Strasbourg, 23 March 2007 **CDL-AD(2007)014**

Study No. 404 / 2006 Or. Engl.

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

OPINION

ON VIDEO SURVEILLANCE IN PUBLIC PLACES BY PUBLIC AUTHORITIES AND THE PROTECTION OF HUMAN RIGHTS

Adopted by the Venice Commission at its 70th Plenary Session (Venice, 16-17 March 2007)

on the basis of comments by

Mr Pieter van DIJK (Member, the Netherlands)
Mr Vojin DIMITRIJEVIC (Member, Serbia)
Mr Giovanni BUTTARELLI (Expert, Italy)

TABLE OF CONTENTS

I. *Introduction*

1. By letter dated 10 October 2006, the President of the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly, Mr Dick Marty, requested the opinion of the Venice Commission on the question "The extent to which video surveillance is compatible with basic human rights". In particular, the Committee on Legal Affairs raised the following question: "At what moment does normal observation of people in public places (by authorities, by institutions, by citizens) become a legal and political problem because of this observation cameras are used, sometimes in a network?"

2. Mr Pieter van Dijk (CDL(2007)010) and Mr Vojin Dimitrijevic (CDL(2007)011) were appointed as rapporteurs. In addition, in order to have the perspective of issues related to the protection of personal data with regard to video surveillance, comments of an expert were sought. Mr Giovanni Buttarelli (CDL(2007)012), Secretary general of the Data protection Supervisory Authority, Italy, was asked to contribute to this study.

3. The present study, drawn up on the basis of their comments, was adopted by the Venice Commission at its 70th plenary session (Venice, 16-17 March 2007).

1. Scope of the study

4. The present study will focus on the observation of people in public areas by public authorities, performed 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 the main practices with current European Human Rights and Standards.

5. In the limited time of which it disposed, the Venice Commission could only reach preliminary conclusions, which must in no way be considered exhaustive or final. The Commission intends to develop further its reflection in order to lay down guidelines for balancing the public interests involved against the human rights and freedoms of the individual in a democratic society. In that context, video surveillance performed by private operators and surveillance at private places performed by public authorities also deserves to be studied. However, that implies different legal issues and will be dealt with in a forthcoming opinion of the Venice Commission.

6. In order to define the scope of the study, a definition of the terms and concepts concerned is necessary.

2. Public authorities

7. The current study will address the legal issues linked to video surveillance systems that are used by public authorities within the framework of the State's duty to ensure public safety and order and the protection of anyone's rights and freedoms. The study will hence concern national or local authorities in their preventing and protecting activities as well as those related to crime prosecution. Hence this study will not touch upon video surveillance performed by public authorities for purposes concerning defense matters. Nor will this paper concern video surveillance systems set up by individuals or private bodies like banks, casinos, commercial and semi-public establishments.

3. Public areas

8. A public area is a place which can be in principle accessed by anyone freely, indiscriminately, at any time and under any circumstances. Public areas are open to the public. In principle anyone at anytime can have the benefit of this area. A person benefits freely from public areas. Public areas are governed by public authorities whose power to enforce the law and intervene are wider than within private property.

9. Examples of relevant public areas to this study include: public parks, pedestrian streets in the city centers, outdoor public parking areas, residential neighborhood streets, areas such as sports arenas and subway stations. Some public areas like universities, discos or cafés, that may be considered as semi-public areas, should also be included.

4. Private sphere

10. The private sphere in a physical meaning is a place to which access can be restricted by law and by those who own this private sphere. Private spheres are in principle not open freely to the public, are not accessible by anyone, at any time or in any circumstances, are not accessible indiscriminately. Rules governing private sphere belong mainly to private law. The powers of public authorities over these areas are more restricted than over public areas. The present study will not include legal issues raising from the video surveillance of private areas which would for instance concern banks, casinos, stores, private residential areas. Nevertheless, video surveillance of public areas might accidentally cover private premises, and constitute, for instance, a visual intrusion by the authorities into people's home.

