11750/02/EN
WP 67

Working Document on the Processing of Personal Data by means of Video Surveillance

Adopted on 25 November 2002

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 14 of Directive 97/66/EC.

The secretariat is provided by Directorate E (Services, Intellectual and Industrial Property, Media and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.
Website: www.europa.eu.int/comm/privacy

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

HAS ADOPTED THE PRESENT WORKING DOCUMENT:

1. FOREWORD

Public and private bodies have been having increased recourse to image acquisition systems in Europe for the past few years. This circumstance has raised a lively debate both at Community level and in the individual Member States in order to identify prerequisites and limitations applying to the installation of equipment giving rise to video surveillance as well as the necessary safeguards for data subjects.

The experience gathered in the latest years also following transposition at national level of Directive 95/46/EC showed the huge proliferation of closed circuit systems, cameras and other more sophisticated tools that are used in the most diverse sectors.

Furthermore, the development of the available technology, digitalisation and miniaturisation considerably increase the opportunities provided by image and sound recording devices also in connection with their deployment on intranets and the Internet.

In addition to the processing operations in the employment context, which have already been addressed by the Working Party in a detailed document (*Opinion 8/2001 on the processing of personal data in the employment* context[2]), the growing proliferation of video surveillance techniques can be easily appreciated by all citizens.

A non-exhaustive analysis of the main applications shows that video surveillance can serve quite different purposes [3], which can be grouped, however, into a few main areas:

---

1 Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

2 WP 48, adopted on 13 September 2001, available at: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

3 Different video surveillance systems are installed:
a) within and near public and/or publicly accessible buildings such as museums, places of worship or monuments in order to prevent offences and/or minor acts of vandalism,
b) within stadiums and sports facilities especially in connection with certain events,
c) in the transports sector and in connection with road traffic with a view to monitoring traffic on highways and motorways, or else in order to detect speed limit offences and/or breaches of

1) protection of individuals,

2) protection of property,

3) public interest,

4) detection, prevention and control of offences,

5) making available of evidence,

6) other legitimate interests.

Different prerequisites also apply to the installation of video cameras and similar devices.

In a few cases, using a video recording system may actually be compulsory on the basis of specific Member States provisions – this has been the case, for instance, in a few casinos -, or else it serves a purpose to which special importance is attached by the data subjects' relatives – e.g. in connection with the search for missing children and adults. On the other hand, extravagant instances of such use can be quoted – mainly concerning third countries –, in which facial recognition systems have been deployed in order to prevent bigamy or where a local police authority has decided to make publicly available images concerning the hard life led in prison by non-consenting convicts.

Therefore, whereas video surveillance appears to be somehow justified under certain circumstances, there are also cases in which protection is sought impulsively by means of video cameras without adequately considering the relevant prerequisites and arrangements. This is sometimes due to the economic benefits granted on a large scale by public bodies as well as to the offer of better insurance terms in connection with the use of video surveillance equipment.

This is therefore a multifarious, continuously evolving sector, in which several techniques are already available.

The present working document is meant to provide an initial analysis starting from the existence of partially different regulations as well as from the presence of over-

---

regulations on traffic in city centres, or else to control underground premises giving access to subway lines, to monitor petrol stations and inside taxi cabs,

d) in order to prevent and/or detect unlawful conduct in the surroundings of schools, also in connection with the soliciting of minors,

e) within medical facilities during surgery and/or with a view to, for instance, providing distance care to or monitoring patients in intensive care units and/or in areas where seriously ill and/or quarantined patients are hospitalised,

f) in airports, on board ships and near border areas in order to monitor alien smuggling as well as to facilitate searching minors and other missing persons,

g) by private detectives,

h) within and near supermarkets and shops especially when dealing in luxury goods with a view to making available evidence in case offences are committed as well as for the purpose of marketing goods and/or profiling consumers,

i) within and in areas adjacent to private condominiums both for security purposes and in order to make available evidence in case offences are committed,

j) for journalistic and advertisement purposes that are pursued on line by means of either web cams or cameras on line used for tourist promotion and advertising purposes as also related to beach resorts and dancing premises, by filming customers and visitors at regular intervals without any warning.

detailed provisions in the individual national laws, which require a more systematic and harmonised approach.

This working document concerns surveillance aimed at the distance monitoring of events, situations and occurrences, whereas it does not directly consider other instances in which certain events are publicised on an occasional and/or tendential basis in connection with, for instance, transparency of the activity of local authorities and/or parliamentary bodies.

Each operator will then be able to further specify the indications provided herein, both in the relevant sector and as regards future technological developments that the Working Party intends to investigate.

Additionally, the principles considered here apply to the acquisition of images, possibly in association with sound and/or biometric data such as fingerprint data [4].

The above principles may also be taken into account, where concretely applicable, in connection with the processing of personal data that is not performed by video equipment but rather via other types of surveillance i.e. distance control – as is the case, for instance, with satellite-based GPS systems.

This working document is aimed, in the first place, at drawing attention to the wide scope of criteria for the assessment of lawfulness and appropriateness of installing individual video surveillance systems.

