employees’ privacy rights.

19. As regards the intimate aspect of the private sphere, this refers to the intimate aspect of a human being’s personality. It entails the right of everyone to be protected against unwarranted intrusion by government agencies, the media, any institutions or individuals. Hence, private life in the sense of, e.g. Article 8 of the European Convention on Human Rights (hereafter: ECHR), is a very broad sphere which is not easy to define; it is not limited to an “inner circle” in which the individual may live his/her own personal life. The private sphere includes the right to establish and develop relationships with other human beings, especially in the emotional field

for the development and the fulfilment of one's own personality.¹ Private life also covers the physical and moral integrity of a person, including his/her sexual life.

20. It is recalled that freedom of thought, conscience and religion fall into the sphere of private life whether under Article 18 of the International Covenant on Civil and Political Rights (hereafter: ICCPR) or by virtue of Article 9 ECHR.

Video surveillance

21. While the video surveillance system used and set up by public authorities on public places for crime prevention or crime prosecution is usually a "CCTV system" (which consists of a system of video cameras connected in a closed circuit television), video surveillance operated by private operators or by public authorities over private spheres might consist of various types of video surveillance.

22. This study will therefore cover not only the CCTV system, but also other video surveillance possibilities such as simple video cameras mounted in a corner of an entrance of a house or other private property, "nanny cams" or web-cameras.

23. The fact that video surveillance, in comparison with human observance as such, offers far broader potential and scope, and hence might be more intrusive with regard to human rights, is even more obvious here than when considering video surveillance by public authorities in public places.

III. Legal analysis

A. The international protection of privacy

24. The human right that is primarily affected by video surveillance, that is, overt and covert collection of records, images data and information on persons, is generally assumed to be the right to privacy.

25. The provisions of international human rights treaties applicable in this context, which bind all member States of the Council of Europe, are primarily contained in the ICCPR and the ECHR.

¹ European Commission of Human Rights, *X v. Iceland*, Decision of 18 May 1976, 86.87.

ECtHR, Case of *Klass and Others v. Germany*, Judgment of 6 September 1978.

ECtHR, *Leander v. Sweden*, Judgment of 26 March 1987. A summary is given by the same court in its judgment in ECtHR, *P.G. and J.H. v. the United Kingdom*, Judgment of 25 September 2001: "Private life is a broad term not susceptible to exhaustive definition. The Court has already held that elements such as gender identification, name and sexual orientation and sexual life are important elements of the personal sphere protected by Article 8 (see, for example, ECtHR, *B. v. France*, Judgment of 25 March 1992, § 63; ECtHR, *Burghartz v. Switzerland*, Judgment of 22 February 1994, § 24; ECtHR, *Dudgeon v. the United Kingdom*, Judgment of 22 October 1981, § 41; and ECtHR, *Laskey, Jaggard and Brown v. the United Kingdom*, Judgment of 19 February 1997, § 36). Article 8 also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world (see, for example, European Commission of Human Rights, *Burghartz v. Switzerland*, and ECtHR, *Friedl v. Austria*, Judgment of 31 January 1995, opinion of the Commission). It may include activities of a professional or business nature (see ECtHR, *Niemietz v. Germany*, Judgment of 16 December 1992, § 29, and ECtHR, *Halford v. the United Kingdom*, Judgment of 25 May 1997 § 44, § 56).

Article 17 ICCPR reads :

*“1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.”*

Article 8 CEDH reads :

*“1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”*

26. While international human rights bodies have been wary to define the right to privacy, the notion of privacy is very high in the set of values protected in the present European system of human rights.

27. The best approach would seem to be to take privacy as a cluster of values related to the intimate sphere of a person, which are reflected in various rights and which can only be interfered with or restricted following the general and specific principles and rules pertaining to the enjoyment of the human rights concerned.

28. Whether and how international law afford protection depends on the type of the operator of the video surveillance activity.

