Protection of personal data with regard to surveillance (2000) and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance, by Mr. Giovanni BUTTARELLI

(Secretary General of the Data Protection Supervisory Authority of Italy)

Notice

The importance of the phenomenon of surveillance and surveillance activities by technical means which are becoming increasingly sophisticated demands serious thought at both national and international level with regard to the advantages and risks for democratic societies and individuals.

Several states have undertaken work in this field, even considering it necessary to draft specific legislative provisions on data protection in the field of (video-)surveillance.

In this context, the Council of Europe wishes to draw attention to certain particular aspects of surveillance. The Project Group on Data Protection (CJ-PD) of the Council of Europe asked a consultant, Dr Giovanni BUTTARELLI, to write a report on data protection in relation to surveillance activities. This Report acknowledged that any study of surveillance is linked to technological developments in the means of control and should thus be situated in the historical context.

It was therefore wished to highlight a list of Guiding Principles specifically for video surveillance, which ought to be taken into account when preparing specific legislative provisions on data protection with relation to video surveillance. These principles could, where appropriate, be applied to other forms or technical means of surveillance after making any necessary adjustments to them.

The report and guiding principles prepared by Mr Buttarelli were published on the Council of Europe's website in December 2000 for public consultation. Comments on the text were received only from the International Communications Round Table (ICRT) who considered that the principles should be restricted to video surveillance and not extend to all other sectors of surveillance. On the basis of the report and guiding principles prepared by Mr Buttarelli, the CJ-PD decided to prepare a draft containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance. Members of the CJ-PD have been asked to send final written comments on the guiding principles prepared by the Co-ordination Group of the CJ-PD (June 2002). The Co-ordination Group will submit the guiding principles to the CJ-PD at its meeting in October 2002 for examination and approval. It is also preparing the third evaluation of Recommendation R (87) 15 regulating the use of personal data in the police sector.

1) FOREWORD

Any research and/or report on surveillance is related to the technological development of control systems and is therefore to be considered in connection with the relevant historical context.

This is confirmed by a summary overview of the development of surveillance techniques, which initially focused (especially starting from the 1970s) on the monitoring of road traffic or else on the prevention of theft and robberies in banks and shops selling luxury items.

However, the relationship between surveillance and personal rights had long been pointed out, in particular concerning labour relations – so much so that the use of audiovisual and other devices for controlling employees in the workplace was prohibited or specifically regulated by various countries (see, for instance, Italy's Act no. 300/1970).

In subsequent years surveillance techniques were especially refined in respect of the workplace: indeed, it became possible to control better the security of equipment, the quality and regularity of labour performance as well as productivity. The opportunity was also created for monitoring facts and circumstances having no relevance in terms of skill assessment.

During the 1980s there was also an increased use of surveillance techniques in the transportation sector – in particular on subways and in nearby areas – as well as within certain public buildings (in order to prevent vandalism) and in recreational areas.

The growing use of surveillance techniques by an increasing number of highly patronized shops resulted in facilitating the assessment of customer habits and behaviour with regard to the arrangement of the products on sale. In this specific sector, surveillance systems (especially video surveillance systems) became a valuable tool for commercial purposes even though they had been initially (or seemingly) deployed for the prevention of theft and robberies; in turn, this made it possible to rationalize business resources both within a given shop (for example, by determining the number of tills to be opened in accordance with the time of day and the monitoring of entrances) and from a more general standpoint (for example, by devising "shopping routes" that could be found more stimulating by consumers).

Surveillance techniques have been subsequently developing uninterruptedly and have been applied to the most diverse sectors.

In the transportation sector, there has been a continued increase in the number of controlled roads – both motorways and highways – with a view to the monitoring of traffic misdemeanours (even by means of infrared devices) and, more recently, the access to town centres – both big and small.

For instance, video surveillance devices have been installed :

- in stadiums (Footnote 1) and sports facilities;

- in petrol stations;
- in casinos;
- in health care centres (in particular, emergency or reanimation rooms and during surgical operations)
- in sewage and waste disposal plants.

Museums and cathedrals have been the subject of this surveillance, which has also been applied to air or satellite observation activities (in connection with regular filming, with a view to geographic research, for air traffic management and for urban planning purposes).

Similar remote control techniques based on signal transmission are being used in respect of the electronic bracelets for convicts either paroled or released on licence or under house arrest.

Additional applications are related to the following sectors:

- the fight against illegal migrants;
- security of domestic units and residential districts (in this regard, there is a significant trend towards setting up, in the industrial and commercial sectors, "fortress units" as a way of preventing thefts, burglaries and vandalism);
- taxi services (for example, in New York a few cabs have been equipped with infrared cameras filming either clients when they get on the cab or the meter as it starts operating; the relevant images are recorded on digital media and automatically erased unless either the driver or the car owner decides otherwise);
- use of web-cams or online cameras for broadcasting images in connection with tourist promotion activities or else for advertising public places such as bars or night-clubs, or even for showing living conditions in prisons;
- banking institutions, where hidden devices are frequently installed allowing the taking of fingerprints and photographs so as to identify, visually and based on the relevant fingerprints, all visitors – whether they are clients or not, including possible robbers and individuals reconnoitring the place with a view to a robbery.

The voluntary use of remote control techniques for managing the so-called e-family should also be pointed out; it has even been suggested that statistical surveys could be performed on the images recorded in order to establish the behavioural patterns of members of a given community/group.

Finally, reference should be made to the economic interests related to the production of the relevant equipment and devices and to the reduction in insurance premiums granted by insurance companies if surveillance systems or satellite anti-burglar devices are installed in a vehicle.

2) A SHORT OVERVIEW OF THE AVAILABLE TECHNIQUES

As already pointed out, the increasing pace of technological evolution makes it absolutely necessary to set the surveillance issue against the relevant background.

Based on the technical development of these systems, it has progressively become possible :

- to transmit images to a "control centre" from terminals connected either via cable, optic fibres or digital network;
- to record images that in the past were only visible via CCTV (closed circuit television);
- to obtain images with higher resolution and reproduce them in colour;
- to associate images and sound;
- to expand the visual field up to a 360° vision;
- to use fixed and/or mobile, stationary and/or rotational cameras;
- to use zooming functions and therefore, magnify – even to a considerable extent – individual areas in a photogram.

Thus, there is the actual risk that any overview in this sector will rapidly become obsolete.

On the whole, it can be argued that the most significant contribution was not made so much by the enhancement of transmitting equipment (only think of the recently developed subcutaneous transmitters that are used for the surveillance of paroled convicts) or by the possibility of recording and keeping images instead of simply watching them, but rather by the introduction of "intelligent systems" for assessment and intervention. (Footnote 2)

Indeed, the latest surveillance systems do not simply include an image-freezing (and printing) function nor are they exclusively connected to a control centre whence sound or visual alarm signals can be issued or else the closing of entrances to and/or exits from places and shops can be ordered, or where the intervention of staff or even helicopters can be requested. Nowadays, surveillance systems can be equipped or associated with software for automated image retrieval. There are systems allowing the recognition of persons by means of techniques for the targeting of suspected offenders – for instance, based on automatic facial recognition techniques (facial mapping computers).