However, account has been also taken of the following aspects:

a) it is necessary for the relevant institutions in Member States to evaluate video surveillance from a general viewpoint, also with a view to promoting a globally selective as well as systematic approach to this matter. The over-proliferation of image acquisition systems in public and private areas should not result in placing unjustified restrictions on citizens' rights and fundamental freedoms; otherwise, citizens might be actually compelled to undergo disproportionate data collection procedures which would make them massively identifiable in a number of public and private places.

b) The trends applying to the evolution of video surveillance techniques could be usefully assessed in order to prevent the development of software applications based both on facial recognition and the study and forecasting of the imaged human behaviour from leading inconsiderately to dynamic-preventive surveillance – as opposed to the conventional static surveillance, which is aimed mostly at documenting specific events and their authors. This new form of surveillance is based on the automated acquisition of the facial traits of individuals as well as their "abnormal" conduct in association with the availability of automated alerts and prompts, which possibly entail discrimination dangers.

[4] The more general question of application of Directive 95/46/EC on biometrics will be dealt by the Working Party in a separate document.

2. INTERNATIONAL LEGAL INSTRUMENTS.

a) Convention of Human Rights and Fundamental Freedoms

The protection of privacy is ensured by Article 8 of the Convention of Human Rights.

b) Council of Europe Convention No. 108/1981 for the protection of individuals with regard to automatic processing of personal data.

The scope of this Convention is not limited like Directive 95/46/EC to first pillar activities (see infra). Video surveillance activities entailing the processing of personal data fall within the scope of application of this Convention. The Consultative Committee set up by this Convention has stated that voices and images are considered personal data if they provide information on an individual by making him/her identifiable even if indirectly.

The Council of Europe is currently finalising a set of guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance. These principles should further specify the safeguards applying to data subjects contained in the provisions of Council of Europe instruments.

c) Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union provides in Article 7 for the protection of private and family life, home and communication and in Article 8 for the protection of personal data.

3. SURVEILLANCE UNDER DIRECTIVE 95/46/EC.

The specific features of the processing of personal information included in sound and image data have been expressly highlighted by Directive 95/46/EC (hereinafter referred to as "the Directive"), which refers to them expressly in several points.

The Directive ensures the protection of privacy and private life as well as the larger gamut of protection of personal data with regard to fundamental rights and freedoms of natural persons (art. 1, par. 1).

A considerable portion of the information collected by means of video surveillance concerns identified and/or identifiable persons, who have been filmed as they moved in public and/or publicly accessible premises. Such an individual in transit may well expect a lesser degree of privacy, but not expect to be deprived in full of his rights and freedoms as also related to his own private sphere and image.

Consideration is also to be given here to the right to free movement of individuals who are lawfully within a State's territory, which is safeguarded by Article 2 of Additional Protocol No. 4 to the European Convention for the Protection of Human Rights and Fundamental Freedoms.

This freedom of movement may only be subject to such restrictions as are necessary in a democratic society and proportionate to the achievement of specific purposes. Data subjects have the right to exercise their freedom of movement without undergoing excessive psychological conditioning as regards their movement and conduct as well as without being the subject of detailed monitoring such as to track their conduct on account of the disproportionate application of video surveillance by several entities in a number of public and/or publicly accessible premises.

Specificity and sensitivity of the processing of sound and image data concerning natural persons are highlighted in the initial recitals of the Directive. In addition to the considerations that will be made below as to the scope of application, these recitals and the relevant articles in the Directive clarify that

a) the Directive applies, in principle, to this matter by also having regard to the importance of the developments of the techniques used to capture, manipulate and otherwise use the specific category of personal data collected in this way (see recital no. 14),

b) the principles of protection of the Directive apply to any information – including sound and image information – concerning an identified or identifiable person, by taking account of all the means likely reasonably to be used either by the controller or by any other person to identify the said person (see Article 2, subheading a), and recital no. 26).

In addition to the above specific references, the Directive obviously produces all its effects within the framework of its individual provisions relating, in particular, to

1) *Data quality*. Images must be processed fairly and lawfully as well as for specified, explicit and legitimate purposes. Images must be used in accordance with the principle that data must be adequate, relevant and not excessive, and not further processed in a way that is incompatible with those purposes; they must be kept for a limited period, etc. (see Article 6),

2) *Criteria for making data processing legitimate*. Based on these criteria, it is necessary for the processing of personal data by means of video surveillance to be grounded on at least one of the prerequisites referred to in Article 7 – unambiguous consent, necessity for contractual obligations, for compliance with a legal obligation, for the protection of the data subject's vital interests, for the performance of a task carried out in the public interest or in the exercise of official authority, balancing of interests,

3) The processing of *special categories of data*, which is subject to the safeguards applying to the use of either sensitive data or data concerning offences within the framework of video surveillance (as per Article 8),

4) *Information* to be given to data subjects (see Articles 10 and 11),

5) *Data subjects' rights*, in particular the right of access and the right to object to the processing on compelling legitimate grounds (see Articles 12 and 14 a),

6) The safeguards applying in connection with *automated individual decisions* (as per Article 15),

7) *Security* of processing operations (Article 17),

8) *Notification of processing operations* (as per Articles 18 and 19),

9) *Prior checking* of processing operations likely to present specific risks to the rights and freedoms of data subjects (under Article 20), and

10) *Transfer of data to third countries* (as per Article 25 and ff.).

Specificity and sensitivity of the processing of sound and image data are finally acknowledged in the last article of the Directive, in which the Commission undertakes to examine, in particular, the application of the Directive to this subject matter and to submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society (see Article 33).

4. NATIONAL PROVISIONS APPLYING TO VIDEO SURVEILLANCE

In several Member States case studies have already been carried out concerning video surveillance based either on constitutional provisions[5]or specific legislation or on orders and other decisions issued by the competent national authorities[6].