1. The video surveillance activity is performed by a private operator (irrespective of whether public or private areas are concerned)

29. The fact that international standards enshrined in the ICCPR and the ECHR are directed to States and their public bodies, not to individuals, could be seen as problematic.

30. However, regarding the ICCPR, one could argue that there is nothing in the wording of Article 17 CCPR that implies that the prohibition of interference applies only to State authorities. Its paragraph 1 is impersonal and the protection of law against "interference and attacks" implies the right of the victim to rely on protection provided by law (i.e. by the State).

31. A State not providing such protection against arbitrary and unlawful interference may be held to be in violation of its treaty commitments, irrespective of the fact that the interference in private life was committed by a private person.

32. According to the ICCPR, interference with the enjoyment of the right to privacy may be justified only if the intervention is not "arbitrary or unlawful."²

33. Concerning the ECHR, any complaint lodged before the European Court of Human Rights (ECtHR) directed against a private party would be declared inadmissible for reason of incompatibility with the Convention *ratione personae*. This implies that the State's responsibility is the only one at stake, and not that of a private actor.

² According to the Human Rights Committee "arbitrariness in the meaning of Article 17 is not confined to procedural arbitrariness, but extends to the reasonableness of the interference with the person's rights under Article 17 and its compatibility with the purposes, aims and objectives of the Covenant". Views in *Canepa v. Canada*, No, 558/1993, para 11.4.

34. Nevertheless, although the ECtHR is reluctant to elaborate a general theory on the extent to which the Convention should also apply to relations between private parties it has become established case-law that the Convention does not only oblige the authorities of the Contracting States to respect the rights and freedoms embodied in it, but also requires them to ensure the effective exercise of these rights and freedoms by preventing and remedying any breach thereof.

35. This may imply the so called "positive obligation" on the part of the Contracting States to adopt legislative and other measures in the sphere of the relations between private parties.³

36. The primary duty of the State and public authorities under Article 8 ECHR is to refrain from interfering with an individual's right to respect for his or her private life. However, the State should take positive steps to secure or protect the enjoyment of rights under Article 8.1 ECHR.

37. This so called *Drittwirkung* of provisions of the Convention is also relevant for the protection of the right to respect of one's private life under Article 8 ECHR.

38. The State has thus not only the duty to refrain from interfering illegally with the privacy of the private individual but also to prevent others from doing the same.

39. The right to privacy belongs in the first place to the person who enters a private or public area and who would legitimately expect not to be surveyed by a camera.

40. However, the right to privacy also includes the right of a person to control access to and the behaviour in his or her private property. Hence in both cases the right to respect privacy is concerned.

41. To achieve a balance between the public or private interest involved in monitoring and the private interest not to be intruded upon one's privacy, a proportionality test on the infringement in view of the interest(s) to be protected has to be found.

42. This proportionality test will be found by the State through adequate legislation and administrative practice, and by administrative and judicial control.

43. The Venice Commission has already reaffirmed in its study on video surveillance in public places by public authorities (CDL-AD(2007)014) that a person retains some of her/his privacy in a public place. Consequently, when a person enters an area, he or she will not, as a rule, expect to be surveyed.

44. On the other hand, the right of a person to control access to and behaviour in his or her private property should also be taken into consideration.

45. The State is then facing two possible infringements of the right to respect for private life and according to its positive obligation has the duty to effectively protect both aspects of the right to respect for private life.

46. Consequently, the surveillance operated by private operators in private or public areas does also need a justification on the basis of the criteria listed in Article 8.2 ECHR.

³ ECtHR, *Marckx v. Belgium*, Judgment of 13 June 1979, §31; ECtHR, *Botta v. Italy*, Judgment of 24 February 1998, § 33; ECtHR, *Craxi (No. 2) v. Italy*, Judgment of 17 July 2003, §§ 73-76.