It is increasingly feasible to issue various types of alarm (including the signalling to watchmen) regarding persons suspected either on account of specific descriptions or based on behavioural patterns that are automatically classified as "abnormal" by the software (for example, in a parking place or at the entrance to a stadium).

This points to the possible identification in future of alleged misbehaviour based either on the outward appearance (physical features, clothing, skin colour) or on actions and events that are regarded as especially interesting (sudden movements, smoke, opening of doors).

Whereas in the past there was just the exchange among supermarkets of videotapes including images of consumers either "suspected" or caught in the act, the most

sophisticated systems available nowadays allow identifying the voice or conversation of the persons filmed – or, at the very least, significant words spoken by such persons – and even searching for a voice or face in an indexed file. For instance, a test system implemented in 1998 allowed retrieving over 1000 images per second, in real time, in order to find a given face; the system could not be fooled by the fact that the person in question was growing a beard or moustache as camouflage.

Recent tests have also allowed tracking the route presumably followed by a person or vehicle within complex scenarios or else identifying persons who frequently or at given intervals follow a certain route.

All the above techniques can obviously be implemented not only for the prevention and control of offences, but also for different purposes – such as finding missing persons or children – and in connection with the public interest; this is why the Council of Europe recommended their utilisation in some cases. (Footnote 3)

Facial recognition systems have been used even with a view to preventing false marriages and – based on consensus – in order to allow access to workplaces or buildings (for example, by providing for the automatic opening of doors and gates in respect of the members of a given family) and for purchasing air tickets and using ATMs (automated teller machines).

There are ceaseless technological innovations in this sector. (Footnote 4)

3) OVERVIEW OF THE EFFECTS OF SURVEILLANCE

In evaluating the effects of surveillance it is necessary, again, to take account of the relevant background.

This type of assessment is usually carried out with delay and is committed to experts, without any information to the public as a whole. Whenever it is decided that the relevant results should be disclosed to the public, the technology is found to have developed further and new considerations and analyses are required. (Footnote 5)

For instance, the use of facial recognition techniques is currently far from widespread and the considerations mentioned above have been made exclusively by enlightened scholars and journalists. Meanwhile the growing diffusion of surveillance techniques and the increased number of entities keeping recorded images would require a different, more advanced type of analysis. It is time for legal scholars not to limit themselves to stressing the dangers of surveillance, but rather pay greater attention to the issue of the real-time interconnection of images obtained via surveillance which are kept by different entities (for example, motorway management companies, banks, town councils, etc.).

Given the above premises, the issue of the effects of surveillance should not only be the province of legal scholars, as the development of control mechanisms in the public sector makes it necessary for Parliament and the relevant institutions to carry out a political

analysis.

In the first place, there is the need for assessing the proportional relationship between security and privacy requirements.

Indeed, surveillance systems may have positive effects in terms of security; however, there is no uniformity in the extent to which this effect can be regarded as positive. In a few cases there has been undoubtedly a decrease in the number of criminal offences in public places; in other cases this surveillance has proved ineffective or caused criminals to move to other nearby areas, or else it has simply allowed obtaining evidence against the persons filmed.

Additionally, it should be considered that facial or behavioural recognition systems may frequently result in mistakes to the detriment of "innocent bystanders" – as they are based on the reduction of a face to a few dozen building elements and on the measurement of distances between key parts.

Since surveillance systems are likely to attain wider diffusion, their beneficial effects are also likely to decrease on account of their becoming rather commonplace. Finally, there is the risk that surveillance is implemented to an excessive extent as a handy way to cope with basic flaws in organisational and/or law enforcement matters rather than in order to meet actual requirements. As an example, consider that in Italy it has been proposed by a town council that video surveillance devices be installed under the wide vaulted passages of a few downtown streets since the police patrolling those streets in a car are unable to keep such passages under visual control.

It has even been suggested that a distinction should be drawn between:

- surveillance for control purposes (i.e., aimed at allowing the taking of measures in case of misconduct), and
- surveillance for prevention purposes (i.e., aimed at establishing a relationship with citizens in order to get them to behave in accordance with a given pattern).

In other words, it is feared that modern society may inadvertently tend to replace or supplement control with the incitement to self-control and the repression of impulses.

This consideration cannot but lead to expanding the scope of the assessment concerning surveillance, instead of limiting the analysis – as is often the case – to establishing whether control mechanisms cause a disproportionate damage to individual freedom as compared with the need for preventing and controlling crime. (Footnote 6)

From this standpoint there can be no doubt as to the need in future for a definitely more selective approach to the use of surveillance systems: the public as a whole should not suffer excessive limitations on account of the need to prevent the misbehaviour of a minority.

The scope of discussion should therefore be expanded by going beyond the issue of the beneficial effects on security for persons and property: it would be more appropriate to evaluate also the effects, if any, on citizens' freedom and conduct.

In other words, in addition to considering the extent to which surveillance causes a breach of privacy, one should evaluate the effects resulting from the widespread use of surveillance as regards citizens' freedom of movement and behaviour.

As to the former issue, one should actually argue whether the freedom of movement which is referred to in many constitutional charters (as well as in Article 2 of Additional Protocol no. 4 to the European Human Rights Convention) means the freedom to move not only in a physical sense, but also in a more fundamental sense – that is to say, the freedom to move without having inevitably to leave continued and/or frequent traces of one's movements for the benefit of permanent "optic informers".

As to the latter issue, it has been suggested that the fact of "being seen without seeing" may influence a person's conduct and activity. On the one hand, hidden filming and/or control devices do not promote openness for citizens; on the other hand, cameras and other devices that are known to have been installed at a given location might lead to "submissive" behaviour on the citizens' part.

It is undoubtedly true that one should expect less privacy in public places; still, the concept that no privacy exists in public places is to be rejected.

Indeed, reference should be made in this regard :

- to domestic laws applying to non-economic rights in connection with copyright matters, which provide for safeguards even in respect of the dissemination/broadcasting of images related to facts, events and ceremonies either of public interest or occurring in public;
- to the national measures implementing Directive 95/46/EC, under which data subjects are entitled to object, on legitimate grounds, to the processing of their personal data even though the processing is ultimately lawful.

Additionally, it should be noted that the openness requirement is sometimes complied with exclusively by providing notification of the fact that cameras or other control devices have been installed and are in operation: citizens are "compelled" to provide personal data (often consisting of images) and no information is given as to their use, even though the data or images are included in data files or used for identification purposes. Citizens may thus be turned into information "subjects", without respecting the right to information self-determination. (Footnote 7)

The lack of openness deprives citizens of the right to know that certain items of evidence included in the relevant data and/or images can be used against them.