In a few countries there are also specific provisions applying irrespective of the circumstance that video surveillance may entail the processing of personal data. Under these regulations, installation and deployment 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. Such regulations may differ in connection with the public or private nature of the entity responsible for operating the relevant equipment.

In other countries, video surveillance is not currently the subject of specific laws; however, data protection authorities have been working to ensure appropriate application of the general data protection provisions inter alia by way of opinions, guidelines or codes of conduct – which have already been adopted in the UK and are being drafted in Italy, for instance.

---

5 See the Decision of the Portuguese Constitutional Court 255/2002. The Court 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".

6 At least in one country (Belgium – Gaia case), the non-compliance with the data protection legislation in the framework of collection of images has led to a refusal of admissible evidence before the Court.

Belgium	Opinions of the DPA, in particular opinion 34/99 of 13 December 1999, related to the processing of images in particular through the use of systems of video-surveillance; Opinion 3/2000 of 10 January 2000 related to the use of video-surveillance systems in entrance halls of apartment buildings.
Denmark	Consolidation Act nr. 76 of 1 February 2000 on the ban on video-surveillance. DPA's decision of 3 June 2002 concerning the video-surveillance by a large group of supermarkets and live transmission from a pub on the Internet.
France	Act n°78-17 of January 6 1978 on Processing, Files and Liberties (CNIL) DPA's Recommendation n° 94056 of 21 June 1994 DPA's guidance concerning video surveillance at workplace: http://www.cnil.fr/thematic/index.htm; on other matters (i.e. webcam)[7] Specific Act concerning video-surveillance for public safety in public areas : Act no. 95-73 of 21 January 1995 on security (as amended by Ordonnance 2000-916 of 19 September 2000) Decree no. 96-926 of 17 October 1996 and Circular Letter of 22 October 1996 on implementation of Act no. 95-73
Greece	DPA's decision of 28 January 2000 (Athens subway)
Germany	Section 6, b in Federal Act 2001.
Ireland	Case study no. 14/1996 (use of CCTV)

[7] See the annual reports of the French Commission Nationale de l'Informatique et des Libertés.

Italy	Section 20 of legislative decree no. 467 of 28.12.2001 (providing for the adoption of codes of conduct) Garante's decisions no. 2 of 10 April 2002 (promoting adoption of codes of conduct), 28 September 2001 (biometrics and facial recognition techniques as implemented by banks) and 29 November 2000 (so-called "video surveillance decalogue") Presidential decree no. 250 of 22.06.1999 (regulating access of vehicles to city centres and restricted access areas) Decree no. 433 of 14.11.1992 and Act no. 4/1993 (applying to museums, state libraries and Archives) Legislative decree no. 45 of 04.02.2000 (passenger ships on national routes) Section 4 of Act no. 300 of 20.05.1970 (so-called Workers' Statute)
Luxembourg	Articles 10 and 11 of the law of 02.08.2002 on the protection of individuals with regard to the processing of personal data
Netherlands	Report of the data protection authority issued in 1997 contains guidelines for video surveillance especially for the protection of individuals and properties on public places. Draft bill which will extend the scope of the criminal offence of making pictures of places accessible for the public without informing them was recently approved by the Lower House. A draft bill which will give explicitly competence to city councils to use video surveillance systems under certain conditions will be transmitted to the Parliament very soon.
Portugal	Decree-Law 231/98 of 22 July 98 (private security activity and systems of self-protection) Law 38/98 of 4 August 98 (measures to be adopted in case of violence associated to sport events) Decree-Law 263/01 of 28 September 2001 (dancing areas) Decree-Law 94/2002 of 12 April 2002 (sport events)

Spain	Ley organica no. 4/1997 (video surveillance by security agencies in public places) Real Decreto no. 596/1999 implementing Act no. 4/1997
Sweden	Video surveillance is specifically regulated in the Act (1998:150) on general video surveillance and the Act (1995:1506) on secret video surveillance (in criminal investigations)[8].
United Kingdom	CCTV Code of practice 2000 (Information Commissioner)

Additional important regulatory instruments have been also adopted in Iceland (Section 4, Act no. 77/2000), Norway (Title VII in Act no. 31 of 14.04.2000), Switzerland (Federal Commissioner's recommendation) and Hungary (DPA's recommendation of 20.12.2000).

5. AREAS WHERE DIRECTIVE 95/46/EC IS WHOLLY OR PARTLY INAPPLICABLE

The Directive does not apply to the processing of sound and image data for purposes concerning public security, defence, State security and the activities of the State in areas of criminal law and/or in the course of any other activity which falls outside the scope of Community law[9]. Nevertheless, many Member States, in transposing Directive 95/46/EC, covered such issues in a general way, by providing, however, for specific exemptions.

A) In a few countries, the processing operations performed for the above purposes are also subject in any case to safeguards in compliance with Convention no. 108/1981 and the relevant Council of Europe recommendations as well as with certain national provisions (see Article 3(2) and recital no. 16 of Directive 95/46/EC). In the light of its peculiar features and the existence of specific provisions also related to the investigational activities carried out by police and judicial authorities as

[8] In Sweden, general video surveillance requires in principle authorisation from the county administrative board although there are a number of exemptions, for example as regards surveillance of post offices, bank offices and shops. Secret video surveillance must be authorised by a court. A decision by the county administrative board according to the Act on general video surveillance may be appealed by the Chancellor of Justice in order to safeguard public interests. Video recording by use of digital cameras has been considered to constitute processing of personal data in the sense of the Swedish Personal Data Act and has consequently fallen under the Data Protection Authority' s supervision. A commission of enquiry is currently analysing the use of video surveillance from a crime prevention perspective. The commission shall i.a. evaluate the Act on general video surveillance to see if amendments are required. The commission of enquiry shall also analyse the scope of application of the Swedish Personal Data Act in respect of video surveillance and the possible need for specific legislation regarding processing of personal data in connection with video surveillance.

