nes) 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- coordination 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. [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. [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.

(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).

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" [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 [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. [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), [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.

(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).

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. [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.

(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".

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 [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 [21] or the prohibition on throwing waste and cigarette stubs on public roads. [22]

In other words, surveillance should be focused on areas that are really at risk, [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 [24] 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.

(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.

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). [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.

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.

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. [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.

(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.

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

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.

Autorità di controllo comune Schengen

111 Implementation of Schengen in the UK

JOINT SUPERVISORY AUTHORITY

Brussels, 11 March 2002
(OR. EN)
SCHAC 2502/2/02
REV 2

NOTE
from : The Chairman of the JSA
to : The Chairman of the Article 36 Committee (EU/Iceland and Norway Mixed Committee)
Subject : Implementation of Schengen in the UK

I. Introduction

By Council Decision of 29 May 2000 the Council decided that the United Kingdom and Northern Ireland shall participate in the provisions of the Schengen Acquis. This participation includes the provisions concerning the Schengen information system to the extent that they do not relate to Article 96.

In its opinion (SCHAC 2520/01) of 23 October 2001 the JSA Schengen informed you that the UK solution as described in document 8913/01 COMIX 374, leads to processing Article 96 data by the UK in breach of Article 94 of the Schengen Agreement.

In reaction to your request for an opinion regarding new solutions of the UK and Dutch delegations (doc.nr. 6340/02 SIS 12 COMIX 115), the JSA Schengen has reviewed this matter at its meeting of 8 March 2002.

This opinion is closely related to the opinion of the JSA Schengen of 23 October 2001.

II. Grounds for the JSA Opinion

The Schengen Convention that was signed on 19 June 1990, regulates in Title IV a co-operation between the Contracting Parties with the Schengen Information System (SIS) as an instrument to support that co-operation. Leading principle is the full participation of all Contracting Parties in the provisions of Title IV.

The first three chapters of Title IV contain specific rules for the setting up of the SIS, the operation, utilization and the data protection rules. These rules are tailored for a SIS that is composed of identical national sections (N.SIS) and a technical support function (C.SIS).

Since the Council Decision of 29 May 2000 concerning the participation of the United Kingdom and Northern Ireland in some provisions of the Schengen acquis, the questions arises if the provisions in Title IV can be applied in situations where the basis principle of full co-operation is set aside.

From a data protection point of view this means that the proposals which are subject of this opinion must be assessed on the basis of the meaning of the data protection provisions in Title IV. These provisions that are also integrated in the rules regarding the operation and utilization of the SIS are not imposed to the Contracting Parties with the sole purpose of protection the rights of an individual. These pro-

visions also focus on aspects of decent processing of data, confidentiality, reliability and more in general a professional organisation.

The SIS is composed of the N.SIS of the Contracting Parties and the C.SIS that is established to keep the N.SIS identical. Since the questions concerning the participation of the United Kingdom and Northern Ireland focus on the data that will be processed in the N.SIS, the opinion of the JSA will in principal be limited to the N.SIS.

Data in the N.SIS

According to Article 92(2) the data files of the N.SIS of all Contracting Parties must be materially identical. Article 94(1) explicitly limits the processing of data in the N.SIS to those data that are required for the purposes laid down in the Articles 95-100.

This principle of Article 94(1) originates from the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data of 1981 (Convention 108) and the Recommendation nr. (87) 15 adopted by the Committee of Ministers of the Council of Europe on 17 September 1987 regulating the use of personal data in the police sector, and is also incorporated in the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data.

A decision to keep all the N.SIS 100% identical with all categories of data, even if some Contracting Parties do not participate fully with Article 95-100, will be in breach of Article 94(1) and lead to an infringement with the rights of an individual that cannot be justified by mere motives of economic and operational aspects.

A decision to allow a co-operation with only certain aspects of Title IV may cause an operational problem with the C.SIS and the N.SIS, but the non-compliance with Article 92(2) does, from a data protection point of view, not cause an infringement on the rights of an individual. If a procedure is set in place that upholds the principle that an individual can still exercise his rights in every Contracting Party, the mere fact that not every Contracting Party has all the SIS information will cause no infringement on his rights.

This means that applying the Articles 92 and 94 in view of the partial participation by the United Kingdom and Northern Ireland, the principle of Article 94(1) that limits the processing of data in the SIS to the purpose for which the data were entered in the SIS, prevails the principle of Article 92(2).

The effect of the Council Decision regarding the participation of the United Kingdom and Northern Ireland leads - from a data protection point of view- to an interpretation of Article 92(2) that allows the national sections of the SIS not to be materially identical.

The question if Article 92(2) allows the existence of N.SIS-files that are not materially identical with other N.SIS files can also be answered from an operational point of view. The wordings "data-files" in Article 92(2) may correspond to all the data regarding an individual that must be identical in all the N.SIS, as well as to data regarding all the individuals whose data are processed in the N.SIS.