47. According to Article 8.2 ECHR, an interference may be justified if it is in accordance with the law and necessary in a democratic society in the interest of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

48. In order to be justified, a restricting rule or measure has to serve a "pressing social need."⁴

49. In concrete terms: a private person may have an interest to intrusively scrutinise a public place with a view to protecting his or her property and /or ensuring security or only to prevent disorder and crime or some of his/her rights. The rule of proportionality would then command *inter alia* that the relevant public place be closely adjacent to the private area the person wants to protect. This means that the surveillance may not cover larger parts of the street concerned than the immediate vicinity, nor be installed in such a way that it also covers the exterior or even interior of other houses.

50. However, the right of the owner or inhabitant to protect his or her private property does not mean that a person who enters somebody else's territory, has no right to respect for his or her privacy. He or she must instead be informed, or reasonably be made aware on other grounds, of the surveillance or the possibility of incidental surveillance. In addition, as is the case with surveillance in public places by public authorities, the person concerned is entitled to know if data have been collected and how the data collected will be processed and what use may be made thereof. And finally, he or she must have a legal remedy to have the legality of the surveillance reviewed.

51. Video surveillance operated by private operators (an owner, inhabitant or licensee of private premises) may be ordered by the public authorities in order to prevent or prosecute disorder or crimes, e.g. in discos or football stadiums. In these circumstances the rule of proportionality and other rules set out above would equally apply.

52. As regards workplaces, the introduction of video monitoring requires respecting the privacy rights of the employees.

53. Here, video surveillance would, in general, be allowed to prevent or detect fraud or theft by employees in case of a well-founded suspicion. However, except in very specific circumstances, videotaping would not be allowed at places such as toilets, showers, restrooms, changing rooms, or smoking areas and employee lounges where a person may trust to have full privacy.

54. Moreover, secret surveillance should only be allowed, and then only on a temporary basis, if proven necessary because of lack of adequate alternatives.

55. Surveillance at the working place will not be proportional if its only purpose is to check if and in what way a person performs his or her job.

56. Without going into depth and into the variety of collective or other labour agreements which might exist in the member States of the Council of Europe regarding the protection of privacy rights of the employees, employers should adhere to written privacy guidelines that provide with adequate insurance and effective supervision.

⁴ See ECtHR, *Leander v. Sweden*, Judgment of 26 March 1987, §58 ; ECtHR *Gillow v. the United Kingdom*, Judgment of 24 November 1984, § 55 ; ECtHR, *B v. United Kingdom*, Judgment of 8 July 1987, § 61.

57. As regards shops, camera surveillance may be justified to protect the property, if such a measure has proven to be necessary and proportional. It may also be justified at certain locations in the shop to prevent and prosecute robberies under threat but, again, only if proven necessary, and no longer than necessary.

58. National legislation will have to clearly define the legal basis of the surveillance and the necessity of the infringement in view of the interests protected.

59. In this respect, and especially in assessing the proportionality of the infringement concerned, national courts have an important role to play.

2. The video surveillance activity is performed by a public authority in private areas

60. As specified above at §§ 15-20, the category of private places is not restricted to private homes, offices, shops, restaurants and working places, where the owner, user or licensee is primarily responsible for what takes place there. One also has to think of places like stadiums, post offices, hospitals and schools; places where the public authorities have also an evident responsibility for the prevention of disorder and crimes.

61. To enable those authorities to install and operate cameras to exercise the necessary surveillance, they will usually do so on the basis of a law and then proceed in good consultation and cooperation with the responsible private parties.

62. However, if they do not get the permission and cooperation needed, on the basis of their public duties and responsibilities (mostly prevention of disorder, crime prevention and crime prosecution) and their related powers, they could be given, on the basis of a law, the right to enter these private places to install the necessary equipment, and also to enter whenever necessary to operate that equipment.

63. If the private place is a home, or an office where also private documents and other private belongings are located, the justification of the interference has to be reviewed on the basis of the criteria of Article 8.2 of the ECHR. In other cases, the test will be the necessity under Article 1.2 of Protocol No. 1 to the ECHR.⁵ In general, only incidental and temporary surveillance of these private places by public authorities will be necessary and proportional.

