Second evaluation of the relevance of Recommendation No. R (87) 15 regulating the use of personal data in the police sector (1998)

CONTENTS

I. AD HOC TERMS OF REFERENCE

1. Name of the Committee:
PROJECT GROUP ON DATA PROTECTION (CJ-PD)

2. Source of terms of reference:
Decision No. CM/547/180193 of the Committee of Ministers and Decision of 7-8 February 1995

3. Completion date:
December 1998

4. Terms of reference:
To evaluate every four years the relevance of Recommendation No. R (87) 15 regulating the use of personal data in the police sector.

5. Other Committee to be informed of terms of reference:
Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD)
European Committee on Crime Problems (CDPC)
Committee of Experts on Police Ethics and Problems of Policing (PC-PO)

II. THE CJ-PD'S CONCLUSIONS

6. The Project Group reached the conclusion that Recommendation No. R (87) 15 gives adequate protection for personal data used for police purposes in the fields which it covers which were relevant at the time of its adoption.

7. It is proposed that the CJ-PD, in particular in consultation with the CDPC, be instructed to consider the question of whether the application of the principles of Recommendation No. (87) 15 to present-day police and judicial practices in combating crime requires the adoption of a supplementary legal instrument to this recommendation.

8. The following points mentioned in the appended report should be taken into consideration for future work:
- the identification of targets of criminal intelligence, either in a substantive way, defining criteria in the law, or in a procedural way, defining the authorities and the circumstances that can give rise to the collection of criminal intelligence;
- the time limit for storing criminal intelligence data after which the data should be reviewed or deleted;
- the use of data about unsuspected persons, collected in the course of the investigation of a specific offence, for the investigation of other unrelated offences;
- the matching of data from open sources, such as the Internet or public files, with police data in order to find data about persons who were not suspected beforehand;
- the notification of the persons about whom data are stored by the police;
- the storage and use of genetic data with a view to the identification of criminals;
- the establishment of a supervisory authority for the protection of personal data held by the police;
- instruments for monitoring development in the use of investigative methods involving the collection, storage and use of personal data.

III. REPORT

i) INTRODUCTION

9. On 17 September 1987 the Committee of Ministers adopted Recommendation No. R (87) 15 regulating the use of personal data in the police sector (Appendix B to the present report).

10. In its Recommendation 1181 (1992) on police co-operation and protection of personal data in the police sector (Appendix C to the present report), the Parliamentary Assembly recommended that the Committee of Ministers, among other things, draw up a Convention enshrining the principles laid down in Recommendation No. R (87) 15.

11. During its 478th meeting (June 1992), the Committee of Ministers adopted Decision No. CM 537/220692 entrusting the Project Group on Data Protection and the Consultative Committee of Convention 108 with the drawing up of an opinion on the Assembly's Recommendation 1181.

12. In the light of these opinions, the Ministers' Deputies, at their 486th meeting (January 1993), adopted Decision No. CM 547/180193, conferring on the Project Group the task of evaluating the relevance of Recommendation No R (87) 15 with a view to its possible revision.

13. The CJ-PD completed a first evaluation of the recommendation in 1994, which appears in document CJ-PD (94) 7.

14. In the light of this evaluation and the conclusions of the CJ-PD, the Committee of Ministers, at its 528th meeting (7 Feburary 1995), entrusted the CJ-PD with the ad hoc terms of reference which appear above.

ii) SUMMARY OF THE WORK DONE

15. At its 34th meeting (14-17 October 1997) the CJ-PD entrusted a rapporteur, Mr A. Patijn (Netherlands), with the drafting of a report on the evaluation of the recommendation, at the end of a period of four years, in accordance with the Committee of Ministers' decision (7 February 1995).

16. The draft report, presented by the Rapporteur at the 35th meeting of the CJ-PD (25-27 March 1998 and amended by him in the light of observations made during meetings of the Bureau and the CJ-PD which followed, appears in Appendix D to this report.

17. At its 36th meeting (28-30 October 1998), the Project Group considered and approved this Final Activity Report.

APPENDICES

APPENDIX A

Report by Mr A. PATIJN, Expert of the CJ-PD from the Netherlands

Data protection and the police. Evaluation of Recommendation R (87)15 regulating the use of personal data in the police sector

1. Background

The Committee of Ministers decided to review the Recommendation R (87) 15 regulating the use of personal data in the police sector (Decision CM/547/180193). The previous evaluation was accomplished in 1994 and appears in the document CJ-PD (94) 7. In that report, as adopted by the Committee of Ministers, it was established that the Recommendation be the subject of periodic review on a regular basis every four years. A next evaluation is to be accomplished in 1998. This paper is a draft evaluation to this end. (A previous draft was circulated in March 1998.) This version deals with reactions received from Belgium, Germany, Hungary, Ireland and the Netherlands.