The first interpretation makes participation with some provisions of the Schengen acquis in compliance with Article 92(2) as long as the data regarding an individual, processed in view of one of the purposes mentioned in Article 95-100, will be processed identical in all the N.SIS.

Access to- and use of the SIS data.

Article 92 (1) describes the different sections of the SIS and restricts the access to the alerts for purposes of border checks and controls and other police and customs checks.

Article 101 (1) specifies the categories of authorities that shall have the right of access. The main principle in this article is that only those authorities that are responsible for the checks and controls as mentioned in Article 92 (1) may be granted the right to have access to the data in the N.SIS.

Article 102(1) limits the use of data provided for in the Articles 95-100 to the purposes laid down

for each type of alert referred to in those articles.

Access and use are thus restricted to the purposes for each type of alert as referred to in the Articles 95-100. Since the United Kingdom and Northern Ireland do not participate with the provisions of Article 96, access and use of these data cannot be related to the purpose of Article 96. This also applies to the special provisions that allows the use of these data for examining visa applications and residence permits (Article 101(2)).

The right of access for an individual

The JSA has in its first opinion already described this item in detail and refers to its opinion of 23 October 2001 (SCHAC 2520/01)

The problem with the double alerts

The access to- and use of the N.SIS data is primarily regulated through the Articles 94, 101 and 102. In order to prevent the existence of conflicting alerts in the N.SIS, Article 107 contains a special procedure.

To comply with Article 107, a Contracting Party must check if an alert that it intends to process in the SIS conflicts with an existing alert on the same person.

This obligation to check can be regarded as a special rule for access to - and use of to data for the sole purpose of complying with Article 107. The way this access and use is granted and exercised must be limited to such as is necessary for the prevention of conflicting double alerts.

Since the present Contracting Parties already processed the data that must be checked to comply with Article 107, and provided that this check is exercised in a way limited to such as is necessary for the prevention of conflicting alerts, no problem exists.

In the situation of the participation of the United Kingdom and Northern Ireland the requirement to prevent conflicting alerts needs a different solution compared with those Contracting Parties that have access to all the categories of data.

The requirement to comply with Article 107, does, in the situation where the processing including the use and access to some of some of categories of data is not permitted by the Articles 94(1), 101(1) and 102(1), not provide a legal ground for processing these categories of data. The obligation to limit the access to data for the sole purpose of complying with Article 107 forces to look for a solution that minimise the infringement of the rights of the individual. In practice this solution is generally found in technical- and organisational solutions.

Since the United Kingdom and Northern Ireland are not allowed to process data on reports for purposes, to which they do not participate, a technical- and organisational solution must be established to comply with Article 107.

III. The UK and Dutch solutions

The JSA has assessed these solutions on the basis of the legal grounds as described in Paragraph II.

The proposals of the UK and Dutch delegations give various alternatives for enabling the UK to fulfil all the obligations of participating in the provisions of the Schengen acquis.

The proposed UK solutions start from the idea that all SIS-data are transmitted to and processed by the UK. The access to the Article 96 data is subsequently restricted to a limited number of people with a strictly regulated access.

Since these proposals upholds the principle of transmitting data regarding Article 96 to the UK, these proposals will be in breach of Article 94 of the Schengen Agreement.

The proposed Dutch solutions both starts from the idea that the Article 96 data are not transmitted to the UK but vary in the way this is worked out.

The first Dutch option places a filter at the technical support function (C.SIS) that prevents transmitting Article 96 data to the UK and at the same time provides for a special data base for the purpose of checking for double alerts.

If this check in the special data base is limited to such as is necessary for the prevention of conflicting double alerts, this technical- and organisational solution is in line with the opinion of the JSA as described in Paragraph II.

The second Dutch option places the unfiltered UK data base within the C.SIS. Since this proposal is closely related to the discarded option in annex 1 of doc.nr 6340/02, the JSA shall not comment on that option.

IV Proposal for amending the Schengen Acquis

In the request for a further opinion a request was included to indicate what rules of the Schengen acquis might have to be adapted in respect of each of the available options.

In view of the limited time for the JSA to prepare and adopt this opinion, this request can not be met. However, changing the Schengen acquis in a sense that all the Article 95-100 data shall be distributed to all the N.SIS, even in the case that one or more Contacting Parties do not participate with all the provisions of Title IV, shall not be possible. A change like that shall always be in breach with the basic legal principle underlying Article 94.

V. Opinion

The choice for one of the options in doc.nr. 6340/02 SIS 12 COMIX 15 must be in compliance with the basic data protection principle as laid down in Article 94(1) of the Schengen Convention. The NSIS of the United Kingdom and Northern Ireland may only process data that are required for the purpose laid down in the Articles 95-100 of the Schengen Convention.

The only solution that is in compliance with this basic principle is the Dutch solution, option 1.

Mr. Giovanni Buttarelli , Chairman