[9] See Recital 16.

well as for State security purposes[10] - which may include video surveillance that is "hidden", i.e. carried out without providing information on the premises -, this category of processing operations will not be addressed in detail in this document.

However, the Working Party would like to stress that, similar to several other processing operations of personal data that likewise fall outside the scope of the Directive, video surveillance performed on grounds of actual public security requirements, or else for the detection, prevention and control of criminal offences should respect the requirements laid down by Article 8 of the Convention of Human Rights and Fundamental Freedoms and both be provided for by specific provisions that are known to the public and be related and proportionate to the prevention of *concrete* risks and *specific* offences – e.g., in premises that are exposed to such risks, or in connection with public events that are likely reasonably to result in such offences[11]. The effects produced by video surveillance systems should be taken into account – e.g. the fact that unlawful activities may move to other areas or sectors -, and the data controller should always be specified clearly in order for data subjects to exercise their rights.

The latter requirement is also related to the circumstance that video surveillance is increasingly implemented jointly by police and other public authorities (e.g., local authorities) and/or private bodies (banks, sports associations, transportation companies) – which carries the risk of blurring the individual roles and responsibilities as regards the tasks to be discharged [12].

B) Secondly, the Directive does not apply to processing operations performed by a natural person in the course of a purely personal or household activity (see Article 3(2) and recital no. 12).

Whilst the above circumstances may pertain if, for instance, video surveillance is implemented for the distance control of what happens inside one's home – e.g., to prevent thefts, or in connection with management of the so-called e-family -, this is not the case if the video surveillance equipment is installed either outside or close to private premises with a view to protecting property and/or ensuring security.

---

10 Reference may be made here to the principles laid down by the European Court of Human Rights in the Rotaru v. Romania case, which was examined on 4th May 2000. See above.

11 For instance, a circular letter issued in France on 22.10.1996 referred to isolated places and shops closing late at night.

12 A significant instance of this risk is provided by the activities carried out by a few municipalities in Italy in order to monitor, by video surveillance, public areas where prostitutes are present at night. A number of municipalities claimed in the past that they were – questionably – competent over the prevention of this phenomenon, whilst other municipalities issued orders only prohibiting the prostitutes' clients to park and/or drive their cars in those areas and threatened sending a photograph to their home addresses if they failed to comply. The Italian authority has issued a decision in order to clarify the appropriate arrangements for charging the breach of the relevant provisions.

In the latter cases, it may be, in the first place, that the system is not deployed by individual owners as regards the doors giving access to their own premises, but rather by several owners on the basis of an agreement or else by a consortium or condominium in order to monitor several entrances and areas in a tenement – which makes the Directive applicable to the relevant activities.

Whenever the system is managed for the benefit of an individual family and to monitor a single door, landing, parking, etc., the fact that the Directive does not apply on account of the exclusively personal utilisation as well as of the unavailability of the data to third parties does not exempt the system controller from respecting legitimate rights and interests of his neighbours and other persons in transit. In EU Member States, these rights and interests are actually protected irrespective of data protection principles by the general (civil law) provisions safeguarding personal rights, image, family life and the private sphere – one need only think, for instance, of the visual angle of a camera installed outside the door of a flat, which may allow systematically recording the clients of a medical clinic and/or law firm located on the same floor and thereby cause undue interference with professional secrecy.

Special attention will have to paid to the orientation of video equipment, the need for posting notices and information and the timely deletion of the images - to be performed within a few hours – if no housebreaking or offences are found to occur.

C) Finally, Article 9 of the Directive foresees that Member States shall provide for exemptions or derogation from some of its provision where the processing is carried out solely for purposes of journalism or literary or artistic expression, in particular in the audio-visual field (see recital no. 17). Only the exceptions necessary to reconcile the right to privacy with the rules governing freedom of expression must be provided[13]. In this connection, special care will be required in particular when installing web cams and/or cameras on line, in order to prevent flaws and gaps in the protection of individuals under video surveillance for purposes that may be found to consist in advertising and/or tourist promotion activities [14].

6. VIDEO SURVEILLANCE AND PROCESSING OF PERSONAL DATA

In the light of the diverse situations mentioned, the Working Party is of the opinion that attention should be drawn to the fact that Directive 95/46/EC applies to the processing of personal data, including image and sound data by means of CCTV and other video surveillance systems, wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

---

13 See Recommendation 1/97 of the Working Party on data protection law and the media.

14 A webcam that had been installed surreptitiously near the stairs leading out of a subway station in Milan showed directly on the Net images of the private parts of women in transit for purposes only seemingly related to journalistic activities. The fact that the persons involved could not be identified did not allow the national data protection authority to take steps in this connection.