In the meantime, the recommendation has been referred to in two international agreements. Article 115, first paragraph, of the Schengen Agreement states that control by the supervisory authority should take account of the recommendation. The Treaty of Amsterdam incorporated the Schengen Agreement into the EU Treaty. Likewise, in its article 14, paragraph 1, the Europol Treaty provides that processing of police data should take account of the 1987 recommendation of the Council of Europe. These two references would make it a complicated affair to change the contents of the recommendation. At least formally it would imply a change of both conventions. Up till now, no serious problems have been raised that would necessitate changing the recommendation. It is proposed therefore not to revise the recommendation.

The 1987 recommendation dealt with police data as perceived in the first half of that decade. Organised crime was not yet an issue of international concern. Criminal intelligence files were not as evolved as they are nowadays. At that time, the police held mainly data about the people they suspected of having committed a criminal offence. The information remained separate from the criminal records. Recommendation R (84) 10 of the Council of Europe on the criminal record and the rehabilitation of convicted persons deals more specifically with this last topic. Things have changed since then. This raises the question of whether an additional international instrument dealing with certain specific questions in more detail would be useful

Proposal: It is proposed that the Committee of Ministers change its original decision to evaluate the 1987 Recommendation periodically, to the effect that periodically the question be answered whether any additional international instrument should be formulated.

This report mentions elements that could be relevant in answering to the question whether an additional instrument would be desirable. It proposes that the Committee of Ministers recommend that national legislators explicitly deal with certain questions of data protection, either in the national Data Protection Act, the national Code of Criminal Procedure, or national or regional Police law.

2. General Remarks

There is an inherent but inevitable tension between police powers and human rights. Adequate police powers are necessary to allow the police to fulfil their tasks. For the present paper the combating of crime is the prevailing perspective. But these powers, to be adequate, necessarily interfere with the respect for private life and should therefore be restricted to the extent that is necessary. The balance between powers necessary for the police and the restrictions necessary to protect private life shifts continually with progressing information technology. This technology enables criminals to reach their goals more effectively; on the other hand it enables the police to fulfil their tasks more effectively. If they are not properly regulated though, the new abilities of the police might again affect the private life of ordinary citizens. Article 8 of the European Convention on Human Rights requires a legal basis in this case. Practical possibilities to use new technology should be accompanied by legal powers where the use of technology by the police interferes with private life. The tension between the availability of adequate police powers and the protection of private life thus becomes a creative force generating new law to safeguard the quality of life in our changing democratic societies.

At the national level first, the legislator should be continuously aware of this challenge. The pressing social needs are a factor to be weighed. In the area of crime, these differ nationally more strongly than in other areas of society. Secondly, at an international level, one could look for possibilities to harmonise rules if there appear to be common elements in the national law of the different countries of the Council of Europe.

These general remarks are valid for all sorts of interference in private life, such as searches in premises and the interception of telecommunications. Data protection is just one of them and does not constitute an exception; nor is it something special in this respect. It is this last aspect though that is the further topic of this paper.

Proposal: It is recommended starting with a list of points of awareness for national legislators, before trying to harmonise national approaches. In due course it will be seen whether it might be desirable to regulate, at the international level, certain elements that have evolved. This work should be done in close co-operation with the CD-PC, competent in criminal matters, since both areas of law are involved.

3. Are criminal data sensitive data?

The main new developments are in the area of criminal investigation. Personal data collected and processed in the performance of other police tasks, such as the maintenance of public order or the lending of help to those that need it, have not changed much during the period of evaluation. The recommendation seems to suffice for those data. An additional instrument with regard to data collected and processed for the purpose of suppressing criminal offences might however be considered. These data are further referred to in this paper as criminal data. Hereafter, this paper deals with criminal data only.

Should criminal data be regarded as sensitive? Article 6 of Convention 108 does not mention them as such. It only states that, with regard to data relating to criminal convictions, the same applies as to the other special categories of data that are generally referred to as sensitive data. This implies that these data may not be processed unless domestic law provides appropriate safeguards. This article is, however, restricted to criminal convictions. Criminal data about persons who are not yet

convicted are not covered. One might question, though, whether in practice these data are often not even more sensitive, since no impartial tribunal has yet convicted a data subject on the basis of legally collected evidence in accordance with article 6 of the Human Rights Convention. It goes without saying that in most cases, after a conviction, a person has a right of appeal. Since somebody's position in society may be affected by data based on suspicions even more than by data based on convictions, particularly when the data become known outside the police sector, criminal data in the wider sense, are, for the purposes of this paper, regarded as sensitive.

It should be recalled that the EU Directive 95/46 has a broader approach towards criminal data. In paragraph 5 of article 8 about special categories of processing, appropriate safeguards are requested for all data relating to offences, whether they relate to convictions, to suspected persons, criminal intelligence or to any other personal data collected during the course of a criminal investigation. The directive is applicable to subjects falling under the scope of community law, e.g. insurance companies that process criminal data about persons that have tried to deceive the company. The directive, however, is, having regard to article 3, paragraph 2, not applicable to police files as such. It is relevant again, for the purpose of this paper, where the question arises whether data from processing falling under the scope of the directive, may be communicated to the police. E.g. under paragraph 6 hereafter the use of public files for police purposes is discussed. Since most public files fall under community law, the processing of the data they contain for police purposes should, within the European Union, be judged against the background of article 13, paragraph 1, under d, of the directive.