11. The private sphere covers 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 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 fulfillment of one's own personality.[1] Private life also covers the physical and moral integrity of a person, including his/her sexual life.

12. Other human rights, like freedom of thought, conscience and religion, fall also into the sphere of private life, whether under Article 18 ICCPR[2] or by virtue of Article 9 CEDH.[3]

---

[1] European Commission of Human Rights, X v. Iceland , Decision of 18 July 1976, pp. 86.87. ECtHR, Klass and Others, 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 on Human Rights, Burghartz v. Switzerland, Decision of 19 February 1992, and ECtHR, Friedl v. Austria, judgment of 31 January 1995, Opinion of the Commission, § 45). 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 June 1997, §§ 44, 56.

[2] "Article 18 ICCPR reads:

1. Everyone shall have the right to freedom of thought, conscience and religion. This right shall include freedom to have or to adopt a religion or belief of his choice, and freedom, either individually or in community with others and in public or private to manifest his religion or belief in worship, observance, practice and teaching.

5. Video surveillance

13. Video surveillance is a technology system of surveillance by cameras which can be chosen, set up and used by public authorities on public places for crime prevention or even crime prosecution. The system usually consists of a number of video cameras which are connected in a closed circuit television (CCTV). The images are sent to a central television monitor and/or recorded. Commonly CCTV installation includes a number of cameras connected to a control room where operators watch a bank of television screens. Hence, the CCTV system requires the intervention of a human being to watch the monitors or review the recording.

14. This study will not deal with video systems that automatically recognize license plates of moving vehicles, or systems that monitor traffic flow and catch people violating traffic laws.

15. It will also not deal with the legal issues and consequences that could arise from the use of fake cameras or video surveillance tools which might achieve the same preventative aim as active systems in terms of public order but which would imply liability issues and not specifically human rights issues.

16. The present study will deal with video surveillance or CCTV - both terms will be used indistinctively in this study - used in public places as an instrument to prevent and prosecute disturbances of public order in general and serious crime in particular. CCTV allegedly aims also to promote, enhance and restore public security.

17. In comparison with human observance, video surveillance is by far more effective under several accounts. In the first place, technology has dramatically improved and can be very sophisticated: for instance, night vision is feasible; zoom and automatic tracking capacities are common; specific detection can be performed on events, details and traits that would be invisible, or not visible to an human eye. An intelligent system can even detect things as a fake beard or fake moustaches and can include facial or voice recognition. Moreover, the possibility for the same image to be reproduced on several monitors that can be monitored by several observers increases the capability for keeping under control events, facts and behaviors that might otherwise escape an on-the-spot observer's attention.

---

2. No one shall be subject to coercion which would impair his freedom to have or to adopt a religion or belief of his choice.

3. Freedom to manifest one's religion or beliefs may be subject only to such limitations as are prescribed by law and are necessary to protect public safety, order, health, or morals or the fundamental rights and freedoms of others.

4. The States Parties to the present Covenant undertake to have respect for the liberty of parents and, when applicable, legal guardians to ensure the religious and moral education of their children in conformity with their own convictions."

[3] Article 9 CEDH reads :

"1. Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion of belief and freedom, either alone or in community with others and in public or private, to manifest his religion or belief, in worship, teaching, practice and observance.

2. Freedom to manifest one's religion or beliefs shall be subject only to such limitations as are prescribed by law and are necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the protection of the rights and freedoms of others."

18. In addition to the sophistication of video surveillance technologies and continual improvement in optical resolution, CCTV also enhances the scope of surveillance. The operator who watches the monitors of the CCTV is capable of controlling simultaneously images coming from several recording devices placed in different locations. The opportunities for pervasive, unrelenting supervision over individuals and places are thereby enhanced; the scope of vision is thus broadened in comparison with human observance.

19. In the case of human observance, one may adjust his/hers own behavior, and ultimately behave in a more "conformist" way; a CCTV system instead might not be visible to the public, and the existence and identity of the controller are normally unknown to the public: this distorts the appreciation by the latter of the existence of any controller, even his/her identity.