Image and sound data that relate to identified or identifiable natural persons is personal data:

a) even if the images are used within the framework of a closed circuit system, even if they are not associated with a person's particulars,

b) even if they do not concern individuals whose faces have been filmed, though they contain other information such as, for instance, car plate numbers or PIN numbers as acquired in connection with the surveillance of automatic cash dispensers,

c) irrespective of the media used for the processing – e.g., fixed and/or mobile video systems such as portable video receivers, colour and/or BW images -, the technique used – cabled or fibre optic devices -, the type of equipment – stationary, rotating, mobile -, the features applying to image acquisition – i.e. continuous as opposed to discontinuous, which may be the case if image acquisition only occurs in case a speed limit is not respected and has nothing to do with video shootings performed in a wholly casual, piecemeal fashion – and the communication tools used, e.g. the connection with a "centre" and/or the circulation of images to remote terminals, etc. .

Identificability within the meaning of the Directive may also result from matching the data with information held by third parties, or else from the application, in the individual case, of specific techniques and/or devices.

Hence, one of the first precautions to be taken by the data controller is to check whether the video surveillance entails the processing of personal data as it relates to identifiable persons. If so, the Directive applies regardless of national provisions requiring, in addition, authorisation for public security purposes.

This may be the case, for instance, with equipment located either at the entrance of or inside a bank, where said equipment allows identification of customers; conversely, in certain circumstances the applicability of the Directive may be ruled out for air survey images that cannot be usefully magnified or else do not include information related to natural persons – as may be collected to identify water sources or waste disposal areas – as well as for equipment providing sweeping images of motorway traffic.

7. OBLIGATIONS AND APPROPRIATE PRECAUTIONS APPLYING TO THE DATA CONTROLLER

A) Lawfulness of the Processing

Also in the light of the requirement that processing must be lawful (as per Article 6 (a) of the Directive), the data controller must verify in advance whether the surveillance is compliant with the general and specific provisions applying to this sector – such as laws, regulations, codes of conduct having legal relevance. These provisions may also be laid down in connection with public security purposes as well as with purposes other than those related to personal data protection – e.g. the need to obtain ad-hoc authorisations by specific administrative bodies and comply with their instructions.

All suitable measures must be taken in order to ensure that video surveillance is in line with data protection principles, and inappropriate references to privacy should be avoided [15].

In this regard, account should also be taken of best practices as may be set forth in recommendations issued by supervisory authorities as well as in other self-regulatory instruments.

It is also necessary to check the remaining domestic law provisions – including constitutional principles, civil and criminal law provisions – as regards, in particular, those applying to the "droit à l'image"[16] or the protection of one's domicile; account must be taken of the relevant case law, which may have ruled that premises other than those related to one's household – such as hotel rooms, offices, restrooms, cloakrooms, in-house phone booths, etc. – are to be regarded as private premises.

Where the equipment has been installed either by private entities or by public bodies, especially local authorities, allegedly for purposes of security or else for detecting, preventing and controlling offences, special care will have to be taken, when determining and informing on said purposes, as to the tasks that may be lawfully discharged by the data controller – given that certain public functions may only be exercised under the law by specific non-administrative bodies such as, in particular, law enforcement agencies.

This issue has been raised specifically in respect of a few local authorities having no direct competence over public order and public security matters, which nevertheless carry out auxiliary activities for surveillance purposes. Likewise, surveillance that is often accounted for on grounds of crime control is actually aimed at making available evidence in case criminal offences are committed.

---

15 Recently, a bank and a local police station failed to comply with a customer's request to extract, from the images recorded by a camera also filming an ATM device, those relating to a thief who, after stealing the customer's bank card, had used it to unlawfully collect money via the cash dispenser – on grounds allegedly related to "privacy".

16 This right requires in France and Belgium "prior consent".

B) Specificity, Specification and Lawfulness of Purposes

The data controller should ensure that the purposes sought are neither unclear nor ambiguous, also in order to be provided with a precise criterion when assessing compatibility of the purposes aimed at by the processing (see Article 6 b) of the Directive).

This clarification is also necessary with a view to listing the purposes both in the information to be provided to data subjects and in the relevant notification, as well as in connection with the prior checking to be possibly carried out with regard to the processing in pursuance of Article 20 of the Directive.

It should be clearly ruled out that the images collected may be used for further purposes with particular regard to the technical reproduction opportunities – e.g. by expressly prohibiting copying.

The relevant purposes should be referred to in a document where other important privacy policy features should be also summarised – in respect of such major issues as documenting the time when images are deleted, possible requests for access by data subjects and/or lawful consultation of the data.

C) Criteria Making the Processing Legitimate

The data controller should verify that the video surveillance complies not only with the specific provisions referred to under A), but also with at least one of the criteria making the processing legitimate under Article 7 of the Directive – as regards specifically personal data protection.

Apart from the less frequent cases in which a legal obligation is to be fulfilled – reference has been made to the activities in a casino – or where processing is necessary to protect vital interests – e.g., for the distance monitoring of patients in resuscitation units -, it often happens that a data controller is required to perform a task in the public interest or in the exercise of official authority possibly by complying with specific regulations – e.g. to detect road traffic offences or violent conduct on public transportation means in high-crime areas – as per Article 7 e) of the Directive; alternatively, the data controller may pursue a legitimate interest which is not overridden by the data subject's interests or fundamental rights and freedoms (see Article 7 f)).

In both cases, though especially in the latter one, the sensitive nature of the processing operations requires careful consideration of the scope of the tasks, powers and legitimate interests concerning the data controller. Superficiality and the groundless extension of the scope of such tasks and powers should be absolutely banned in carrying out this analysis.