4. Several areas of law and the purpose of this paper

Recommendation No. (87) 15 on police data is intended to make the principles of Convention 108 more concrete with regard to the police sector. In most countries that have ratified Convention 108 and therefore have data protection rules in force, the police sector is covered by these general rules. Some countries have specific data protection rules for the police sector. The rules for collection of data usually find their origin in the Code of Criminal Procedure or in a specific Act regulating the police. These acts sometimes also contain rules about the use and length of storage of specific criminal data, e.g. the use and storage of data as a result of the interception of telecommunications or other intrusive investigation methods that might lead to an indiscriminate amount of personal data.

The dividing line between data protection, criminal procedure and rules organising the police, is not the same in all countries. The rules of criminal procedure differ widely between the countries while remaining within the framework of the Human Rights Convention. The level and nature of crime in member countries differ, as do their policies in criminal matters. The varying pressing social needs in the countries differ and have their legitimate influence on the regulation of police powers. It is not the task of the CJ-PD to make proposals with regard to rules of criminal procedure. This does not affect the fact that the CJ-PD is competent for the application of data protection principles in Codes of Criminal Procedure. It is neither possible nor desirable, though, to strive for a far-going harmonisation of data protection rules for criminal data. This does not affect the fact that, from a data protection perspective, in view of the on-going development of information technology and its possible threats for private life, some questions may be raised to make national legislators in either area of law, aware of these threats so they can take them into consideration in any decision either to regulate or to abstain from regulation.

5. Criminal intelligence

5.1. Scope of the concept of 'criminal intelligence'

A new phenomenon that is not specifically dealt with in Recommendation No. R (87) 15 is the area of criminal intelligence. This term is not unambiguous. Several distinctions can be made.

a. Hard data versus soft data. The police data about criminals may vary from (1) data flowing from a well established source to (2) data based on very vague indications about somebody's possible involvement with serious crime. The first category is referred to as hard data, the second as soft data. This last category may even stem from an anonymous source, resulting in complete uncertainty about its trustworthiness. The nature of the information may yet be such that storage, at least for a limited period of time, might be deemed necessary for the proper performance of the police task.

b. Data about persons suspected of having committed a specific crime or about persons about whom there are indications that they are involved in committing or preparing a serious crime, either as part of an organisation or alone. As police and judicial powers in most national Codes of criminal procedure are limited to cases where there is a suspicion against a person with regard to a specific criminal offence, new information technology is increasingly used to store data about criminals as persons as such, without relation to specific criminal offences. The data can comprise both soft and hard data, as made explicit above. It does not necessarily meet the standard of a well established suspicion against a person, a standard which must be fulfilled in order to apply the powers conferred on the police in the Code of Criminal Procedure. Nevertheless many countries collect data which may even imply the profiling of the alleged criminal, his behaviour, his contacts and his way of life without much relevance with regard to a specific criminal offence. The data are used to solve any crime, either already committed or expected to be committed in the future. Their use is not limited to the investigation of, or use as evidence in, a specific criminal offence. As long as no specific rules are foreseen in a national Code of Criminal Procedure or a (regional) police law, general data protection principles apply to these data. The term 'criminal intelligence' will for the purposes of this paper further be used in this second sense.

This implies that data are not regarded as 'criminal intelligence' if they are gathered in the course of a criminal investigation where there are reasonable grounds for a suspicion against an individual person having committed a specific criminal offence, irrespective of whether:

(1) these data are only used in the criminal case in the investigation of which they were gathered or are afterwards also used to possibly solve future crimes as well;

(2) these data have been gathered using powers granted in the Code of Criminal procedure or not.
In some countries the data cannot be used as evidence in a trial. They serve only to guide the police investigations. They might become relevant, though, during a trial if the defence challenges the way the evidence has been gathered. The legality of their storage might then be questioned since the evidence might be a fruit of the poisoned tree.

5.2. Questions with regard to criminal intelligence

There are different questions to be answered with regard to the collection and storage of criminal intelligence.

5.2.1. Who can be data-subject as part of criminal intelligence?

Since the right to respect for private life implies that not everybody can indiscriminately become the subject of criminal intelligence, the law must define the criteria for identifying the targets that can be the subject of criminal intelligence. These criteria will differ according to national law and can be criteria based on content or on procedure. Criteria based on content are, for example, the restriction to gather criminal intelligence only in cases of serious organised crime and crimes of a comparable threat to society. A criterion based on procedure is for instance that a Ministry of Justice, a Ministry of Internal Affairs, a judge or a public prosecutor, mandating the collection of criminal intelligence during a limited period of time and, if possible, within a geographically defined area about a precisely defined group of persons who are suspected of being involved or becoming involved in a specifically circumscribed area of crime. The question then to be answered is whether the mandate should be a publicly available document, either from the very beginning, or as soon as possible if the investigation can no longer be jeopardised.