If the concern for the possible discrimination against minorities and/or the sexual orientation of persons may be regarded by some as excessive in modern democratic

societies, there is the actual risk of an all-pervasive control: indeed, technology should not be an obstacle to retaining the possibility of anonymity or privacy – all the more so if images are reproduced for private purposes or else for purposes less directly related to the public interest (see the recently reported use of advertising web cams in seaside resorts, which regularly perform close-ups of persons without their being aware of it).

4) THE INSTRUMENTS ADOPTED SO FAR BY THE COUNCIL OF EUROPE

It is probably unnecessary to point out here that the principles of Convention No. 108/1981 are based on the provisions of the Human Rights Convention (Footnote 8) ; by the same token, there is no need to stress that the processing of any personal data relating to natural persons that have been collected in connection with surveillance activities falls – as a rule – within the scope of application of Convention No. 108.

Indeed, this type of processing is performed in part by means of automated procedures on account of the tools used (for example, video cameras, bugs, computers, microphones, satellites, GPS equipment, etc.) (see Article 2(c) of Convention No. 108).

With regard to those Parties which – as is the case with Italy – have made use of the possibility of applying the Convention to the processing of data concerning groups, associations, foundations, societies, etc. as well as to manual processing operations (see Article 3(2), litt. b) and c) of Convention No. 108), the safeguards provided in the Convention also apply to the latter sectors.

Additionally, a few Parties have also provided for the above-mentioned safeguards in respect of collection; by so doing, they have in practice applied Article 11 of the Convention in line with Directive 95/46/EC, which includes collection in the definition of processing – unlike Convention No. 108.

This entails that the processing of data for surveillance purposes falls within the scope of application of Article 5 (quality of data), 7 (security), 8 (right of access), 10 (penalties and remedies) and 12 (transborder data flows) of the Convention – without prejudice to the derogations provided by domestic law in accordance with Article 9 of the Convention.

The application of the above-mentioned provisions to surveillance raises a few issues that will be addressed subsequently in connection with possible new initiatives by the Council of Europe.

It should be pointed out, however, that the application of Article 5 to surveillance activities results in the obligation for any entity processing the data to comply with safeguards that – if domestic legislation also takes account of collection operations and the strict observance of Article 5 is ensured – markedly influence the technical mechanisms underlying data collection. Only think, for instance, of the orientation and visual field of cameras, of the sensitivity of microphones, of the choice as to recording

the data or not, and so on.

As to Article 6 in the Convention, it should be noted that certain data collected for surveillance purposes fall definitely outside the scope of this article: this may be the case, for instance, of surveillance for some commercial purposes or else performed in respect of direct marketing trainees, or even for some surveillance activities carried out by private detectives in connection with civil litigations, etc. There are, however, other data categories that are undoubtedly the subject of Article 6 provisions: reference can made in this regard to the surveillance in operating or emergency rooms, or else to the targeted surveillance activities performed by the police in respect of political and/or trade-union manifestations or small areas in which racial or ethnic minority groups are resident, or else in connection with prostitution activities.

It is currently debated whether Article 6 can also apply to the data collected (in particular by law enforcement agencies) with regard to persons suspected, but not yet convicted of an offence. Based on the wording of the second sentence in Article 6, one might argue that the answer should be negative as it only refers to criminal convictions; however, it has also been pointed out that even the data related to crime should be considered sensitive data, also where there is not yet a criminal conviction, but merely suspicion. (Footnote 9)

Apart from the possibility for the Parties to extend the protection by applying Article 11, this interpretation issue is quite important: with regard to the processing of sensitive data, or data equated to sensitive data pursuant to Article 6, there must be suitable safeguards as provided for by a law, specific regulations or administrative directives (Footnote 10) . Conversely, pursuant to Article 9, any derogations from individual principles in the Convention should be provided for exclusively by a law which also takes account of the "necessity" principle as defined by the European Court of Human Rights. (Footnote 11)

This summary overview of the Convention is based on the following preliminary considerations:

- the Parties to the Convention can exclude certain processing operations from the scope of application of the Convention, as may be the case for the processing of data in connection with State security (a declaration to this effect has been made by Ireland) or else the processing of data for personal or domestic purposes (which has been excluded by various Parties);
- the data and information collected via surveillance are subjected to the Convention insofar as they relate to an individual that is identified or identifiable by reference to other information, irrespective of whether such information concerns linguistic data, static or dynamic images or sound. In this regard, the Consultative Committee of the Convention has rejected the opinion according to which voices and images are not to be regarded as personal data if they are unaccompanied by nominal information: in fact, it is sufficient for voices and images to provide information on an individual by making him/her identifiable even though indirectly. (Footnote 12)

5) CONCEPT OF SURVEILLANCE UNDER CONSIDERATION

The scope of the surveillance concept is wide-ranging by nature and goes well beyond the control via video equipment - which constitutes nevertheless a major issue at stake. It can actually include the control of phone and computerised conversations as well as of the circulation of documents. It may even apply to the distance control of specific users of a service (see, for instance, the location of mobile phones) or else of persons in connection with a judicial action (this is the case with the use of electronic bracelets).

Thus, the attempt at taking into consideration the surveillance issue as a whole either in a single Recommendation or in a single instrument laying down Guidelines is undoubtedly to be commended, but is quite ambitious and may give rise to difficulties in drafting the text and ensuring its implementation.

Reference should be made in this regard to the specific issues related to the performance of surveillance activities for the defence of a legal claim as well as to the derogations from the right of access that in such cases should be provided for on a temporary and detailed basis.

Another important issue in this sector is related to the surveillance of correspondence (whether on paper or via electronic means) with prison convicts – an issue that was the subject of a recent, non-final decision by the European Court of Human Rights (28.09.2000), in which further considerations were made with regard to the legal grounds issue (*2me Section – Affaire M. c. Italie, Requete n. 25498/94*).

The Council of Europe Project Group on Data Protection has been working hard and with the contribution of highly qualified experts in order to add to the array of instruments that has already been developed by the Council of Europe via the inclusion of specific suggestions also in connection with technological innovation.

On account of the importance attached to this target the utmost care will be required in order to :

- avoid overlapping, possible inconsistencies, lack of co-ordination and unwanted softening of the relevant provisions as compared with the measures laid down in the existing Council of Europe Recommendations, and
- avoid following an excessively general approach with a view to including all the existing types of surveillance in the broad sense of the word; this would entail the risk of, on the one hand, setting out measures that are applicable specifically to video surveillance but are not suitable for other sectors, and, on the other hand, failing to envisage rules or exceptions that would be actually necessary when addressing more specific issues.

The scenario resulting from the existing applicable Recommendations points to the existence of incomplete safeguards concerning surveillance; it is necessary, however, not

to jeopardise these safeguards as also related to their scope of application.

A) For instance, if Recommendation No. R(87) 15 is taken into account as a term of comparison, it would be appropriate for any future initiative by the Council of Europe not to fail to consider police activities that are performed in the course of a specific investigation provided for by law, as well as activities of a state security or military intelligence agency. As to specific investigation activities, consideration might be given to the possibility of exemptions applying to investigations in connection with the committing of a criminal offence pursuant to criminal procedural laws – subject to the differences in the existing legal systems.