As regards, in particular, the balancing of different interests, special attention will have to be paid, also by hearing the parties concerned in advance, to the possibility that an interest deserving protection may be in conflict either with installation of the system or with certain data retention arrangements or other processing operations [17].

[17] Under Section 6b of the new German federal data protection act, which came into force on 23 May 2001, the observation of publicly accessible areas by means of optical and electronic devices

Finally, as regards obtaining the data subject's consent, the latter will have to be unambiguous and based on clear-cut information. Consent will have to be provided separately and specifically in connection with surveillance activities concerning premises where a person's private life is led[18].

Lawfulness of the processing should be also assessed by taking account of the provisions in the Directive laying down specific safeguards for the data relating to offences (see Article 8(5) of the Directive) [19].

Processing operations by means of video surveillance should always be grounded on express legal provisions if they are carried out by public bodies.

D) Proportionality of the Recourse to Video Surveillance

The principle that data must be adequate and proportionate to the purposes sought means, in the first place, that CCTV and similar video surveillance equipment may only be deployed on a subsidiary basis, that is to say:

for purposes that actually justify recourse to such systems.

It should be avoided, for instance, that an administrative body may install VS equipment in connection with minor offences – e.g. in order to reinforce the ban on smoking in schools and other public places or else the prohibition to leave cigarette stumps and litter about in public places.

In other words, it is necessary to apply, on a case by case basis, the *principle of adequacy* in respect of the purposes sought, which entails a sort of *data minimisation duty* on the controller's part.

Whilst a proportionate video surveillance and alerting system may be considered lawful if repeated assaults are committed on board buses in peripheral areas or near bus stops, this is not the case with a system aimed either at preventing insults against bus drivers and the dirtying of vehicles – as described to a data protection authority -, or else at identifying citizens liable for minor administrative offences such as the fact of leaving waste disposal bags outside litter bins and/or in areas where no litter is to be left about.

Proportionality should be assessed on the basis of even stricter criteria as regards non-publicly accessible premises.

---

is allowed if, inter alia, there are no grounds to believe that it is to be overridden by interests of the data subject deserving protection.

[18] Specific attention should be given to the real possibility to express a valid consent in the meaning of Article 2 h) of Directive 95/46/EC ("any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed") in case of installation of video surveillance in co-ownership (condominiums etc.).

[19] Reference can be made here to Article 8 of the Portuguese Act no. 67/98 as regards the data concerning persons suspected of participation in unlawful and/or criminal activities.

The exchange of information and experiences among the competent authorities of different Member States may be helpful in this regard [20];

additionally, these systems may be implemented if other protection and security measures entailing no image acquisition – e.g. use of armoured doors to fight vandalism, installation of automatic gates and clearance devices, joint alarm systems, better and stronger lighting of streets at night etc. – prove clearly insufficient and/or inapplicable with a view to the above legitimate purposes.

The above considerations apply, in particular, to the increasingly frequent use of video surveillance for the purpose of self-defence and protection of property – above all near public buildings and offices including the surrounding areas. This type of implementation requires assessing, from a more general viewpoint, the indirect effects produced by the massive recourse to video surveillance – i.e., whether the installation of several devices is really an effective deterrent, or whether the offenders and/or vandals may simply move to other areas and activities.

E) Proportionality in Carrying Out Video Surveillance Activities

The principle under which data must be adequate, relevant and not excessive entails careful assessment of the *proportionality of the arrangements* applying to the data processing once the lawfulness of the latter has been validated.

The *filming arrangements* will have to be taken into account in the first place, by having regard, in particular, to the following issues:

a) the visual angle as related to the purposes sought [21] - e.g., if the surveillance is performed in a public place, the angle should be such as not to allow visualising details and/or somatic traits that are irrelevant to the purposes sought, or else the areas inside private places located nearby, especially if zooming functions are implemented,

b) the type of equipment used for filming, i.e. whether fixed or mobile,

c) actual installation arrangements, i.e. location of cameras, use of fixed-view and/or movable cameras, etc.,

d) possibility of magnifying and/or zooming in images either at the time the latter are filmed or thereafter, i.e. as regards stored images,

e) image-freezing functions,

---

20 This would also allow better harmonisation of both regulatory approaches and administrative decisions, which have sometimes diverged – as has been the case, for instance, with Bingo halls.

21 Examples of specific precautions to be taken as regards visual angle may be found in two provisions issued by the Italian Data Protection Authority. A health care body planning introduction of a service allowing relatives to continuously observe, from a distance, patients in a coma, quarantined and/or seriously ill at an emergency care unit was made aware of the need for making suitable arrangements in order to prevent simultaneous visualisation of other patients as well. In another case, the Authority pointed out to police administrative bodies that it was necessary for a system detecting speed limit breaches to only film the relevant plates rather than the inside of vehicles as well.

f) connection with a "centre" to send sound and/or visual alerts,

g) the steps taken as a result of video surveillance, i.e. shutting down of entrances, calling up surveillance staff, etc. .

Secondly, it is necessary to consider the *decision to be taken as to retention of images and retention period* – the latter having to be quite short and in line with the specific features of the individual case.

Whilst in a few cases a system only enabling closed circuit visualisation of images, which are not recorded, may be sufficient – e.g., in the case of the tills at a supermarket –, in other cases - e.g. to protect private premises – it may be justified to record the images for a few hours and automatically erase them, no later than at the end of the day and at least at the end of the week. An exception to this rule will obviously be the case in which an alert has been issued or else a request has been made deserving specific attention; in such cases there are reasonable grounds to await, for a short time, the decision to be possibly taken by either police or judicial authorities.