5.2.2. Storage of data about persons related to targets of criminal intelligence

The principle is that data are processed relating to criminal offences about a group of persons, to be precisely defined by law, with regard to whom there is not yet any concrete suspicion on reasonable grounds of committing a specific offence. When these persons are profiled with regard to their behaviour, as far as that might be criminally relevant, it is necessary to store data about other, unsuspected persons, as well, even though they do not fit the criteria of targets of criminal intelligence. Two categories can be distinguished.

(1) persons with whom targets of criminal intelligence are in contact either physically as observed in the ordinary world or by telecommunications as observed by means of electronic surveillance of their telecom (telephone, fax, electronic mail etc), or

(2) persons who inform the police (informants, often criminals themselves): a record of all their conversations with the police and, moreover, perhaps of their own behaviour, in order to establish their trustworthiness and to keep control over the policemen that maintain the contact with informants.

The data about the persons under (1) and (2) should be kept separate from the data about the targets of criminal intelligence as they are collected for different purposes. The data under (1) should be restricted to the extent that is necessary to get a clear picture of the data-subject. The purpose of storage does not allow a profiling of these contacts themselves. The data under (2) could therefore be more extensive in order to allow in court, if contested, to judge the legality of the gathering of data (and therefore the admissibility of evidence) gathered from these informants. This can imply that the data gathered about persons under (2) are more extensive than about persons under (1), since the data are gathered for different purposes.

The different purposes also imply that decisions about queries, matching and datamining should be justified against the background of each separate set of data, taking account of the purpose for which they are processed. The purpose of the data under (1): they are meant to give information about the target of the criminal intelligence; under (2): to check the trustworthiness of the informant. Other usage of these data should be compatible with these original purposes if the use is not restricted to these purposes only. The processing by matching, combining and datamining of the data under (1) and (2), in order to find patterns of contact between criminals and establish new suspects or new targets of criminal intelligence, can be regarded as a form of compatible use. This is less evident where these data are used outside the police task, e.g. to establish somebody's

trustworthiness to fulfil a specific task outside the police. In view of article 9 of Convention 108, such use would need an explicit legal basis.

5.2.3. How long should criminal intelligence data be stored?

The law should be explicit about the duration of storage of criminal intelligence. As a direction of thought, one could think of a period of some years after the last time any relevant data has been added to the record. After this period one could think of a periodic review (as is done in article 112 of the Schengen Agreement). If, after a review, there are no reasonable grounds to justify further storage then deletion should be the rule. Data protection does not justify storage simply for the reason that you never know whether any data 'might perhaps come in handy in any unforeseeable future'. This leaves open the possibility that each review leads to the decision to continue storage, in the end possibly for an indefinite time. If there are good reasons to do so each time, this must be accepted. One could also think of a stricter system of obligatory deletion after a certain lapse of time.

5.2.4. Final remark on criminal intelligence

Any regulation of criminal intelligence only makes sense if the storage and use of criminal data about other unsuspected persons is not allowed unless for specific purposes and for short periods mentioned in the law.

Proposal: It is recommended that member States define in their domestic legislation, in a strict sense, the targets that can be subject of criminal intelligence. A time-limit for periodic review of continued storage should be made explicit in the law.

6. The data collected by the police during an individual criminal investigation

6.1. Scope of the problem

The rapid changes in information technology do not leave the police unaffected. The instruments of information technology make work more effective, both for criminals and for the police. Sometimes this means that the police, in order to do their work properly, have to collect vast amounts of data either by downloading computers during searches in premises, by intercepting (tele)communications or by searching the E-mail of criminals. Particularly criminals participating in organised crime may engage in massive storage and exchange of data in order to run their organisation. The data is sometimes collected by rather intrusive investigational methods granted to the police under the Code of Criminal Procedure. They often contain personal data in bulk, possibly completely unrelated to the crime under investigation or any other crime, but entered nevertheless into the police computers in the course of a criminal investigation. 'Unrelated' is meant in the sense that no grounds for the specific criminal investigation at hand justify the continued storage and use in the light of article 8. The storage can be justified only for the time needed to find out that they are really unrelated, unless other compatible use or other use explicitly permitted by law come in view.

6.2. Other use

To what extent are the police entitled to use this data also in other criminal investigations? What do the principles of purpose specificity and compatibility mean within this context? What are the limits of article 9 of Convention 108 to allow by law other purpose to be served by the data?

It is arguable that the data can be used to investigate new unrelated offences if it is clear from the collected data - this means: without comparing or matching with data collected in other cases - that there are enough indications to base a reasonable suspicion for this new offence. The police are obliged to notify any criminal offence they have knowledge of. It is irrelevant whether this knowledge is the result of the use of investigative powers in another, even completely unrelated case. This sort of use can therefore be regarded as compatible with the original purpose.