B. The international protection of processed data

64. Video surveillance might imply, or lead to a processing operation in respect of personal data. Such processing of personal data falls also within the scope of the protection of private life in the meaning of Article 8 ECHR.

⁵ Article 1 reads:

“Article 1 – Protection of property

Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.

The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties.”

65. In addition, video surveillance and the processing of the collected data fall under the scope of the Council of Europe “Convention for the protection of individuals with regard to automatic processing of personal data”⁶ which was opened for signature on 28 January 1981 and which entered into force on 1 October 1985. This Convention purports to protect individuals⁷ against abuses which may accompany the collection and processing of personal data,⁸ and seeks to regulate at the same time the trans-frontier flow of personal data, for instance data collected by video cameras and disseminated in real time, even without being recorded.

66. Video surveillance falls within the scope of the “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data” insofar as the data arising out of sounds and images concern individuals that are or can be identified by way of the connection with other information – such as spoken words, static or dynamic images or other sound data.

67. The “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data”, also enshrines the individual’s right to know that information is stored on him or her and, if necessary, to have it corrected. Thirty – eight member states of the Council of Europe have ratified this convention.⁹

68. An additional Protocol¹⁰ to the above-mentioned Convention entered into force on 1 July 2004. The Protocol enhances the protection of personal data and privacy by improving the original Convention of 1981 in two areas. Firstly, it provides for the setting up of national supervisory authorities responsible for ensuring compliance with laws or regulations adopted in pursuance of the Convention, concerning personal data protection and trans-border data flows. The second improvement concerns trans-border data flows to third countries. Data may only be transferred if the recipient State or international organization is able to afford an adequate level of protection. The Protocol has been ratified by fifteen countries of the Council of Europe.¹¹

⁶ ETS No. 108

⁷ Article 1 of the Convention reads :

“Article 1 – Object and purpose

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him (“data protection”).”

⁸ Article 2 – Definitions

For the purposes of this convention:

- a) *“personal data” means any information relating to an identified or identifiable individual (“data subject”);*
- b) *“automated data file” means any set of data undergoing automatic processing;*
- c) *“automatic processing” includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination;*
- d) *“controller of the file” means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.*

⁹ Albania, Austria, Belgium, Bosnia & Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, “The former Yugoslav Republic of Macedonia”, United Kingdom.

¹⁰ ETS. No. 181, full title: “Additional protocol to the convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows.”

¹¹ Albania, Bosnia & Herzegovina, Croatia, Cyprus, Czech Republic, Germany, Hungary, Lithuania, Luxembourg, Netherlands, Poland, Portugal, Romania, Slovakia, Sweden.

69. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹² is in principle applicable to the processing personal data, including that of sound and image data relating to natural persons, such as in cases of video surveillance. However, video surveillance does not come within the scope of this Directive if it is carried out for the purposes of public security, defense, national security or in the course of State activities relating to the area of criminal law or of other activities which fall outside of the scope of Community law, or if it is carried out by a natural person in the course of a purely personal or household activity.

C. A further element of the legitimacy of video surveillance: the issue of consent

70. In order to be valid, consent – whatever the circumstances are in which it is expressed – must be a “*freely given, specific and informed indication of the data subject’s wishes*”, as defined in Article 2(h) of the Data Protection Directive.¹³

71. aa) Consent must be given freely: “Free” consent means a voluntary decision, by an individual in possession of all of his faculties, taken in the absence of coercion of any kind, be it social, financial, psychological or other. Any consent given under the threat of non-treatment or lower quality treatment in a specific situation cannot be considered as ‘free’. Consent given by a data subject who has not had the opportunity to make a genuine choice or has been presented with a *fait accompli* cannot be considered to be valid.