To quote another instance, a system aimed at detecting unauthorised accesses of vehicles to city centres and restricted traffic areas should only record images in case a breach is committed.

The proportionality issue should also be taken into due account whenever less short retention periods are deemed to be necessary which should not be in excess of one week[22] – e.g., as regards video surveillance images that may be used to identify the persons frequenting the premises of a bank prior to performing a robbery.

Thirdly, attention will have to be paid to the *cases in which identification of a person is facilitated* by associating the images of the person's face with other information concerning imaged conduct and/or activities – e.g., in the case of the association between images and activities performed by clients in a bank at an easily identifiable time.

In this regard, account will have to be taken of the clear-cut difference existing between temporary retention of video surveillance images obtained by means of equipment located at the entrance of a bank and the definitely more intrusive establishment of data banks including photographs and fingerprints provided by bank clients with the latter's consent.

Finally, consideration will have to be given to the decisions to be made in respect of both the *possible communication of the data to third parties* – which in principle should not involve entities that are unrelated to the video surveillance activities – and their total or partial disclosure possibly abroad or even online – also in the light of the provisions concerning adequate protection, see Article 25 and ff. of the Directive.

22 The Danish and Swedish DPA expressed the view that video recording may only be stored in a short period and this period should not exceed 30 days.

Obviously, the requirement that images should be relevant and not excessive also applies to the matching of information held by different controllers of video surveillance systems.

The above safeguards are meant to implement, also operationally, the principle referred to in the domestic laws of a few countries as the *principle of moderation in the use of personal data* – which is aimed at preventing or reducing, to the greatest possible degree, the processing of personal data.

This principle should be implemented in all sectors by also having regard to the fact that many purposes can be actually achieved without making recourse to personal data, or by using really anonymous data, even though they may initially seem to require the use of personal information.

The above considerations also apply in the presence of the justified need to streamline business resources [23] or else improve the services delivered to users [24].

F) Information to Data Subjects

Openness and appropriateness in the use of video surveillance equipment entail the provision of adequate information to data subjects pursuant to Articles 10 and 11 of the Directive.

Data subjects should be informed in line with Article 10 and 11 of the Directive. They should be aware of the fact that video surveillance is in operation, even where the latter is related to public events and shows or else to advertising activities (web cams); they should be informed in a detailed manner as to the places monitored.

It is not necessary to specify the precise location of the surveillance equipment, however the context of surveillance is to be clarified unambiguously.

The information should be positioned at a reasonable distance from the places monitored – unlike what has been done in a few cases, in which location of information plates at 500 metres from the areas under surveillance has been considered acceptable – also in the light of the filming arrangements.

The information should be visible and may be provided in a summary fashion, on condition that it is effective; it may include symbols that have already been proved useful in connection with video surveillance and no-smoking information – which may differ depending on whether the images are recorded or not. The purposes of the video surveillance and the relevant controller will have to be specified in all cases. The format of the information should be adjusted to the individual location.

---

[23] This may be the case, for instance, with the need to calculate the number of tills to be kept simultaneously open in a supermarket depending on the number of incoming customers, or else with the requirement of building optimised shopping routes for customers in a supermarket.

[24] To facilitate access to a working place and/or a specific transportation means requiring identity controls, personal cards with photographs may be enough, possibly on computerised media, without implementing a facial recognition system.

Specific, well-grounded limitations to the information requirements may only be allowed in the cases referred to in Articles 10, 11 and 13 of the Directive – e.g., a temporary limitation may apply in respect of the data collected in the course of investigations carried out lawfully by defence counsel, or else with a view to exercising the right of defence, for as long as provision of the information may jeopardise achievement of the specific purposes sought.

Finally, specific attention should be given to the appropriate way to furnish blind persons with the information.

G) Additional Requirements

In connection with such additional requirements, precautions and safeguards as are referred to in data protection legislation and are summarised under point 3) above - also with regard to the need for the processing of personal data to be notified to and subject to the supervision of an independent authority in line with Articles 18, 19 and 28 of the Directive -, the Working Party would like to draw attention, in particular, to the following issues:

a) A limited number of natural persons, to be specified, should be allowed to view or access the recorded images, if any, exclusively for the purposes sought by means of the video surveillance or else with a view to maintenance of the relevant equipment in order to only verify its proper operation; alternatively, this may occur on the basis of either a data subject's request for access or the lawful order issued by police or judicial authority for crime detection purposes.

   Whenever video surveillance is only aimed at preventing, detecting and controlling offences, the solution consisting in the use of two access keys – of which one would be held by the controller and the other one by the police – may prove useful to ensure that images are only viewed by police staff rather than by unauthorised staff – without prejudice to the data subject's legitimate exercise of his right of access by means of a request made during the short image retention period.

b) Appropriate security measures should be implemented in order to prevent occurrence of the events referred to in Article 17 of the Directive, including dissemination of information that may be helpful to protect a right of the data subject, a third party or the data controller himself – also with a view to preventing manipulation, alteration or destruction of evidence.

c) Quality of the images recorded, if any, is also fundamental – in particular if the same recording media are used repeatedly, which entails the risk of failing to fully erase previously recorded images.

d) Finally, it is fundamental for the operators concretely involved in video surveillance activities to be adequately trained in and made aware of the steps to be taken to fully comply with the relevant requirements.

