COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

COMMITTEE OF MINISTERS

Strasbourg, 29 July 1974

Restricted
CM (74) 171
/Addendum to
CCJ (74) 38/

EUROPEAN COMMITTEE ON LEGAL CO-OPERATION (CCJ)

Addendum

to the report on the 21st meeting of the CCJ

Draft resolution on the protection of privacy of individuals vis-à-vis electronic data banks in the public sector and draft explanatory report

(Texts drawn up by the Committee of Experts on the Protection of Privacy and revised by the CCJ at its 21st meeting)

35.971
05.2

PART I

DRAFT RESOLUTION

on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector

---

The Committee of Ministers of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its Members;

Desiring to contribute to public understanding and confidence with regard to new administrative techniques which public authorities in the member states are using in order to ensure the optimal performance of the tasks entrusted to them;

Recognising that the use of electronic data banks by public authorities has given rise to increasing concern about the protection of the privacy of individuals;

Considering that the adoption of common principles in this field can contribute towards a solution of these problems in the member states and can help to prevent the creation of unjustified divergencies between the laws of the member states on this subject;

Recalling its Resolution (73) 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector;

Bearing in mind Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms;

RECOMMENDS THE GOVERNMENTS OF MEMBER STATES:

a. To take all steps which they consider necessary to give effect to the principles set out in the Annex to the present resolution;

b. to inform the Secretary General of the Council of Europe in due course of any action taken in this field.

./.

A N N E X

The following principles apply to personal information stored in electronic data banks in the public sector.

For the purposes of this resolution, "personal information" means information relating to individuals (physical persons) and "electronic data bank" means any electronic data processing system which is used to handle such information.

1.

As a general rule the public should be kept regularly informed about the establishment, operation and development of electronic data banks in the public sector.

2.

The information stored should be:

a. obtained by lawful and fair means;

b. accurate and kept up-to-date;

c. appropriate and relevant to the purpose for which it has been stored.

Every care should be taken to correct inaccurate information and to erase inappropriate, irrelevant or obsolete information.

3.

Especially when electronic data banks process information relating to the intimate private life of individuals or when the processing of information might lead to unfair discrimination,

a. their existence must have been provided for by law, or by special regulation or have been made public in a statement or document, in accordance with the legal system of each member state;

b. such law, regulation, statement or document must clearly state the purpose of storage and use of such information, as well as the conditions under which it may be communicated either within the public administration or to private persons or bodies;

./.

c. the data stored must not be used for purposes other than those which have been defined unless exception is explicitly permitted by law, is granted by a competent authority or the rules for the use of the electronic data bank are amended.

4.

Rules should be laid down to specify the time-limits beyond which certain categories of information may not be kept or used.

However, exceptions from this principle are acceptable if the use of the information for statistical, scientific or historical purposes requires its conservation for an indefinite duration. In that case, precautions should be taken to ensure that the privacy of the individuals concerned will not be prejudiced.

5.

Every individual should have the right to know the information stored about him.

Any exception to this principle or limitation to the exercise of this right should be strictly regulated.

6.

Precautions should be taken against any abuse or misuse of information. For this reason

a. everyone concerned with the operation of electronic data processing should be bound by rules of conduct aimed at preventing the misuse of data and in particular by a duty to observe secrecy;

b. electronic data banks should be equipped with security systems which bar access to the data held by them to persons not entitled to obtain such information and which provide for the detection of misdirections of information, whether intentional or not.

7.

Access to information that may not be freely communicated to the public should be confined to the persons whose functions entitle them to take cognizance of it in order to carry out their duties.

8.

When information is used for statistical purposes it should be released only in such a way that it is impossible to link information to a particular person.

./.

PART II

DRAFT EXPLANATORY REPORT

to the resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector

---

I. INTRODUCTION

1. It is hardly necessary to emphasise how important it is that every individual in modern society is guaranteed satisfactory protection with regard to the electronic processing of data concerning him.

In the early 1960s when computers made their first appearance as administrative aids, the need to protect citizens against possible risks for their privacy did not appear to be urgent. Computers were expensive and their use was limited to a small number of public services.

In recent years, however, the need to provide adequate safeguards for the individual has become more acute as a result of two parallel and interdependent processes: the growing complexity of the social fabric and the headway made by information technology.

2. In all fields of human activity, electronic data processing has been introduced as an efficient and powerful instrument to solve complex problems. In certain fields it has already become virtually indispensable.

The advantages derived from the use of computers in the public sector are very obvious. They can help to rationalise administrative work. In relieving the administration from tedious tasks such as copying, filing, keeping records up to date, issuing certificates, documentation, etc information technology raises administrative productivity.

Information technology improves the capacity of every administration to store, process and utilise data on which its decisions are to be based. It enables, moreover, several administrations, at different levels (central, regional, local), to pool their data.