20. Lastly, another important feature of video surveillance in comparison with human observation is that many CCTV systems will have recording devices where all images or those selected by the human monitor can be recorded and stored. On the other hand, variations to this configuration exist, to the extent that the images collected can even been misused or disseminated on the Internet on real or delayed time.

21. In conclusion, if one compares video surveillance with human observation as such it becomes evident that CCTV offers far broader potential and hence might be more intrusive with regard to human rights than human observation.

II. Legal analysis

22. Video surveillance of public areas touches upon several individual rights protected both at the international and national level. Furthermore, CCTV raises issues with regard to the protection of personal data.

A. What human rights are at stake?

1. Right to private life

a. Private life at the international level

23. The right to privacy is protected by international instruments like the International Covenant on civil and political Rights(ICCPR) in its Article 17[4] and by the European Convention of Human Rights (CEDH) in its Article 8.[5]

---

4 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."

5 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."

24. When entering a public space or staying there implies that one is conscious that one will be at least seen, even recognized, and that one's behavior may be scrutinized by anyone on this public sphere, one may draw one's own conclusions with respect to these elements and decide to adapt one's behavior accordingly. In principle, before entering a public sphere a person will adjust his/her appearance and demeanor to the possibility of being seen by others.

25. While any human being moving in public areas may well expect a lesser degree of privacy, they do not and should not expect to be deprived of their rights and freedoms including those related to their own private sphere and image (see §§ 10-12).

26. Most cases relating to the protection of the right to privacy concern alleged violations of the latter in places that are not public or by means that are not video surveillance. Private life is not only protected within private areas, though. Indeed, the European Court of Human Rights (ECtHR) has held that there is a zone of interaction of a person with others, even in a public context, which may fall within the scope of " private life".[6]

27. The ECtHR further considered: "There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain".[7]

28. Privacy issues may also arise when pictures are taken by the police during a public demonstration in a public place. This interference will not be considered as intrusive as long as the data collected remain in an administrative file and are not put in a data system process in order to identify the persons.[8]

29. In general, it is not the monitoring as such which is the most problematic, but the recording of the data and their processing which may create an unlawful interference with the right to privacy, especially if the data have been collected by covert surveillance methods.[9]

30. Special problems arise when collected data are used for perverse use. In this regard the ECtHR in the Peck vs. United Kingdom case considered that the publication or general disclosure, for instance for broadcasting purposes, of data obtained by CCTV cameras, constitutes an intrusion into privacy, even if the behavior to which public attention was drawn was performed in public.[10]

31. The Peck case deserves full description of its context since it is most relevant to the subject of this study. A man suffering from depression walked alone down the street, with a kitchen knife in his hand, and attempted suicide. He was unaware that he had been filmed by a CCTV camera installed by the local authorities. The camera operator notified the police who arrived at the scene, where they took the knife and detained the man, suspecting mental derangement

---

6 ECtHR, P.G. and J.H. v. United Kingdom, Judgment of 6 February 2001, § 56.

7 Ibidem, § 57.

8 Ibidem, § 58.

9 ECtHR, Amann v. Switzerland, Judgment of 16 February 2000, §§ 65-66.

10 ECtHR, Peck v. United Kingdom, Judgement of 28 January 2003, § 44.

and eventually freed him. Afterwards photographs were published taken from the CCTV footage supporting favorable publicity for police use of CCTV surveillance. Material obtained on that occasion was thereupon used in a number of media with little or no effort to conceal the applicant's face. The ECtHR observed that, following the disclosure of the CCTV footage, the applicant's actions were seen 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. The disclosure by the Council of the relevant footage therefore constituted a serious interference with the applicant's right to respect for his private life.

32. The right to privacy protects a human being on all occasions and pertains to his/her dignity in all places. The mere observation of a person's appearance and conduct under normal circumstances will cause grave concerns if it serves a purpose which can be detrimental to the privacy, the honor and dignity of that person.