The next question is whether it can be used for the investigation of other related or, even more broadly, for similar offences, also in cases where from the data no reasonable suspicion can be inferred. According to some legal systems, in some cases: yes.

1. In cases where data about a suspect or even a person condemned afterwards is collected in the course of one investigation, the data about him is stored with the purpose of further usage. E.g. fingerprints and photographs, besides the nature of the offence, remain available for the solution of possible future offences. This may be regarded as compatible use. There is divergence between member States as to the necessity of deleting such data in cases of acquittal by lack of evidence though the suspicion remains. It is less questionable that these data should in principle be deleted in a case where somebody's innocence has been established or where afterwards any suspicion has been removed.

2. Data about persons other than the suspect or the convicted person collected in the course of a criminal investigation are, in principle, collected for that investigation. A use for other purposes, e.g. for a possible investigation of future criminal offences, cannot be regarded as compatible with the original use. Thus, if such use is deemed necessary, a legal basis in the sense of article 9 of Convention 108 is needed. One could think of cases where such data are used to update files about targets of criminal intelligence.

Domestic law should give explicit answers to these questions. Convention 108 seems to leave room for some digression.

6.3. Final remark

From a practical point of view, one could think of data collected in the course of a specific criminal investigation being used by the police indiscriminately in order to see whether perhaps there might be something useful in it, e.g. to solve yet unresolved criminal cases. This could however easily lead to a general power of the police to survey large portions of the population on the basis of any data once legitimately gathered during the course of a criminal investigation. If however one departs from the principle 'if there is no crime, there is no investigation', it might be questioned whether such broad use would fit the compatibility test of article 8, under b, of Convention 108. In the Campbell-case the European Court of Human Rights judged that 'the existence of facts or information (should) satisfy an objective observer' that there is reasonable cause to use such data for the purpose of combating crime (1992, 15 EHRR 137). Since the processing of criminal data, being sensitive data, could be regarded as an interference with private life, such cases need to be legitimised in the sense of paragraph 2 of article 5 of the Convention on Human Rights.
This leaves unaffected the matching, datamining and other forms of processing of personal data, if allowed by law, with regard to any existing file, whether public or established for a certain legitimate purpose and therefore restricted in its use.
Proposal: It is recommended that any power to perform a general data surveillance check or matching for the purposes of the suppression of crime on the basis of police data gathered in the course of criminal investigations on the basis of vast amounts of persons possibly completely

unrelated to any crime, be limited to specific cases described in the Code of Criminal Procedure and be granted on the basis of a specific mandate of the judiciary.

7. Datamining with other data than police data

Computing power has increased enormously. It has become possible to interconnect and compare extensive databases in order to find evidence about crime also about persons that might be completely unsuspected beforehand. In most Codes of Criminal Procedure there are powers for the judiciary to request the submission of any objects, including data carriers or data unrelated to its carrier. Most of these powers were formulated in an age where there was no practical reason to distinguish between information about one person and information about a vast amount of people. Since information technology has made the searching, the monitoring of communications and the combining of data so easy, it might be argued that from a perspective of data protection this distinction has gradually become legally relevant. It is therefore recommended that this differentiation in a Code of Criminal Procedure be made explicitly wherever it might be relevant. The submission of a vast amount of personal data in bulk for purposes of criminal investigation should be made dependent upon stricter criteria and the interpretation of these criteria in a specific case be made dependent on the decision of a more independent (judiciary) authority than the submission of data about some individual person or persons, whose identity is specified before the search is done and their data are submitted. Several situations can be distinguished.

(A) A rather recent development made possible by information technology is the collection of large amounts of personal data from open sources. From this point of view Internet and digitalized public files should be dealt with specifically.

1. The Internet allows collection of data about persons. Like everybody else, the police, if acting in the legitimate performance of their task, can consult the open sources on Internet, as well as sources from abroad. No specific power laid down in domestic legislation is needed, as these forms of consultation do not constitute an invasion into private life. Personal data about subjects that are already investigated for the purposes of a criminal investigation can thus be collected and added to the police data if they might be or become relevant for the case. This should be distinguished from the indiscriminate collection about a vast amount of persons previously unknown to the police. As everybody can perform these forms of collection, one could argue that this is not denied to the police if this is necessary for the performance of their task. A legally relevant borderline is passed though if such massive collection is matched with police files. A general matching of downloads from Internet with police files, just in order to see whether perhaps a criminal offence can be detected, could easily imply a general surveillance of large parts of the population to the extent that there is an invasion of private life without sufficient legitimate grounds. This leaves it to member States to regulate such matching specifically linked to the investigation of a specific criminal offence.