72. The “Article 29 Working Party”¹⁴ takes the view that reliance on consent should be confined to cases where the individual data subject has a genuine free choice and is subsequently able to withdraw the consent without detriment.¹⁵

73. bb) Consent must be specific: “Specific” consent must relate to a well-defined, concrete situation in which the processing of personal data is envisaged. Unambiguous, as a matter of principle, which excludes considering silence as an indication of will, or opting-out. Therefore a ‘general agreement’ of the data subject e.g. to the collection of his data through video-surveillance would not constitute consent in the terms of Article 2 (h) of the Directive.

74. cc) Consent must be informed: “Informed” consent means consent by the data subject based upon an appreciation and understanding of the facts and implications of an action. The individual concerned must be given, in a clear and understandable manner, accurate and full information of all relevant issues, in particular those specified in Articles 10 and 11 of the Directive, such as the nature of the data processed, purposes of the processing, the recipients of possible transfers, and the rights of the data subject. This includes also an awareness of the consequences of not consenting to the processing in question.

¹² Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; OJ L 281, 23.11.1995, pp. 31-50.

¹³ See, e.g. Art. 29 Working Party’s working documents WP 12 and WP 114.

¹⁴ An independent European advisory body to the European Commission on data protection and privacy (the “Article 29 Data Protection Working Party”).

¹⁵ See also Article 29 Working Party “Opinion 8/2001 on the processing of personal data in the employment context” (WP 84, Section 10).

75. In a growing number of situations, video surveillance for security reasons has become so widely used that people would even expect video surveillance devices installed in semi-public/private areas like banks, sport stadiums, airports, train station, or shops. In some countries and in certain cases installing video recording may actually even be compulsory for security reasons. In such situations the visitor would even expect for security reasons to enter an area under video surveillance.

76. In that context, and as a consequence, the visitor may have no choice but to “consent” or otherwise be deprived of access to the location and service.

77. On the other hand, if consent would systematically be assumed on the ground that the surveillance is to be expected, this would ultimately lead to the enjoyment of the right to privacy being limited to very narrow private places.

78. Moreover, the freedom of the owner/host is not unlimited regarding exactly where and how surveillance takes place and how data are handled. For instance, visitors are entitled to assume that there will be no surveillance in areas that are generally considered to be strictly private in comparison with the wider space, such as toilets and bathrooms. In hotels and guesthouses surveillance is expected in lobbies and corridors, but not in guest rooms. And even if there are good reasons for surveillance, the surveyor is not free in handling the collected data.

79. The question of consent is particularly crucial in case of recording operations in purely personal or household situations, for instance with management of the so called nanny cams or e-family. These cameras provide a way for parents to observe what employees and housekeepers are doing while at home with the children. In this case the consent of the employee should be requested by law.

D. How can national law afford protection?

80. Due to the positive obligation described above, the State has the duty to make sure that surveillance of private areas or public places performed by private operators can be justified on the basis of the criteria listed in the second paragraph of Article 8 ECHR: (a) in accordance with the law; (b) necessary in a democratic society; and (c) in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

81. The Venice Commission’s previous Opinion on video surveillance by public authorities in public places gave an overview of national provisions applying to video surveillance and data protection which may be found either at the constitutional level¹⁶ or at the legislative level.¹⁷

¹⁶ See § 34. CDL-AD(2007)014 “The right to privacy is specifically protected at the constitutional level in almost all member States of the Council of Europe (CoE).” See in CODICES, e.g. Constitution of Andorra (Art. 13-14), Armenia (Art. 20 - 21), Austria (Art. 10), Azerbaijan (Art. 32), Belgium (Art. 22), Bosnia & Herzegovina (Art. 3), Bulgaria (Art. 32), Croatia (Art. 35), Cyprus (Art. 15), Finland (Section 10), Georgia (Art. 20), Greece (Art. 9), Hungary (Art. 59), Iceland (Art. 71), Ireland (Art. 40-42-44-45), Latvia (Art. 96), Lithuania (Art. 22), Malta (Art. 32), Moldova (Art. 28), Netherlands (Art. 10), Poland (Art. 30-31), Portugal (Art. 26), Romania (Art. 26), Russian Federation (Art. 23), Slovak Republic (Art. 19-21), Republic of Slovenia (Art. 35), Spain (Art. 18), Sweden (Chapt. 1 Art. 2), Switzerland (Art. 13), “The former Yugoslav Republic of Macedonia” (Art. 25), Turkey (Art. 20), Ukraine (Art. 32).