33. Although personal data also fall within the scope of private life, the protection of this right will be further analyzed under §§ 38-46 below.

b. Private life at the national level

34. The right to privacy is specifically protected at the constitutional level in almost all member States of the Council of Europe (CoE).[11] Hence, Constitutional Courts or courts of equivalent jurisdiction may ground their decisions concerning the protection of private life is not only upon the interpretation of binding international instruments given by international courts but also on their own constitution.

35. With regard to the right to privacy in the context of video surveillance, national court decisions have analyzed the lawfulness of video surveillance in the light of the constitutional right to private life. For instance, the Constitutional Tribunal of Portugal, in its decision No. 225/2202 determined that "the use of electronic surveillance devices and the monitoring of citizens by private security bodies constitute a limitation or a restriction on the right to preserve private life, consecrated in Article 26 of the Constitution."[12]

36. On the other hand, a case decided by the Constitutional Court of Hungary, No. 35/2002,[13] concerning the constitutionality of certain provisions of the Sports Act under which the organizers of various sports events should carry out video surveillance in order to ensure public safety and the security of people's assets was examined under the point of view of data protection. One of the judges, in a concurring opinion, emphasized that the Court should have examined the challenged provisions of the Sports Act in the light of the right to privacy and not of data protection.

37. This may serve to illustrate that the protection of personal data falls within the scope of private life but benefits additionally from specific protection of data. The two subjects may differ while the purposes remain identical.

---

[11] 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), Iceland (Art.71), Ireland (Art.40-42-44-45), Latvia (Art. 96), Lithuania (Art. 22), Malta (Art. 32), Moldova (art.28), the 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), Republic of Macedonia (Art.25), Turkey (Art. 20), Ukraine (Art.32)

[12] Quoted from Document WP89, No. 4/2004, adopted on 11 February 2004, footnote 5. (www.europa.eu.int/privacy.

[13] See in CODICES: HUN-2002-2-003 a) Hungary / b) Constitutional Court / c) / d) 19-07-2002 / e) 35/2002 / f) / g) Magyar Közlöny (Official Gazette), 2002/100 / h).

2. Right to free movement

38. Video surveillance in public places will also concern the right to free movement of individuals who are lawfully within a State's territory. The right to free movement is provided for in Article 2 of Additional Protocol N° 4 to the ECHR.[14] This freedom not only concerns the right to move freely in the physical space, but also the right to move without constantly being traced.[15]

3. Data protection

39. Since video surveillance might imply a processing operation in respect of personal data, i.e. its collection, the right pertaining to personal data is also at stake.

40. The regulatory framework concerning data protection is aimed at ensuring that data are processed by respecting not only private life, but also fundamental rights and freedoms.

a. Data protection at the international level

41. As mentioned above, protection of personal data falls within the scope of private life in the meaning of Article 8 ECHR.

42. In addition, video surveillance falls under the scope of the Convention for the protection of individuals with regard to automatic processing of personal data, ETS N° 108, which entered into force on 1 October 1985. This convention purports to protect individuals[16] against abuses which may accompany the collection and processing of personal data [17] and seeks to regulate

---

[14] Article 2 reads:

1. Everyone lawfully within the territory of a State shall, within that territory, have the right to liberty of movement and freedom to choose his residence.

2. Everyone shall be free to leave any country, including his own.

3. No restrictions shall be placed on the exercise of these rights other than such as are in accordance with law and are necessary in a democratic society in the interests of national security or public safety, for the maintenance of ordre public, for the prevention of crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

4. The rights set forth in paragraph 1 may also be subject, in particular areas, to restrictions imposed in accordance with law and justified by the public interest in a democratic society.

[15] Thus, that the measure requiring a person to wear an electronic belt as an alternative for detention is regarded to be a limitation of personal freedom.

[16] 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")."

[17] 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;

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.