2. All countries have public files containing all sorts of personal data that can be consulted by anybody for a wide range of different purposes, e.g. the land estate register or the commercial register containing the personal data of persons involved in the management of a company. Until a few years ago it was not possible to combine these files and make queries in order to discover hitherto unknown relations. Since some of these public files become available digitally on CD-ROM or on Internet, extensive queries, according to all sorts of criteria, combining different public files, have become possible, unless specific technical measures have been taken to prevent such queries. Legislators have established a public file with the often implicit idea that some specified information about individual persons can be consulted. It is not self-evident that this implies

automatically that these files can also be made digitally accessible with the result that on the basis of the information in the file individual persons, hitherto unknown, can be found. It seems that from a data protection point of view security devices are needed to prevent the public file from being compared with other (public) files in an unlimited way. For example, a group of previously unknown persons that fulfils a predetermined set of characteristics can be identified, contrary to any purpose of any of the public files involved. Different concepts, all referring to some slightly different characteristics, have become the vogue: datamining, matching, knowledge discovery, information resource management etc.

This immediately raises the question of whether the police are allowed to compare these files mutually or with police files, for example in order to enrich these files or to detect new crimes. Again, it is proposed limiting these forms of matching to specific cases of an investigation of a criminal offence on the mandate of the judiciary, thus excluding general surveillance by the police of large portions of the population outside the situation of the investigation of a specific criminal offence. Datamining with regard to public files, or the matching of different public files, if deemed necessary in order to detect crime, should be explicitly authorised by law according to specific criteria.

(B) On the basis of article 6 of the EC Directive of 10 June 1991 (91/308/EEC) on prevention of the use of the financial system for the purpose of money laundering, there is general collection of certain data about unusual transactions for the purpose of preventing criminal offences. These data are collected for the purpose of the suppression of a specific category of crime, though about unsuspected persons, who do not fulfil the criteria of being subjects of criminal intelligence. According to this article, in principle these data may not be used for other purposes, unless explicitly permitted by law. For a specific area there is thus general data surveillance of the population for the purpose of the suppression of a specific form of crime according to specific criteria. The question to be answered explicitly by the legislator is whether, and if so to what extent, the police have access to the data thus gathered. It seems desirable that the police have at least access to the financial data thus collected about the persons already legitimately in their own files. It is less evident that these data may be indiscriminately used by the police, unless there is an explicit legal base according to certain procedures.

Proposal: It is recommended that the Code of Criminal Procedure allow for a mandate of the judiciary in specific cases if this is deemed necessary for the investigation or the ending of a specific criminal offence to match public files, financial data about unusual transactions or a download from Internet with police files.

8. Genetic data

Scientific progress in the use of DNA as a means of recognising people will increasingly lead to the importance of this tool. For that purpose many countries have or are developing DNA bases. Within the EU a transnational database is being discussed. From a data protection point of view, the following can be brought forward.

DNA is scrutinised for a number of reasons. Some persons are convicted because their DNA has been found at the place of the crime. The DNA is part of the evidence that the person is guilty. In case of sexual offenders, these data are stored and used in the investigation of future crimes. The legislator should be explicit about whether to limit the use of DNA of sexual offences, or to extend the use of the DNA bank also to petty offences, such as simple maltreatment. If the use of a DNA bank by law is limited to sexual offences, DNA found at the place of a petty offence can be used to

identify the perpetrator. It is however excluded that the DNA will be used again in the future if any DNA is found.

DNA is used to identify perpetrators of serious criminal offences. It can also happen that the DNA test leads to somebody's acquittal. The test can prove that he did not commit the offence. If a DNA test has proven that somebody is not guilty of a criminal offence (or more limited: a sexual offence), storage of the data in the DNA bank for the purpose of investigating possible future crimes should be forbidden.

In practice, it cannot be excluded that DNA of one person can be used to identify another person in the same genetic line. The legal question then arises, of whether this is permitted. E.g. the DNA bank contains DNA of a father, and his fugitive son is suspected of having committed a sexual offence, having left traces of DNA, but the DNA of the son is not available. Can the DNA of the father be used as evidence that the son has committed the crime? The legislator has to answer the question whether, from a legal point of view, there is a good reason why somebody whose father appears in the DNA bank should be an easier target for law enforcement than somebody whose relatives have not been caught by the police. One could think of limiting such use to exceptional, serious cases.

Sometimes large parts of the population are requested to co-operate for the solution of some criminal offences by making available their DNA (or other biometric data, such as fingerprints). On a voluntary basis this is possible. Other use of these data, e.g. for the solution of other criminal offences without additional consent for this other use, must be regarded as incompatible with the original purpose. This implies the deletion of the data after the investigation of the criminal offence in question has been ended.

Proposal: A multidisciplinary group within the Council of Europe will study certain problems in relation to genetic data. The group could take the questions mentioned above into account.