¹⁷ See § 38 CDL-AD(2007)014. For an overview of the national law on data protection and their main provisions, see table under: http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/National_laws/index.asp#TopOfPage

82. According to the independent European advisory body to the European Commission on data protection and privacy (the "Article 29 Data Protection Working Party"), several member States have already adopted specific regulations or provisions concerning video surveillance and its supervision.¹⁸¹⁹ Under these regulations installation and use of CCTV and similar surveillance equipment are to be authorised in advance by an administrative authority - which may be represented, in whole or in part, by the national data protection authority, or the national data protection authority directly.

83. Regulations may differ in connection with the public or private nature of the entity responsible for performing the activity of video surveillance.

84. Domestic legislation concerning the protection of personal data usually also contains obligations and prohibitions for private parties.

85. Thus, in the Netherlands, the Law on the Registration of Persons also sets conditions and restrictions for the recording on private premises. That Law, *inter alia*, requires that the recording must serve a reasonable interest, must be in accordance with the law, must not be in violation of public order and good morals, must not be used for another purpose than the one for which the recording took place, and must be adequately protected against loss, theft and unauthorized use. It also provides that the data collected may only be provided to third persons if that ensues from the purpose of the recording, is required by law or is done with the permission of the person concerned.

86. Some countries, like Belgium and France, have specific criminal law provisions concerning a "right to image". It derives from the principle that everyone has an exclusive right to his/her image and could prevent the diffusion of this image. In France Article 226-1 of the Penal Code prohibits editing (by any means) the picture or photomontage of a person without his or her consent.

87. The lawfulness under domestic law of the video surveillance process must be addressed not only under the criteria of Article 8.2 ECHR, incorporated in domestic law, but also under additional criteria such as those laid down in the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" and Directive 95/46/EC.

E. Additional safeguards

a. with regard to the right to be informed

88. The public must be adequately informed about the presence of cameras.²⁰ Such as in the circumstance of video surveillance at public places by public authorities, the person who has reason to believe that his or her data have been recorded at a private place by a private person or public authority, has the right to demand access to the data and correction or destruction, as

¹⁸ Denmark, Finland, France, Greece, Germany, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden.

¹⁹ Further details can be seen in Document WP89, No. 4/2004, adopted on 11 February 2004, footnote 5 (www.europa.eu.int/privacy).

²⁰ For instance, in France, the CNIL (French Data Protection Authority) gives an example of an information board which should be made visible at the entrance of an area under video surveillance: the following text must be inserted along with a graphic sign of a camera

"premises under video surveillance we inform you that these premises are under video surveillance for the reason of [indicate the purposes], for any information please contact [identify the person, service, company competent] to whom you may use your right to access, in compliance with the law 78-16 of 6 January 1978 on computer science and liberties as modified by the law of 6 August 2004."

well as the right to be informed about any use made of these data by the collector himself or by another person to whom the data have been transferred.

b. with regard to the processing

89. Personal data undergoing thorough automatic processing must be obtained and processed fairly and lawfully; must be stored for specified and legitimate purposes and not used in a way incompatible with those purposes; must be adequate, relevant and not excessive in relation to the purposes for which they are stored; must be accurate and, where necessary, kept up to date; must be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which this data is stored.

90. This means also that no records should be kept, unless absolutely necessary and then only for a limited time.

c. with regard to access

91. People are entitled to access to the data collected concerning them.²¹ People are also entitled to be informed about the collection and the processing of those data, whether they have been transmitted to other persons or institutions, and about the use that will be made thereof.