43. Video surveillance falls within the scope of the Convention 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.

44. The Convention also enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected. In addition to Montenegro, thirty -three member states of the Council of Europe have ratified this convention.[18]

45. An additional Protocol, ETS. No. 181,[19] to the above-mentioned Convention entered into force on 1 July 2004. This treaty 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. This Protocol has been ratified by fifteen countries of the Council of Europe.[20]

46. Directive 95/46/EC on the protection of individuals with regard to the protection of personal data does not fall within the scope of this study, since the Directive does not apply to the processing of sound and images data for purposes concerning public order, prevention and control of criminal offences in public areas.

b. Data protection at the national level

47. The protection of personal data is protected at the constitutional level in some countries.[21]

48. Many countries, in particular those which have ratified the above-mentioned international conventions,[22] have adopted specific laws on the subject.

---

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.

[18] 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, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The former Yugoslav Republic of Macedonia, United Kingdom.

[19] 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".

[20] Albania, Bosnia & Herzegovina, Croatia, Cyprus, Czech republic, Germany, Hungary, Lithuania, Luxembourg, Netherlands, Poland, Portugal, Romania, Slovakia, Sweden.

[21] In Codices, see e.g Constitution of Albania (Art. 35), Armenia (Art. 20), Azerbaijan (Art. 32), Belgium (Art. 22), Finland (section 10), Georgia (Art. 20), Croatia (Art. 37), Estonia (Art. 42), Netherlands (Art. 10), Poland (Art. 51), Portugal (Art. 35), Sweden (Chapt. 2 Art. 3), The former Yugoslav Republic of Macedonia (Art. 18),

[22] 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

B. Lawfulness of restrictions to the above mentioned rights

1. International conditions

49. Video surveillance of public places can result in restrictions of the right to respect for private life, of the right to freedom of movement and of one's right to protection of personal data. Consequently this activity must conform to the requirement of ICCPR, hence be shown to be "lawful" and not "arbitrary", and must more specially be justified under the conditions laid down in Article 8.2 of the EHRC:

> "There shall be no interference by a public authority with the exercise of this right except such as 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."

50. National regulations or public authorities who want to set up and use video technologies in order to observe public places by means of video surveillance will have to comply with these specific requirements which will be further analyzed .

a. Restrictions to the rights must be prescribed by law

51. Although certain national constitutions,[23] or the French authentic version of Article 8.2 ECHR and Article 2.3 Protocol IV provide that restrictions must be "prévue par la loi", the ECtHR has decided that Article 8.2 ECHR does not require as a legal basis an act emanating from the legislator in the formal sense. Governmental decrees and international regulations may also constitute a sufficient basis[24] as well as unwritten law such as common law.[25]

52. However, the ECtHR has developed rather high standards as to the quality of the legal basis of such an interference with the protected rights:

53. **a.a.** The legal basis must be accessible to the public: It means that "the citizen must be able to have an indication that is adequate, in the circumstances, of the legal rules applicable to a given case."[26] This amounts to the requirement that the legal basis is assumed to be known by the individual, at least with the help of a legal expert.

54. **a.b.** The legal basis must be sufficiently precise in its wording in order for the public to be able to foresee with precision its scope and meaning so as to enable them to adapt and regulate their conduct and behaviour. A citizen "must be able – if need be with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."[27]

---

[23] See, e.g, Article 10 of the Dutch constitution « …except for limitations to be provided by or in virtue of the law… »

[24] ECtHR, De Wilde, Ooms and Versyp v. Belgium, Judgment of 18 June 1971, § 93.

[25] ECtHR, Sunday Times v. United Kingdom, Judgment of 26 April 1979, §§ 47 and 49.

[26] ECtHR, Sunday Times v. United Kingdom, Judgment of 26 April 1979, §§ 47 and 49. Accessibility does not necessarily require codification.

[27] ECtHR, Landvreugd v. the Netherlands, Judgment of 4 June 2002, § 54.

55. **a**.**c.** Adequate safeguards against abuses must be offered in a manner that sufficiently clearly demarcates the scope of the authorities' discretion and defines the circumstances in which it is to be exercised, "having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.[28] This requirement links the legality principle with that of the rule of law, and is of special importance when the surveillance takes place at random.