9. Notification

In principle, persons should be informed about the data that is collected about them, in order to enable them to seek an effective remedy against any alleged invasion of their private life (cf. article 13 ECHR). Suspects ought to be informed as soon as they are arrested of the nature and the cause of the accusation (cf. article 6 ECHR). In a hearing they will be confronted with the collected evidence. In a criminal investigation other data subjects than the suspect might become involved as well. The Klass-case of the European Court of Human Rights of 6 September 1978 (Series A, nr 28) allows for the postponement of informing the data subject as long as this is necessary in order not to jeopardise the performance of the police task. In case of criminal intelligence this exception will probably be applicable in nearly all cases.

The question arises of the extent to which persons concerned should be informed in cases of large downloads of personal data from computer systems during a search. The search as such can no longer be jeopardised, so the Klass-criterion does not apply. An exemption to the obligation to notify will in some cases be possible on the basis of a disproportionate effort. However, if persons exert their right of access with regard to the police, they will have to be informed that data about them have been collected during a search. Moreover data subjects can be informed by the system keeper of the downloaded computer. In principle, he does not have any obligation to confidentiality about the data the police downloaded from his computer. If it is deemed to be necessary that specific categories of controllers of data files remain silent towards the data subjects about the data

that the police have collected from them, this should be explicitly provided for by law. One could think of special circumstances where telecom operators or bankers, having submitted data to the police, could be obliged by law to keep this fact secret from their clients. The legislator could impose such an obligation on Internet Service Providers in cases of the investigation of electronic mail. A general duty of private persons to remain silent towards data subjects if personal data have been submitted or seized by the police must probably be regarded as a disproportionate measure.

This situation should be distinguished from the case where personal data are monitored and collected during a certain period of time on the basis of a legal mandate, e.g. the collection of traffic data in telecommunications in the future. The investigative power would be jeopardised if the data subjects that are monitored are informed beforehand. These are secretive investigative powers by their nature so the data-subject can only be informed afterwards. In these cases it can be useful if the legislator in a general sense obliges private persons on whose co-operation the police depend, to remain secret towards the data-subject at least during the period of the monitoring. After the monitoring data subjects should in principle be informed about the collection of their personal data, e.g. if their telephone conversations have been intercepted during a call with a target of an interception mandate. If this information is omitted for reasons of disproportionate effort, a possible request in the exertion of the right of access by the data subject has to be granted, unless proper performance of the police task would be jeopardised.

Proposal: It is recommended that the legislator be explicit about the circumstances under which the data subject has to be informed, either on the initiative of the police, or upon request of the data-subject. The position of private parties co-operating with the police in submitting personal data about third persons should be made clear.

10. Transborder data flows

Data collected and stored legally by the police can also be transmitted to police bodies of other countries under point 5.4 of Recommendation No. (87) 15 regulating the use of personal data in the police sector. This can be refused if there are specific rules because of the sensitiveness of criminal data or some categories of criminal data (e.g. criminal intelligence) and the other country does not have an equivalent level of protection (article 12 of Convention 108).

The communication should be to police bodies in the other country. This means that the police bodies of the receiving State, according to its domestic law, may communicate these data to government bodies for administrative purposes. This is only different if the country of origin stipulates explicitly that the data are communicated for police purposes only. Such a stipulation is, however, only effective as long as the police bodies in the receiving country do not have a legal obligation under their domestic law to communicate their data to other bodies. Receiving States should inform States of origin about such legal obligations.

The Schengen Agreement and Europol have their own data protection regime that is adequate. There seems to be no specific need to develop new instruments specific to transborder data flows of police data besides the elements already mentioned for national law, which can not avoid having their effect at the international level as well.

11. Accountability

Data protection and the effective performance of the police task are sometimes hard to reconcile. It is accepted that the police for the purpose of preventing or investigating crime need vast amounts of personal data. However, the processing of these data cannot be unlimited and should be regulated by law. In order to allow the competent authorities to legislate in a timely fashion, either to grant the police extra powers to fulfil their task, or to protect citizens against unjustified intrusions into their private lives, one could think of instruments to allow the authorities to monitor developments in this field. One of these instruments could be the obligation for the police to report about the quantity and the precise ways certain powers granted them by law are exerted with regard to the processing of personal data. E.g. one could think of an obligation to report the number of persons subject to criminal intelligence. The question is left unanswered whether this should be a secret report to the government or a public document allowing parliament to control the use of powers that might affect private life.

Proposal: National legislators should consider the possibility of regulatory instruments to monitor the use of investigative methods of the police involving the collection, storage and use of personal data.

12. Supervisory authority

The countries that have implemented the EU data protection directive 95/46/EEC did not make any substantial exception on the powers of the independent supervisory authority with regard to the police, although the directive is not applicable to police files as such. In general terms an improvement in supervision and law enforcement of data protection rules with regard to the police may therefore be expected. It is recommended that other member States of the Council of Europe establish a similar regime of supervision for police files in their countries. This would be advantageous to the unhampered international exchange between police bodies in combating international organised crime.

Proposal: Member States should establish in domestic law a system of independent supervision over police files in their countries with effective powers to enforce data protection rules in case of non-compliance.