In the Preamble to Recommendation No. R(87)15 it is stated that member States have the possibility of extending the relevant principles to processing operations for purposes of State security; this same possibility might be provided for in any new initiative taken by the Council of Europe - subject to appropriate safeguards.

With regard to crime prevention and control and the protection of public order, an attempt should be made in order to prevent simultaneous application of both Recommendation No. R(87) 15 and a new "instrument" developed by the Council of Europe. Indeed, Recommendation No. R(87) 15 includes important provisions that should be taken duly into account in connection with future initiatives.

For instance, Recommendation No. R(87) 15

a) allows introducing new technical means for data processing only if all reasonable measures have been taken to ensure that their use complies with the spirit of existing data protection legislation (item 1.2);
b) allows the collection of personal data for police purposes insofar as this is necessary for the prevention of a *real* danger or the suppression of a *specific* criminal offence. Exceptions to this provision can only be introduced by specific national legislation (item 2.1);
c) allows the collection of data by technical surveillance or other automated means only if this is provided for in *specific* provisions (item 2.3);
d) prohibits the collection of data on individuals solely on the basis of their racial origin, religious convictions, sexual behaviour or political opinions (item 2.4);
e) specifies the cases in which the data may be communicated (item 5), which makes it difficult to lay down additional measures in this regard.

Finally, attention should be paid to the provision included in Recommendation No. R(87)15 as regards the right of an individual whose personal data have been collected or stored without his knowledge to be informed if such data are not destroyed (item 2.2). This is especially important in connection with the proposals made as regards the possible limitations on the data subject’s right to be informed in respect of surveillance activities if these limitations are provided for by law in order not to prejudice surveillance activities.

B) As to Recommendation No. R(89) 2 on the protection of personal data used for employment purposes, consideration might be given in particular to the provision requiring employees to be informed or consulted before introducing automated systems for data collection and utilisation (item 3.1) – in addition to the general provision on the respect for private life and human dignity of employees, with particular regard to the possibility of exercising social and individual relations in the workplace (item 2). The aforementioned provision also applies to the use of automatic telephone call logging devices in the workplace (see Recommendation No. R(95) 4, item 7.15).

Special attention should also be paid to the provisions on collection and storage of "sensitive" data concerning employees (see item 10.1 in Recommendation No. R(89)2).

C) Overlapping should be avoided in respect of Recommendation No. R(95)4, on the protection of personal data in the telecommunications sector, with particular regard to telephone services. Indeed, this Recommendation regulates also the services provided by networks allowing users to be in correspondence via images. In this regard, it is provided that anonymous systems must be made available for accessing the network; any interference with the content of communication is in principle prohibited (items 2.2, 2.3, 2.4 and 2.5). Regarding billing operations for the use of telephone services, it must be ensured that subscribers and called users are not located with precision at the time of utilisation (item 7.2.1).

D) Other Recommendations include general provisions on data processing; although these provisions are not expressly related to surveillance, they lay down safeguards and rules that are nevertheless applicable and therefore require co-ordination – especially in respect of data communication and transborder data flows.

If the Council of Europe sticks to the ambitious target of setting out standards applicable to surveillance as a whole, or else to certain types of surveillance – and in particular to video surveillance- co-ordination with a few existing Recommendations is required. There are two alternatives in this regard:

- instances of overlapping could be prevented and a statement could be made to the effect that any new initiative by the Council of Europe (for example, Guidelines on surveillance) is only meant as an addition to the previous Recommendations and applies to such matters as were not addressed by the said Recommendations, which would therefore be left unprejudiced. However, this approach might fail to be fully satisfactory as only a few Recommendations already include provisions that are applicable to this matter albeit indirectly: certain sectors might therefore be left outside the scope of the relevant provisions;
- the substance of any new initiative by the Council of Europe could be fully harmonised with that of the existing Recommendations whenever they are found to overlap, by indicating that the new instrument specifies and expands the existing requirements (for example, as regards data collection mechanisms, exercise of data subjects' rights, etc.).

Alternatively, it might be considered whether it would be appropriate to adopt a list of Guidelines, a sort of summary "decalogue" aimed more specifically at video surveillance and the provision of additional safeguards that should not overlap with those already available.

Regardless of the approach adopted, the Council of Europe might rapidly achieve a satisfactory solution by completing the analysis that has been carried out so far concerning surveillance.

To that end, I believe consideration might be given to the following initial suggestions - which should by no means be regarded as exhaustive.

6) GENERAL REMARKS

Firstly, one should be aware of the risk of drafting an instrument that is excessively broad in scope: this would make it difficult to simultaneously and reasonably take account of all the requirements and – above all – exceptions in respect of *all* the cases and purposes of surveillance activities without resulting in inconsistencies or reduced protection. (Footnote 13)

Secondly, one should aim at preventing any new initiative by the Council of Europe in this sector from being considered - on account of its possibly broad scope of application - excessively generic and lacking in innovation as it includes no such guidelines as would be required by the specific arrangements applying to the collection and processing of data for surveillance purposes (for example, enhanced compliance with the purpose specification and proportionality principles; ad hoc mechanisms for exercising the right of access; provisions on matching and interconnection of data; more specific rules for the storage of data; ban on automatic processing operations aimed at defining personality; etc.).

7) DEFINITIONS

The surveillance concept could perhaps refer to "any activity operated by technical means, consisting in monitoring, collecting and/or recording, on a non-occasional basis, personal data concerning one or more individuals and relating to their behaviour, movements, communications and utilisation of computerised and/or electronic devices" if the Council of Europe decides to address this issue by going beyond the video surveillance concept. (Footnote 14) It is actually preferable to provide for a wide-ranging definition including no excessively technical details. It would also be preferable to refer to non-occasional surveillance rather than to "systematic" operations. In addition, surveillance activities should be taken into consideration as such, irrespective of whether they may entail the possible infringement upon private life.

It may be appropriate to expressly re-affirm that personal data also include images and sound (if the relevant equipment allows identifying data subjects even indirectly) as well as traffic data or data resulting from signal transmission where such data allow locating

individuals or establishing the time of and the parties to a given conversation or communication.

The definition of "processing", if provided, should clarify that reference is also made to the mere observation of behaviour without recording (unless observation is included in the definition of collection).

It should be considered whether communication is to be distinguished from dissemination.

It should be considered whether it might be appropriate to clarify that the unambiguous, conclusive conduct by the data subject can be equated to consent with regard to certain types of surveillance provided that effective, clear information is given.