92. The issues dealt with so far leave open some issues which normally do not enter the surveillance debate. One of them is the "chilling effect" of being constantly watched by "Big Brother", which traumatically limits the freedom of one's behaviour, movement and expression.²² This unpleasant and frustrating awareness of being watched and tethered may occur even if the cameras are fake and if there is no camera behind the sign.

93. This gives even a new dimension to the fear that modern societies could develop toward total control and impersonality as envisaged in the anti-utopian fantasies of Zamyatin in "We", Orwell in "1984" and the insights provided by Foucault in "Discipline and Punish" (the Panopticism principle).

94. These concerns, actualised by the dramatic increase in technological potential for total control, indicate that legal regulation should be completely innovative and not limited to amendments of the existing legislation.

IV. Conclusions and recommendations

95. The recent growth of video surveillance is common to all contemporary developed societies, whether privately or publicly operated cameras are concerned.

96. Since video surveillance performed by private operators cannot reasonably be prevented or banned altogether, critical analysis and concerted action to set certain limits on the activities of public or private surveyors is urgently needed.

²¹ See footnote 20.

²² This issue was raised in 1996 by Pierre Herbeq on behalf of the Belgian Human Rights League before the European Commission on Human Rights. His application was declared inadmissible (*Herbeq v. Belgium*, 14 January 1998, App. No. 32200/96, 92 D.R. 92).

97. The Venice Commission considers that new and inventive regulations, both at the national, European and international levels are needed in order to respond to the threat to fundamental rights such as the right to privacy and the right to freedom of movement as well as the right to benefit from specific protection regarding personal data collected.

98. Legal regulation should apply to all situations where surveillance occurs – in public, private and semi-private space – as well to all operators, state and private, including private operators to whom public functions are delegated.

99. The Venice Commission would hence reiterate the Recommendations made in its previous study :

- Video surveillance [performed on grounds of security or safety requirements, or for the prevention and control of criminal offences], shall respect the requirements laid down by Article 8 of the ECHR.

- With regard to the protection of individuals concerning the collection and processing of personal data, the regulations shall at least follow the requirements laid down by Directive 95/46/EC, especially its Articles 6²³ and 7²⁴ which are based on Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in its Article 5.²⁵

²³ According to Art. 6 of the Directive, personal data must be:

- processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed...

²⁴ Art. 7 provides that personal data may be processed only if

- “the data subject has unambiguously given his consent;
- processing is necessary in order to protect the vital interests of the data subject;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority;
- processing is necessary for the purposes of the legitimate interests pursued ..., except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.”

²⁵ Article 5 of the Convention reads:

“Article 5 – Quality of data

Personal data undergoing automatic processing shall be:

- a. obtained and processed fairly and lawfully;
- b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
- d. accurate and, where necessary, kept up to date;
- e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.”

100. Furthermore the Commission recommends, in view of the specificities of video surveillance, that the following measures should also be taken on a systematic basis:

- People should be notified of their being surveyed, unless the surveillance system is obvious. This means that the situation has to be such that the person observed may be assumed to be aware of the surveillance, or has unambiguously given his /her consent.

- A specific independent authority should be set up, as it is done in several European States,²⁶ in order to ensure compliance with the legal conditions under domestic law giving effect to the international principles and requirements with regard to the protection of individuals and of personal data.

101. A person who has reason to believe that he/she has been surveyed and that data concerning him/her have been recorded, should have the right to demand access to the data and correction or destruction of these data, unless during a certain period security reasons must be given priority. The person should also have the right to be informed about any use made of these data by the collector himself or by any another person to whom the data have been transferred.

102. All surveillance equipment should be approved and licensed and be accessible to regular control by the authorities if circumstances so demand.

²⁶ Compulsory requirement of Article 28 of Directive 95/46/EC, for all Member States of the EU and the European Economic Area.