./.

Thus, automation can raise the quality of public service notwithstanding the constantly growing volume, diversity and complexity of the tasks of the administration.

3. The main applications of information technology by the public administration will vary considerably from one state to another as a result of certain considerations such as the volume of the operations, their cost, administrative traditions, technical infrastructure, etc. Among the most common uses of computer technology by the European states are to be mentioned: statistics, postal accounts, social security, personnel management, financial administration, health services, land registers, criminal records, business firms' registers, motor vehicle administration and internal revenue.

Information stored in population registers, which are now increasingly being computerised and which deserve special attention because they respond to the needs of all branches and levels of the public administration is a typical example of information used for more than one purpose.

4. The citizens who are seeing the gradual introduction of computers in public administration will form an opinion of its advantages or inconveniences. They will appreciate the speed, clarity and logic with which information is handled in administrative processes affecting them. But at times they may also be anxious about what may appear to them to be an increase in the power of the authorities as a result of computerised administration. First, there are fears that the use of computers will allow several administrations to exchange among themselves various kinds of information on the same persons and that it will be possible in this way for the state to compile and keep up to date a detailed "profile" on individual citizens. In fact, it is by no means a simple matter to build up such profiles; a number of technical difficulties stand in the way. Nevertheless, this potential capacity of modern public administration has awakened in some people a fear that their privacy is losing ground.

Furthermore, the possibility that the same information may be used for more than one purpose as a result of several parts of the administration being able to obtain access to it has led to doubts about the real purposes for which the information is required and about the confidentiality of the information stored.

5. An inherent difficulty hovering over the debate on the protection of privacy vis-à-vis public electronic data banks stems from the delicate problem of the balance of interests. Governments are confronted on the one hand by advocates of the rights of individuals who are asking for measures to secure the

./.

confidential nature of the data held by the state about citizens, and on the other hand by those who demand equal and free access of citizens to information handled by public authorities.

Public anxiety has arisen not because many abuses of information technology have actually been discovered but rather from the possibility of abuse and also from the fact that computers are being used to store certain categories of information about which individuals are traditionally sensitive.

Finally, the public is not sufficiently informed about the new information technology. The reason for this is the novelty of the medium and the fact that the public authorities have not yet adopted a firm policy with regard to it.

In the absence of general rules and of a proper information of the public, the discussion is apt to flare up on the occasion of each new project for the use of information technology. In this connection, it should be kept in mind that the success with which computers can be used in public affairs will depend very much on the degree of confidence the public is willing to give to their use.

6. In several European states initiatives have been taken in the field of protection of the individual with regard to computers, both at legislative level and with regard to information of the public. Bills for new legislation have been or are in the process of being drafted; hearings and consultations are organised and reports are produced by public and private bodies.

Since these preoccupations exist to more or less the same degree in all developed countries, they are also being discussed in several international organisations such as the United Nations, UNESCO, and OECD. Special mention should be made here of the reports which the latter organisation has published in its series "Information Studies".

II. ACTION TO BE UNDERTAKEN AT THE EUROPEAN LEVEL

7. In Europe, action in the legal and administrative field has been undertaken particularly within the framework of the Council of Europe. It should be recalled that this organisation, according to Article 3 of its Statute, endeavours to defend the rule of law and the protection of human rights. Among those rights, as set out by the European Convention on Human Rights, a place is given in Article 8 to the protection of the right to privacy.

./.

The member states of the organisation should therefore each in their own jurisdiction, see to it that this right is respected, not only in traditional fields, but also and above all, with regard to new developments.

This idea has been expressed in a series of texts emanating from the Council of Europe, such as Recommendation 509 on Human Rights and Modern Scientific and Technological Developments, Recommendation 557 on the Use of Computers in Local Government and Resolution 428 containing a Declaration on mass communication media and human rights, which were adopted by the Consultative Assembly in 1968, 1969 and 1970 respectively; Resolution No. 3 on the Protection of Privacy in view of the Increasing Compilation of Personal Data into Computers adopted in 1972 by the Seventh Conference of European Ministers of Justice as well as Resolution (73) 2 on Ways and Means of Encouraging the use of Computers in Local Government and Resolution (73) 22 on the Protection of Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, adopted in 1973 by the Committee of Ministers.

III. OBJECTIVES OF THE PRESENT RESOLUTION

8. One might leave it to the discretion of every state to develop its own rules on the issue of the protection of privacy vis-à-vis computer utilisation by public authorities. However, a number of arguments militate in favour of a common action to be undertaken within the framework of the Council of Europe.

First of all, it should be recalled that by Resolution (73) 22 a common policy with regard to electronic data banks in the private sector has already been recommended to the member states of the Council of Europe. This resolution would remain an imperfect work if the same policy were not to be followed in the public sector.