The exclusion of data processing operations applying to private or family life from the scope of application of any new instrument is basically acceptable, although this provision would be partly superfluous as various Parties have already excluded this sector from the scope of application of the Convention; still, it would not seem to be fully appropriate to provide for the absolute exclusion of :

- surveillance performed by law enforcement agencies in connection with specific investigations pursuant to law; indeed, it would be preferable to refer to criminal investigation activities, which in a few Parties can be performed directly by members of the judicature rather than by law enforcement agencies – in pursuance of the domestic laws regulating criminal procedure;
- surveillance performed by State security agencies; for instance, any exception concerning State security should be harmonised with the possibility granted to Parties by Recommendation No. R(87)15 of applying the latter Recommendation to these matters;
- journalistic activities: indeed, the collection of data in connection with freedom of expression activities should not provide an opportunity for boundless surveillance initiatives – partly on account of the provisions made in various European countries following Directive 95/46/EC.

8) RESPECT FOR PRIVACY

It might be appropriate to briefly refer, in any new instrument drafted by the Council of Europe, to the need for applying national provisions on video surveillance by taking account also of constitutional provisions as well as of the measures laid down in the Criminal Code concerning the protection of domicile - under which certain places such as hotel rooms, offices, public lavatories, locker-rooms, in-house phone booths are regarded as "domicile" (Footnote 15) . In this regard, it should be pointed out that in a few countries items of evidence that have been collected in breach of the law are absolutely inadmissible pursuant to specific provisions of criminal procedural law (Footnote 16) .

It could be considered whether it might be appropriate to call upon member States, manufacturers and service and access providers as well as researchers to commit

themselves to ensuring that software, technologies and technical devices are developed by paying greater attention to data subjects' fundamental rights. (Footnote 17) Similar suggestions are included, for instance,

- in Recommendation No. 1/99 on invisible data processing operations on the Internet, as adopted on 23 February 1999 by the Working Party set up pursuant to Article 29 of Directive 95/46/EC, including the independent DP supervisory authorities of EU member States (this Recommendation also applies, for instance, to clickstreams);
- to a lesser extent, in Recommendation No. R(99)5 of the Council of Europe, on the protection of privacy on the Internet (see the Preamble, where the development of techniques allowing anonymity for data subjects is called upon), (Footnote 18) and in Directive No. 97/66/EC, on the protection of privacy in the telecommunications sector (with regard, for instance, to new forms of anonymous or strictly private access to publicly available telecommunications services – see Recital no. 18).

Conversely, there would be no need for considering another issue which is regulated by public and civil law – namely, the cases in which the owner of a property is under the obligation to allow installation of permanent surveillance devices by a public body, a private entity or else a condominium.

9) COLLECTION AND PROCESSING OF SURVEILLANCE DATA

The principle according to which personal data should be processed lawfully, fairly and for specified, explicit, legitimate purposes could be usefully re-affirmed and highlighted.

10) LAWFULNESS REQUIREMENTS

In laying down the lawfulness requirements for surveillance or video surveillance, account will have to be taken of the safeguards that are already provided for in principle 2 of Recommendation No. R(87)15 : existence of specific legislation; prevention of a real danger.

On the other hand, these requirements will have to be adjusted to other cases - such as the surveillance performed by defence counsel and duly authorised private detectives for the defence of a legal claim, or else the surveillance of the behaviour and conduct of direct marketing trainees.

With regard to the level of specification of domestic legislation, consideration could be given to the decision of the European Court of Human Rights in the Rotaru v. Romania case, which was adopted on 4 May 2000, at the same time as the 5th Meeting of the CJ-PD GC of 10-12 May 2000. (Footnote 19)

Adjustments will also have to be considered in respect of surveillance performed for medical purposes – i.e., in order to safeguard a data subject's life or bodily integrity or in any way protect a legitimate interest of the data subject or a third party. Special attention will have to be paid to those cases in which surveillance may be permitted by law, but

neither the data subject nor the third party are in a position to give their consent. Reference is made here to cases that have occurred in Italy, concerning the continued observation of individuals either in a coma or hospitalised in an emergency room, or else individuals hospitalised and kept in isolation who were only visible at a distance to relatives and friends - in a room where other hospitalised patients could have also been visible if suitable measures had not been taken.

Finally, I would suggest that the lawfulness requirements could be supplemented by providing for the protection of data subjects against "automated individual decisions" related to their personality, professional performance, reliability, behaviour, ethnic origin and so on – as resulting in an "automatic" fashion from the processing of data that have been collected for surveillance purposes (see Article 15 of Directive 95/46/EC). Reference could be made in this regard to the issuing of alarm signals based on facial recognition techniques in connection with skin colour.

I would also like to draw the Council's attention to national laws and regulations providing for the compulsory recording of either the contents or the relevant traffic data, as the case may be, of phone calls and orders placed via computerised means in connection with brokerage activities.

11) PURPOSE

Any instrument providing manoeuvring room for the distance control of employee efficiency – which is currently prohibited in many countries – would be unacceptable. This point needs clarification by the Council of Europe: there must be an absolute ban on any system aimed at intentionally determining quality and quantity of employees' work. Based on the experience gathered by various countries, the use of systems serving *different* purposes should be permitted – such purposes being related to organisational and/or production requirements or else to occupational safety issues; however, given the possibility that these systems result in the distance control of employees, reference should be made to the need for respecting trade unions' rights. Indeed, in a few countries the latter category of surveillance system can only be implemented after informing and – in a few cases – reaching an agreement with the relevant trade unions.

In this regard, safeguards should be set out for all data, whether sensitive or not. Nor would it be acceptable for such safeguards to apply only if the surveillance is "intended" to collect sensitive data (which would not appear to be frequently the case); this would rule out all types of safeguard for those (more frequent) cases in which the data are collected either occasionally or unintentionally or periodically by a surveillance device.

By referring (expressly or not) to Recommendation No. R(89)2 (para. 3), consideration could therefore be given to a few guidelines with a view to, at least,

- suggesting the need to abstain from the filming of places that are reserved for employees and not for work (for example, toilets, showers, locker-rooms, recreational areas);

- hearing the prior opinion of employees in connection with the installation of devices and equipment on account of organisational and/or production requirements, or else for occupational safety purposes; in the latter cases, disclosing the relevant purposes, arrangements, capabilities and utilisation as also related to time and circumstances of the recording;
- granting employees the right also to ground their counterclaims on portions of the recordings that have been taken into account, in whole or in part, in the claims raised against them.

12) BASIC PRINCIPLES TO BE INCLUDED OR SPECIFIED FURTHER

The selectivity and proportionality principles could be specified further in any new instrument that the Council of Europe might decide to develop in future concerning surveillance or video surveillance, by providing that surveillance systems should only be implemented if this is actually necessary in order to prevent or detect crime or else safeguard others' rights and the use of a less privacy-intrusive manner of collection of data proves impossible.

If compliance with the proportionality principle is not ensured, the number of public and private areas under surveillance might increase exponentially in the next few years: the final outcome would be a society placing excessive restrictions on personal freedom. As to proportionality, one should refrain from simply laying down the principle that surveillance must be related to lawful purposes as based on – often generic (Footnote 20) – legislation or else with a view to preventing nondescript offences which might be construed so as to include not only breaches of criminal law, but also breaches of administrative/civil/disciplinary laws. Surveillance should not be ordered for such purposes as detecting non-compliance with the ban on smoking in public lavatories (Footnote 21) or the prohibition on throwing waste and cigarette stubs on public roads. (Footnote 22)

In other words, surveillance should be focused on areas that are really at risk, (Footnote 23) public events that can reasonably be expected to give rise to incidents and more serious crimes.