56. The foregoing observations imply that the national authorities, including the national courts, when considering the compatibility of video surveillance with the Convention, have to pay special attention to the quality of its legal basis.

b. Restrictions must be necessary in a democratic society

57. The ECtHR has consistently held that the adjective "necessary' is not synonymous with "indispensable", but neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable". The interference must correspond to a "pressing social need" and be "proportionate to the legitimate aim pursued."[29]

58. This also implies the requirement that the reasons adduced by the authorities for justifying the interference must be both "relevant and sufficient."[30]

59. Moreover, the kind of measures amounting to the interference must not be such that they have a deterrent effect on the exercise of human rights and other legitimate behaviour.[31]

60. Consequently, the public authorities responsible for the interference in a person's private life must not only prove that their power to do so is grounded on a sufficient and adequate legal basis but also that this power in the concrete circumstances meets the necessity test. Even though there is a margin of appreciation left to the national authorities, ultimately there is a supervision of the ECtHR in this respect also.

c. Restrictions must be justified, inter alia, by the prevention of disorder or crime or the interests of national security

61. National and local authorities are in a better position than the ECtHR to assess what measures are necessary to prevent disorder and restore order, to prevent and prosecute crimes, and to protect national security.

62. Therefore, they are left with a broad margin of appreciation. In the *Leander* Case the ECtHR held as follows: "There can be no doubt as to the necessity, for the purpose of protecting national security, for the Contracting States to have laws granting the competent domestic authorities power, firstly, to collect and store in registers not accessible to the public information on persons and, secondly, to use this information when assessing the suitability of candidates for employment in posts of importance for national security. (…) Having regard to the wide margin of appreciation available to it, the respondent State was entitled to consider that in the present case the interest of national security prevailed over the individual interests of the applicant."[32]

---

28 ECtHR, Olsson v. Sweden, Judgement of 24 March 1988, § 61.

29 ECtHR, Landvreugd v. the Netherlands, Judgement of 4 June 2002, § 74.

30 ECtHR, Olsson v. Sweden Judgement of 24March 1988, § 68.

31 ECtHR, Goodwin v. United Kingdom, Judgment of 27 March 1996, § 39.

32 ECtHR ,Leander v. Sweden, judgement of 26 March 1987, § 67.

63. Although it belongs primarily to the national authorities to assess what is necessary to prevent disruptions of public order and crimes and to protect national security, as with regard to the specific requirement of necessity in a democratic society, the ECtHR may also ultimately control these requirements.

d. Proportionality

64. The measures taken and used by the public authorities must serve a sufficient aim to be justified.

65. A disproportionate measure would be, for instance, to use video-surveillance devices in public toilets to control and maintain a non-smoking policy in this area.

66. The proportionality requirement implies that it must be questioned whether less far-going (less privacy-intrusive) measures are available and would be sufficiently effective to serve the same purpose, e.g. police surveillance. Thus, the aim to prevent the commission of crimes cannot, apart from exceptional situations of imminent threats to security or risks of serious crimes, justify an a-selective surveillance system that implies far-going limitations of privacy and movement for the public at large, since it may be assumed that more selective systems of surveillance are available and sufficiently effective.

67. A surveillance measure is also unjustified if it is devised and/or used in a discriminatory way, for instance in order to register exclusively the criminal behaviour of some components of the population selected under specific criteria like their gender, their membership of a determinate ethnic group, ethnic minority, religious group etc. This data collection would only be admissible when performed for identification purposes.

2. National conditions

68. National regulations can in no way diminish the level of protection enshrined by the ECHR or by other international instruments ratified by a given country.

69. As exposed above, in the field of data protection many countries have not only ratified the Council of Europe's conventions but have also adopted specific laws on this subject.