H) Data Subjects' Rights

The peculiar features of the personal data collected do not rule out exercise by data subjects of the rights referred to in Articles 13 and 14 of the Directive, with particular regard to the right to object to the processing. Directive 95/46 indeed allows the data subject to object at any time to the processing of data relating to him[25] on compelling legitimate grounds relating to his particular situation.

The data subjects' right to oblivion and the usually short retention period of the images do narrow the scope of application of the data subjects' right to access personal data that make them identifiable; however, this right is to be safeguarded especially if a detailed request is made such as to allow the relevant images to be easily retrieved. Account will have to be also taken of the need to temporarily safeguard the rights of third parties.

Any limitations grounded on the efforts to be made for retrieving the images, where such efforts are found to be clearly disproportionate on account of the short retention period of the images, should be laid down exclusively by secondary legislation (see Article 13(1) of the Directive) with due regard for the data subject's right to defence in respect of specific events that may have occurred in the period considered.

I) Additional Safeguards in connection with Specific Processing Operations

It should be prohibited to perform video surveillance exclusively on account of the racial origin of the persons imaged, their religious or political opinions, their membership in trade unions or sexual habits (Article 8 of the Directive).

Without aiming at an exhaustive list of the multifarious applications of video surveillance, the Working Party would like to stress the need to pay greater attention – in principle, where appropriate, within the framework of the prior checking of processing operations mentioned in Article 20 of the Directive – to a few contexts in which images concerning identified or identifiable persons are collected, since these contexts should be evaluated on a case-by-case basis.

Reference is made, in particular, to the following cases as resulting from experiences and/or tests already in progress:

a) permanent interconnection of video surveillance systems as managed by different data controllers,
b) possible association of image and biometric data such as fingerprints (e.g. at the entrance of banks),
c) use of voice identification systems,
d) implementation, in line with proportionality principles and based on specific provisions, of indexing systems applying to recorded images and/or systems for their simultaneous automatic retrieval, especially via identification data,

[25] Except where otherwise provided by national legislation

e) use of facial recognition systems that are not limited to identifying camouflages of persons in transit, such as fake beards and wigs, but are based on the targeting of suspected offenders – i.e. on the ability of the system to automatically identify certain individuals on the basis of templates and/or standard identity-kits resulting from certain outward features (such as colour of a person's skin, eyes, protruding cheekbones, etc.), or else on the basis of pre-defined abnormal behaviour (sudden movements, repeated transit even at given intervals, way of parking a vehicle, etc.). In this connection, human intervention is appropriate also in the light of mistakes possibly occurring in these cases as also mentioned with regard to point f) below,

f) possibility to automatically trace routes and trails and/or reconstruct or foresee a person's behaviour,

g) taking of automated decisions based either on a person's profile or on intelligent analysis and intervention systems unrelated to standard alerts - such as the fact of accessing a place without the required identification or else a fire alert.

8. VIDEO SURVEILLANCE IN THE EMPLOYMENT CONTEXT

In its *Opinion no. 8/2001 on the Processing of Personal Data in the Employment Context*, adopted on 13 September 2001, and in its *Working Document on the Surveillance of Electronic Communications in the Workplace*, adopted on 29 May 2002 [26], this Working Party has already drawn attention, in more general terms, to a few principles aimed at safeguarding data subjects' rights, freedoms and dignity in the employment context.

In addition to the considerations made in the above documents, to the extent that they are actually applicable to video surveillance, it is appropriate to point out that video surveillance systems aimed directly at controlling, from a remote location, quality and amount of working activities, therefore entailing the processing of personal data in this context, should not be permitted as a rule.

The case is different as regards video surveillance systems that are deployed, subject to appropriate safeguards, to meet production and/or occupational safety requirements and also entail distance monitoring - albeit indirectly [27].

The implementing experience has shown additionally that surveillance should not include premises that either are reserved for employees' private use or are not intended for the discharge of employment tasks – such as toilets, shower rooms, lockers and recreation

---

[26] Both documents are available at the following address: www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index/htm.

[27] In these cases, in addition to the considerations made in this document, account should also be taken specifically of the need to respect the rights referred to in collective agreements, which are sometimes based on the collective information of employees and/or their respective trade union organisations – i.e. apart from the information to be provided on an individual basis in pursuance of data protection laws; in other cases, a prior agreement is to be sought either with employees' representatives or trade union organisations as to installation arrangements, also with regard to duration of the surveillance and other filming arrangements. In a few countries, the State's intervention may be required if no agreement is reached between the parties concerned.

areas; that the images collected exclusively to safeguard property and/or detect, prevent and control serious offences should not be used to charge an employee with minor disciplinary breaches; and that employees should always be allowed to lodge their counterclaims by using the contents of the images collected.

Information must be given to employees and every other person working on the premises. This should include the identity of the controller and the purpose of the surveillance and other information necessary to guarantee fair processing in respect of the data subject, for instance in which cases the recordings would be examined by the management of the company, the recording period and when the recording would be disclosed to the law enforcement authorities. The provision of information for instance through a symbol can not be considered as sufficient in the employment context.

9. CONCLUSION

The Working Party has drafted this working document to contribute to the uniform application of the national measures adopted under Directive 95/46/EC on the area of video surveillance.

* * *

In this framework, it is also fundamental that Member States provide guidance as regards the activity of producers, service providers and distributors, and researchers with a view to the development of technologies, software and technical devices that are in line with the principles referred to in this document.

* * *

Done at Brussels, on 25 November 2002
For the Working Party
The Chairman
Stefano RODOTA