Greater emphasis could be placed by the Council on the principle according to which data should be relevant and not excessive in relation to the purposes of their processing. In particular, with regard to video surveillance, the relevant stakeholders should be called upon to

- define precisely, in all cases, the location of cameras and the arrangements for filming (as to storage and conservation of images, visual shooting angles, possible limitations on close-ups and image scans);
- reduce the visual field in connection either with the purpose sought or with the areas actually requiring surveillance, with particular regard to those cases in which cameras filming public places allow identifying sound and images from private places nearby;
- perform the filming in a way only allowing, as a rule, a panoramic view of the area under surveillance (subject to technical limitations) – without the possibility of close-ups

or subsequent magnification and by avoiding the inclusion of irrelevant details or physical traits in relation to the purposes sought.

13) INFORMATION FOR THE DATA SUBJECT

The information principle might actually affirm that the information provided to data subjects may fail to include the location of the surveillance devices. However,

- such devices should be precisely listed in advance by the surveillance data controller and reported in the declaration or registration document referred to above, to be deposited with a (preferably independent) public authority;
- the information should not be provided by using remote signs (for example, placed at a distance of up to 500 metres, as is already the case in a few circumstances), but rather by placing such signs at a reasonable distance;
- as to visual symbols, reference might be made very briefly to the possibility (already tested) of providing a different type of information by using the camera symbol (if images are not recorded) as opposed to another symbol if images are also recorded;
- it could be better specified that data subjects are to be informed clearly (even summarily, provided this is effective) in all cases, regardless of the use of electronic networks;
- any restrictions on the information provided to data subjects should be really in proportion to the purpose sought. It might be appropriate to specify (as is the case in a few legal systems, such as the Italian one) that the limitation resulting from the collection of data for investigational purposes or else the defense of a legal claim is a temporary measure and only applies for as long as the provision of information can be reasonably considered to jeopardise the achievement of the above purposes.

Additionally, it might be appropriate to specify with regard to consent requirements that, at least under certain circumstances, the data subject's consent may also consist in his/her conclusive conduct – provided he/she has been given clear information.

14) COMMUNICATION

It would be necessary to exclude, in principle, dissemination of images and communication to third parties who are not concerned by the surveillance activities; the cases in which this might be permitted as well as the relevant arrangements and purposes should be specified in detail.

15) INTERCONNECTION

The proportionality principle could be developed further in this regard, in order to identify those cases in which the indexing of surveillance personal data is allowed. Indexing of the data – especially on a nominal basis – should only be permitted by specific provisions pursuant to the proportionality principle.

Secondly, the proportionality principle should be better detailed so as to limit the matching of surveillance data processed by different controllers to those cases in which this is actually necessary for the purposes provided for by law – especially if the matching is aimed at tracking the "route" followed by a given individual.

16) RIGHT OF ACCESS

Data subjects' rights should be taken into account in a comprehensive fashion as is the case with Community legislation, rather than by simply referring to access and rectification rights.

Based on the considerations made, the following issues could also be addressed:

- a data subject that cannot object to the surveillance should be granted the right to object, on legitimate grounds that are found to prevail based on his/her specific circumstances, to certain types of data processing as provided for in Article 14 of Directive 95/46/EC. This should apply at least to a few of the cases in which surveillance is permitted by law even without the data subject's consent as well as whenever the data subject is informed that lawful surveillance activities are being performed and cannot in practice but give his/her consent as based on his/her conclusive conduct (for example, whenever he/she happens to be on a public road or in a bank where surveillance is signalled). Reference could be made to a case that occurred in Italy, in which an employee accepted the systematic surveillance of her activity in the workplace in order to document individual production phases (in connection with the tanning of hide), but objected to the fact that such images were broadcast for advertising purposes.

Secondly, the need to somewhat reconcile right of access and specific nature of the data undergoing processing is undoubtedly understandable, also in the light of the media used for recording. Still, it would not appear to be acceptable that this is done by ruling out the right of access if the data subject has not been identified but is identifiable.

Indeed, if limitations on the right of access are considered to be necessary, account will have to be taken of the fact that this is only permitted by Article 9(2), litt. b), of Council of Europe Convention No. 108 to a limited extent – i.e., if it is actually necessary for protecting the rights and freedoms of a third person.

For instance, it might be specified that a request for access can always be made by the data subject since it is the expression of an actual right rather than merely of a "legitimate interest"; under certain circumstances, however, the surveillance data controller can lawfully abstain from answering the request and/or processing data in order to make a data subject identifiable if this entails a manifestly disproportionate effort – without prejudice to such measures and steps as might be taken by law enforcement or judicial authorities in compliance with the law.

Furthermore, it might be considered whether it would be appropriate to provide that recovery and communication of the data be ruled out if the data are to be destroyed

within a very short term (for example, 2-3 days or a week); this would be without prejudice to the possibility of accessing the data for the defence of a legal claim or else with a view to producing evidence following an order issued by law enforcement or judicial authorities.

As regards the possible exclusion of the right of access on account of the legitimate interest of a third person, this should only be permitted if the data controller is unable to take technical measures aimed at reconciling the rights of the data subject with those of the third person who is also the subject of the processing. This is the case, for instance, of the partial magnification or blurring of images in which various persons are visible. Access to the data could be permitted in any case if this is necessary for the defence of a legal claim.

Account might be taken expressly of those cases in which access may be deferred lawfully (albeit as a temporary measure) for as long as the discovery of the data by the controller would actually jeopardise the controller's right of defence of a legal claim. Reference could be made in this regard to the evidence collected in cases of conjugal or other infidelity, which defence counsel may plan to produce at trial following the investigations that a private detective has carried out in pursuance of domestic law.

Finally, reference might be made to those cases in which access can be granted by only permitting the inspection of the data as the latter cannot be recorded on any media.

17) CONSERVATION OF DATA

As regards the period of and arrangements for conservation of data, surveillance data controllers should be required to evaluate - even before deciding for how long the data are to be conserved in connection with the purposes to be accomplished - whether it is necessary to conserve the data or it is enough that these data can be visualised in the light of the purposes sought (for example, in the case of a CCTV system used for checking the opening of doors and entrances). (Footnote 25)

Furthermore, the time limits established for each type of surveillance activity should be without prejudice to the possibility and/or the duty for the surveillance data controller or a third party to retain longer such data as may have been extracted with a view to establishing or defending a legal claim. It might also be suggested that surveillance data controllers should not delete or destroy the data if a request for conservation of the data is submitted either by the data subject or a third person with a view to establishing or defending legal actions.