70. Moreover, in the framework of the implementation of EU Directive 95/46/EC on the processing of personal data by means of video surveillance, EU members countries have adopted legislation, or adapted their regulations to comply with the Directive. Although video surveillance by public authorities falls explicitly outside the scope of this Directive, great improvements have been consequently made in the field of the protection of individuals' rights and more specifically in the field of the data protection .[33]

---

[33] 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…

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

- the data subject has unambiguously given his consent;

71. Some countries, like the Netherlands and France, have adopted specific regulations concerning the installation of video surveillance systems in public places. The French law[34] is an example of strict prerequisites: there must be a security requirement in order to set up a video surveillance system in a public area. Under the law, the security purposes must be very precise. The installation of such devices is subordinate to the approval by the Prefect, after positive decisions by a departmental commission headed by a magistrate. With regard to respect of privacy, the video devices must be set up in such a manner so as not to allow any view into the interior or entrance of a house. Except in the context of criminal proceedings, the records can be stored for a maximum of one month. The public must be clearly and permanently informed of the presence of video surveillance devices and of the authority or person legally responsible.

3. Additional requirements

72. The peculiarities and potentialities of the processing, recording and disseminating of video surveillance devices necessitate additional requirements on several accounts.

a. with regard to people's rights

73. People should be notified of their being watched on public places, or at least the surveillance system has to be obvious.[35] The notification is not only a requirement of privacy protection but also serves the prevention purposes of video surveillance. Particular attention should be given to ensure that the person observed, under normal circumstances, may be assumed to be aware of it or has unambiguously given his consent.[36] Moreover the person who is the subject or alleged subject of surveillance must have an effective remedy, and must be informed about that remedy and how to use it.[37]

b. with regard to data obtained by means of video surveillance

74. Personal data undergoing thorough automatic processing must be obtained and processed fairly and lawfully; stored for specified and legitimate purposes and not used in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are stored; accurate and, where necessary, kept up to date; 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.

- 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

[34] Law N° 95-73, 2&.01.1995, by law N° 96-926.

[35] Notification of video surveillance devices can be done by street signs placed at relevant places or at least by ensuring by any other means that the public is aware of the practice of surveying specific public places.

[36] Even a detained person, who may expect a certain form of constant monitoring of his/her behavior, is entitled to be notified if the data collected in the detention centre re used for a purpose that he or she could not have anticipated. ECtHR, Perry v. United Kingdom, Judgment of 17 July 2003, §§ 42-43

[37] ECtHR, Perry v. United Kingdom, Judgment of 17 July 2003, §§ 47-49.

c. with regard to access to collected data

75. People are entitled to access to the data collected about them. 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.

76. In principle the general rules concerning the public character of governmental information apply, unless there is special legislation.

77. If and as long as access would endanger the prevention or prosecution of crimes, the protection of safety, or the (privacy) rights of others, access may be restricted. This implies a balancing of interests. Thus, a person who needs access in order to prepare his or her defence against prosecution, has a strong claim to protect his or her right to a fair trial with equality of arms. But even then, there must be a balancing of all interests involved, including those of third persons.

78. Lastly, the video surveillance measures should be supervised by an independent authority. For instance, in the Netherlands, the Commission for the Protection of Personal Data has been established by law, and any collection and processing of personal data regulated bylaw is supervised by the Commission, while such collection and processing if not allowed by the law, should be notified to the Commission.

III. Conclusions and recommendations

79. Video surveillance of public areas by public authorities or law enforcement agencies can constitute an undeniable threat to fundamental rights such as the right to privacy and the right of respect for his or her private life, home and correspondence, his/her right to freedom of movement and his/her right to benefit from specific protection regarding personal data collected by such surveillance.

80. Whilst individuals have a reduced privacy expectation in public places, this does not mean that they waive those fundamental rights.

81. Given the high level of sophistication of CCTV, it is recommended that specific regulations should be enacted at both international and national level in order to cover the specific issue of video surveillance by public authorities of public areas as a limitation of the right to privacy.

82. The following elements should in priority be taken into account in these regulations:

- 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 *mutatis mutandis* the requirements laid down by Directive 95/46/EC, especially its Articles 6[38] and 7[39] which are based on

[38] 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;

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in its Article 5.[40]

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

- People should be notified of their being surveyed in public places, 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,[41] 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.

- 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…

39 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.

40 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.

41 France, Italy, Netherlands.