13. Conclusion

It is proposed that the Committee of Ministers of the Council of Europe change their original decision to evaluate the 1987 Recommendation periodically in the sense that periodically the question be answered whether any additional international instrument should be developed.
The Committee could further give guidance to legislators in the Member States with regard to at least the following questions. These could be further elaborated in close co-operation with the CD-PC since the borderline between data protection, criminal procedure and police law will not be the same in all countries and many questions touch all these areas of law.

Proposals:

1. National legislators should explicitly answer a number of questions of data protection, either in the national Data Protection Act, the national Code of Criminal Procedure or the Police law.

2. Member States should define in their domestic legislation, in a strict sense, the targets that can be the subject of criminal intelligence. As a direction of thought, one could think of serious organised

crime and crimes of a comparable threat to society. A time limit for periodic review of continued storage should be made explicit in the law.

3. Any power to perform general data surveillance checks or matching for the purposes of the suppression of crime on the basis of police data gathered in the course of criminal investigations on the basis of vast amounts of persons possibly completely unrelated to any crime should be limited to specific serious cases described in the Code of Criminal Procedure and be granted on the basis of a specific mandate of the judiciary.

4. The Code or Criminal Procedure should make clear in what cases police files may be matched with public files, financial data about unusual transactions or a download from Internet.

5. The law should be explicit about the circumstances under which the data subject has to be informed, either on the initiative of the police, or upon request of the data subject. The position of private parties co-operating with the police in submitting personal data about third persons should be made clear.

6. Member States should establish in their domestic law a system of independent supervision over police files in their country with effective powers to enforce data protection rules in case of non-compliance.

7. It is recommended that any power to perform a general data surveillance check or matching for the purposes of the suppression of crime on the basis of police data gathered in the course of criminal investigations on the basis of vast amounts of persons possibly completely unrelated to any crime, be limited to specific cases described in the Code of Criminal Procedure and be granted on the basis of a specific mandate of the judiciary.

8. It is recommended that the Code or Criminal Procedure allows for a mandate of the judiciary in specific cases if this is deemed necessary for the investigation or the ending of a specific criminal offence to match public files, financial data about unusual transactions or a download from Internet with police files.

9. A multidisciplinary group within the Council of Europe will study certain problems in relation to genetic data. The group could take the questions mentioned above into account.

10. National legislators should consider the possibility of regulating instruments to monitor the use of investigative methods of the police involving the collection, storage and use of personal data.

APPENDIX B

Text of Recommendation 1181 (1992) of the Parliamentary Assembly

RECOMMENDATION 1181 (1992)[1] on police co-operation and protection of personal data in the police sector.

1. As a result of the Schengen Agreement, the European States co-operating in that agreement will proceed with the exchange of automatically processed personal data in the police sector. It is most likely that such an exchange will cover the whole of the European Community after the disappearance of frontier controls at its internal borders.

2. Nowadays there is already an intensive exchange of data in the police sector among Council of Europe member States on a bilateral or multilateral basis and through Interpol.

3. It is of vital importance for an efficient combat against international crime that it is fought at national and at European level.

4. An efficient fight against crime implies an exchange of data in the police sector.

5. In this respect it is useful to recall the Assembly's Recommendation 1044 (1986) on international crime and its plea for a European information and intelligence centre (Europol), and Recommendation No. R (87) 15 of the Committee of Ministers to member States of the Council of Europe regulating the use of personal data in the police sector.

6. It is necessary, however, that there be adequate protection of personal data in the police sector and one may note with satisfaction that the Council of Europe concluded, in 1981, a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. However, in order to be fully effective, it is not sufficient that this convention has, to date, only been ratified by eleven member States.

7. The Assembly therefore recommends that the Committee of Ministers :

i. draw up a convention enshrining the principles laid down in its Recommendation No. R (87) 15 ;

ii. promote the application of these principles in the exchange of data in the police sector between member States and between member States and third countries via Interpol. In this respect the implementation of the following principles is of the utmost importance :

a. data should be accurate, relevant, not exceed the purpose for which they are stored and, where necessary, kept up to date ;
b. they should be screened before they are stored ;
c. an individual should have the right to know whether personal data concerning him are kept ;
d. he should have an appropriate right of access to such data ;
e. he should have the right to challenge such data and, if necessary, have them rectified or erased ;

[1] Text adopted by the Standing Committee, acting on behalf of the Assembly, on 11 March 1992. See Doc. 6557, report of the Committee on Legal Affairs and Human Rights, Rapporteur : Mr Stoffelen

f. individuals who are denied access to files relating to them should have a right to appeal to an independent authority which has full access to all relevant files and which can and should weigh the conflicting interests involved ;
g. there should be an independent authority outside the police sector responsible for ensuring respect of the principles laid down in such a convention ;

iii. appeal to member States to ensure that data in the police sector may only be exchanged with other member States and with Interpol on the lines provided for in the proposed draft convention.