18) RESPECT FOR THE PRINCIPLES

It is appropriate to re-affirm the principle according to which the processing of personal data for surveillance purposes must be the subject of supervision by an independent authority – in line with item 1.1 in Recommendation No. R(87) 15.

This is especially important with regard to local authorities (municipalities, provinces, Regions): although they have in principle no direct competence on matters of public order – and might therefore be considered to fall outside the scope of application of Recommendation No. R(87) 15 - these authorities actually perform various collateral activities for surveillance purposes.

Apart from this general, solemn reference it might be considered whether to provide that surveillance systems be the subject of at least a simple declaration or registration to be made either with a law enforcement agency or an independent authority – in order to ensure transparency and promote the protection of data subjects' rights as well as control by the supervisory authority. (Footnote 26) It might additionally be suggested that in respect of certain more privacy-intrusive surveillance systems the cases be specified in which either prior checking (in line with the relevant provisions included in Article 20 of Directive 95/46/EC) or the prior approval of an authority would be required.

If the surveillance activities performed by media are also taken into consideration (which would seem to be appropriate), the mechanisms envisaged for publicising the processing operations should be brought into line with Recommendation No. R(94) 13 of 22 November 1994 on measures to promote media transparency.

As a conclusion, it might be argued that the Group is faced with the alternative between a new Recommendation on surveillance and the definition of guiding principles to be included in a different type of instrument.

Both solutions are of interest. Twenty years after the adoption of Council of Europe Convention No. 108 what really matters is for the Council of Europe to let its authoritative voice be heard once again.

Footnotes

1) In the *Recommendation on Stewarding* (99/1), adopted on 9-10 June 1999 by the *Standing Committee of the European Convention on Spectator Violence and Misbehaviour at Sports Events and in particular at Football Matches*, attention is drawn to the surveillance of all potentially dangerous areas and the prevention of overcrowding as well as, though in general, to providing spectators with information on all the security devices deployed by organisers.

2) Only think of the DcxNet system which – allegedly – is capable of facilitating driving when coupled with radar systems by operating brakes, steering wheel, etc. or even by guiding the driver in the presence of bad weather (for example, fog). This is an example of electronic networks applied to road traffic.

3) In *Recommendation No. R(96)6 of the Committee of Ministers to Member States on the Protection of the Cultural Heritage against Unlawful Acts* (adopted on 19 June 1996), under item 4 (concerning "*Protective strategies for preventing and responding to unlawful acts*") it is said that the preventive measures applying to museums, cathedrals, etc. should also include electronic surveillance measures (detection, control centre, transmission, closed circuit TV, monitoring access, video surveillance, and so forth).

4) See, for instance, the recently published advertisement by Visionics Corporation (http://www.visionics.com) concerning the new version of the FaceIt Sentinel/Surveillance System 2.0

produced by Visionics.

5) Consider, for instance, that the launching of an "Echelon2" system has been already reported when, in fact, the full picture of the Echelon1 system has not been highlighted yet.

6) In a meeting with Italy's Minister of Justice, it was recently reported alarmingly by 220 Italian chaplains that prison inmates no longer go to confession because they are afraid that bugs may be present in the confessionals.

7) The risks related to the widespread use of video surveillance in respect of the right to information self-determination and free movement in public places are highlighted in the resolution adopted by the 59th Conference of German Data Protection Authorities of the Federation and Länder, which convened in Hannover on 14-15 March 2000 ("Risks and Limitations of Video Surveillance").

8) Mme Marie-Odile Wiederkehr, *Discours d'ouverture, Data Protection in the Police Sector*, Council of Europe, Strasbourg, 13-14 December 1999, p. 10.

9) A. Patjin, Data Protection in the Police Sector, Council of Europe, Strasbourg, 13-14 December 1999, p. 17.

10) Explanatory report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, para. 46.

11) A. Patjin, *Data Protection in the Police Sector*, Council of Europe, Strasbourg, 13-14 December 1999, p. 18.

12) In particular, the Consultative Committee has considered the digital processing of voices and images to always represent "automatic processing", whereas the analogue processing should only be regarded as such if voices and images undergo automatic processing in order to identify data subjects or else contribute to their identification.

13) For instance, in setting out the lawfulness requirements applying to (video) surveillance, the safeguards provided by Recommendation No. R(87) 15 should not be reduced; the latter Recommendation actually requires data collection to be performed for the prevention of a *real* danger (2.1), surveillance to be provided for by *specific* provisions (2.3), no data to be collected concerning an individual solely on the basis of the latter's race etc. (2.4).

14) This definition would include both the tracking of transactions on the Net and satellite surveillance activities, as well as the surveillance aimed at locating a given person (for example, via the signals transmitted by mobile phones).

15) Reference should be made in this regard to two decisions by the Italian Court of Cassation: no. 7063/2000 and no. 8250/2000.

16) This is the case, for instance, of the provision to police of images showing a pusher where such images have been filmed by chance near the restrooms of a shop by surveillance equipment installed by the owner in breach of the law.

17) A similar indication (though aimed actually at permitting the lawful interception of communications) is included in Items II,5 and VI,15 of Recommendation No. R(95)13 concerning problems of criminal procedural law connected with information technology.

18) See also Council of Europe Recommendation No. R(95)4 on telecommunications, where the availability of anonymous access to network and telecommunications services is also called upon (item 2.2).

19) In the decision concerning the lawfulness of the processing of incorrect data by the Romanian Intelligence Service (RIS), the Court stated that:

"*As regards the requirement of foreseeability, the Court noted that no provision of domestic law laid down any limits on the exercise of those powers. Thus, for instance, domestic law did not define the kind of information that could be recorded, the categories of people against whom surveillance measures such as gathering and keeping information could be taken, the circumstances in which such measures could be taken or the procedure to be followed. Similarly, the Law did not lay down limits on the age of information held or the length of time for which it could be kept.*

Section 45 empowered the RIS to take over for storage and use the archives that had belonged to the former intelligence services operating on Romanian territory and allowed inspection of RIS documents with the Director's consent. The Court noted that the section contained no explicit, detailed provision concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed or the use that could be made of the information thus obtained.

It also noted that although section 2 of the Law empowered the relevant authorities to permit interferences necessary to prevent and counteract threats to national security, the ground allowing such interferences was not laid down with sufficient precision.

The Court also noted that the Romanian system for gathering and archiving information did not provide any safeguards, no supervision procedure being provided by Law no. 14/1992, whether while the measure ordered was in force or afterwards.

That being so, the Court considered that domestic law did not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities. The Court concluded that the holding and use by the RIS of information on the applicant's private life had not been "in accordance with the law", a fact that sufficed to constitute a violation of Article 8. Furthermore, in the instant case that fact prevented the Court from reviewing the legitimacy of the aim pursued by the measures ordered and determining whether they had been – assuming the aim to have been legitimate – "necessary in a democratic society".

20) A specific problem is related to local authorities planning the blanket installation of surveillance systems both in respect of crimes falling within their competence (road traffic offences; access to town centres) and as a way to facilitate crime prevention and control (even though local authorities are not always directly competent for ordre public matters).

21) As reported in Belgium concerning a technical high school.

22) A surveillance system was allegedly installed without informing data subjects even at a citizen advice bureau in a German town.

23) This was the concept underlying a French circular letter of 22.10.96, in which isolated places and shops closing late at night were referred to as examples.

24) In Italy, the *Garante per la protezione dei dati personali* has requested that the visual field of cameras used for detecting road traffic offences be limited to the area where number plates are usually located. This is important as regards, for instance, the driver's privacy.

25) For instance, regulations recently passed in Italy (no. 250/1999) provide that the systems used for surveillance of the access to town centres and pedestrianised areas only collect images in case of the commission of offences.

26) The Parties might use, for instance, a portion of the notification form that is commonly available for the notification of a wide range of processing operations.

Guiding principles for the protection of individuals with regard to the collection and processing of personal data by means of video surveillance

Prepared by Mr. Giovanni BUTTARELLI (Secretary General of the Supervisory Authority on Data Protection of Italy) and presented by the Directorate General I (Legal Affairs)

FOREWORD

Many public and private entities have been increasingly using surveillance systems for various purposes and in different sectors, by controlling, in particular, movement of persons and goods, access to property as well as events, situations and conversations – whether by telephone, electronic networks or at a physical location.

Surveillance systems often result into the collection of personal data even though their collection and/or storage is sometimes not aimed at by the surveillance data controller.

A considerable portion of these activities are performed by means of video surveillance devices, which raises specific issues as regards data protection.

Indeed, the data collected during video surveillance activities consist mainly in images and sound which either identify or allow identifying data subjects, whether directly or not, in addition to monitoring their conduct.

Video surveillance activities entailing the processing of personal data fall within the scope of application of Council of Europe Convention No. 108 – whose principles are based on the provisions included in the Convention on the Protection of Human Rights and Fundamental Freedoms.

Additional rights and safeguards are laid down in various Council of Europe Recommendations, in particular:

a) Recommendation No. R(87) 15 on the use of personal data in the police sector;
b) Recommendation No. R(89) 2 on the protection of personal data used for employment purposes;
c) Recommendation No. R(95) 4 on the protection of personal data in the telecommunications sector;

d) various other Recommendations which – though not expressly referring to video surveillance - include safeguards and rules that are relevant in terms of personal data protection as also related to data communication and transborder data flows.

Video surveillance raises specific data protection issues which are not addressed in detail in the instruments that have been referred to, partly on account of the mechanisms of data collection and storage as well as in the light of technological development.

It is therefore necessary to lay down additional guiding principles in order to expand and specify further the safeguards applying to data subjects – without prejudice to the protection already provided by the above instruments in various sectors – as regards any type of video surveillance activity allowing, by means of technical equipment, non-occasional observation, collection and/or storage of personal data relating to one or more individuals in respect of their conduct, movement, communications and use of computers and electronic networks.

These guiding principles are intended for the widest possible dissemination among all public and private users of video surveillance systems, devices and techniques; additionally, they are addressed to Member States, manufacturers, dealers, service and access providers and researchers with a view to developing software and technologies that can pay greater attention to data subjects' fundamental rights in respect of video surveillance.

These guiding principles should also be implemented with regard to other surveillance activities that are not based on the use of video surveillance devices, subject to appropriate adjustments.

GUIDING PRINCIPLES FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE COLLECTION AND PROCESSING OF PERSONAL DATA BY MEANS OF VIDEO SURVEILLANCE

Any video surveillance activity should be undertaken :

1) by checking if and to what an extent it is permitted on suitable grounds of law for lawful, specific, explicit, legitimate purposes and be carried out in a fair manner. Video surveillance activities for police purposes should only be undertaken for the prevention of a real danger or the suppression of a specific criminal offence;

2) by taking such measures as are necessary in order to ensure that this activity complies with personal data protection principles;

3) by only using video surveillance devices if less privacy-intrusive systems cannot be implemented;

4) by complying with the selectivity and proportionality principles as regards the purposes sought in the individual cases, in order to prevent data subjects' freedoms and

conduct (where appropriate, these freedoms may include the data subjects consent, which might be expressed, at least, in conclusive manner) from being unreasonably impinged upon, with particular regard to freedom of movement and right to informational self-determination, and by ensuring a reasonable privacy expectation even in public places;

5) by complying with the principle according to which data must be relevant and not excessive in relation to the image, sound and biometric data collected, by taking especially into account the mechanisms of data collection (e.g. as regards the use of fixed or mobile cameras; extent of visual field; possibility of magnifying images, and so on) and preventing the collected information from being stored, indexed or kept for a long time if this is not necessary for the specific purpose(s);

6) by refraining from video surveillance activities if they are likely to result in discrimination or have been ordered with regard to certain data subjects exclusively on account of their opinions, beliefs or sex life;

7) by complying with the transparency principle, i.e., by publicising the specific video surveillance activity (by submitting a publicly accessible notification to a preferably independent public authority) and informing the data subjects (by providing clear-cut, even summary, information with easily visible signs pointing to the location of filming devices). Restrictions on openness and information requirements should only be permitted to a reasonable, proportionate extent and where they are necessary for protecting the rights, freedoms and purposes which are referred to in Article 9 of Convention No. 108;

8) by ensuring enhanced protection in the presence of specific dangers for data subjects and/or more pervasive controls, e.g. as regards:

- association of images and biometric data;
- use of intelligent analysis and intervention systems;
- software for automatic image retrieval or facial recognition;
- indexing of collected data;
- profiling of data subjects;
- possibility of taking automated decisions in connection with professional skills, performance, reliability, ethnic origin;
- video surveillance aimed at getting citizens to behave in accordance with a given pattern.

9) communication of personal data to third parties who are not concerned by the surveillance activity should be prohibited in principle, subject to specification of the cases in which this can be permitted including the relevant arrangements and purposes;

10) by laying down ad hoc arrangements for the exercise of right of access and other rights by data subjects and only providing for restrictions on these rights to a reasonable, proportionate extent where this is necessary for protecting the rights, freedoms and purposes which are referred to in Article 9 of Convention No. 108. In particular, the

exercise of the right of access should also be permitted (even by means of the visual inspection of images) if the data subject can be identified. The surveillance data controllers should be entitled to refuse access if this entails a clearly disproportionate effort or the data are to be destroyed within a very short time – subject to judicial and legal defense requirements, e.g. as regards postponement of access for defense purposes;

11) by refraining from the use of systems aimed at the intentional surveillance of quality and quantity of performance in the workplace and by ensuring that employees are suitably informed – if necessary by seeking the agreement of the relevant trade unions if such systems are to be implemented on account of organizational and/or production requirements or else for occupational safety purposes entailing distance control; employees' human dignity should be respected in all cases, including the possibility of establishing social and personal relationships in the workplace. In this context, employees should be able to ground their counterclaims on the recordings made.