Secondly, mutual administrative assistance, which implies the exchange of information is of growing importance between the European states, both on the basis of bilateral agreements and on the basis of European conventions. Since part of the information concerned is computerised information, it is desirable that the handling of such information should be subject to a common set of rules for the different states.

Thirdly, the question at issue concerns the right to privacy which is by its very nature a matter belonging to the European public order.

./.

IV. THE PREAMBLE TO THE RESOLUTION

9. The considerations set out above are recited in the Preamble to the resolution. Furthermore, in order to avoid any misunderstanding, the Preamble reaffirms that the use of computers for purposes of public administration should in general be regarded as a positive development. The purpose of the present resolution is not to oppose such use, but to reinforce it with certain guarantees.

V. THE OPERATIVE PART OF THE RESOLUTION

10. With regard to the scope of the present resolution, the question was raised whether it was possible and indeed necessary to adopt a definition on what is understood by "public sector.

It was observed that, in view of lack of uniformity between the notions of "public sector" as they are understood in the laws of the several European states, and in view of the fact that the problem of outlining the scope of the resolution does not seem to have posed any difficulty when the private sector was examined, it seems preferable not to embark on a search for the precise boundaries of the public sector.

On the basis of such considerations and in order not to run the risk of leaving bare a zone of "non-law", it is left to the states concerned by the present resolution to fix the exact perimeters of their public sector.

It should be recalled that in all European states certain tasks are the exclusive province of public authorities. To those traditional tasks new tasks have later been added with the development from the "policeman state" to the "entrepreneur state" or the "welfare state". This development has been different from one stage to another. We may therefore conclude on the one hand that public authorities are fulfilling in certain fields (national defence, maintenance of order, justice, public finance) a special task which has no equivalent in the private sector. On the other hand, in view of the diversity existing between the states where certain functions are sometimes entrusted to the public sector and sometimes left to the private sector, it is advisable to take as a point of departure the principles already examined in the framework of the private sector. The text of the present resolution therefore has been developed along these two lines of thought.

./.

VI. DEFINITION AND TERMINOLOGY

11. Following the example of Resolution (73) 22 on the private sector, the present resolution applies solely to information on individuals, not on corporate bodies.

12. The words "to handle information" cover both the storage and the processing of data. Although there might be slight differences between the words "information" and "data", they are intended to have the same meaning where they are used in the present resolution.

13. The definition of "electronic data bank" applies to all data banks irrespective of their size and of whether they release information to third parties or not.

In this connection, attention should be drawn to the difference between the present resolution and Resolution (73) 22 concerning the private sector. The latter resolution takes into account only those data banks which actually release information to third parties. Purely internal use, such as personnel administration, is left out. With regard to the public sector, however, it is difficult to distinguish between "internal" and "external" use. As a matter of fact in those states where all branches of the public administration are regarded as forming one whole, those different branches could not be considered to be "third party" towards each other.

VII. THE PRINCIPLES

Principle No.1

14. Public concern over the use, or intended use, of data banks by the administration is to a large extent due to a lack of adequate information.

In order to solve this problem, the authorities should enable the public to keep an eye on the development of data banks by providing it, at regular intervals, with facts and figures on such questions as the nature and volume of information stored, the official purpose and the use actually made of the information, the establishment of new data banks or the abolition, merger, or modification of existing ones, the means offered to individuals to know the information and to have corrections made, etc.

./.

15. General information could be provided to the public by means of reports from a special authority or by statement from the government to parliament or the press, covering the full range of electronic data banks in the public sector.

Such public information will undoubtedly constitute an additional guarantee, reinforcing the legal protection and giving individuals an indirect control over the use of information technology by the State.

Principle No. 2

16. This principle concerns the quality of the data stored in computers.

The first paragraph lays down that the information stored should be obtained by lawful and fair means. In this connection, the question has been raised whether the collection of data and particularly the obligatory collection, imposed by public authority, should be subject to special legislation.

It was concluded that, although the rule of "fair collection" applies to all categories of data systems, the criteria for this rule should be determined according to the purpose of the particular system. Thus, for example, it is acknowledged that, in order to obtain information to fight traffic in drugs, resort may be had to means which would be considered unacceptable if used to obtain information for use in connection with a law on aid to invalids.

Furthermore, it is affirmed that the information must be accurate and kept up-to-date. Computerised information is usually regarded as being particularly accurate. Errors may cause considerable damage to the individual, particularly when a decision unfavourable to him is taken on the basis of wrong or obsolete information.

It was recognised that it may be impracticable or uneconomic to maintain statistical information to near perfect accuracy and to keep it absolutely up-to-date. In so far as information is provided by the individuals who are the subject of the information the accuracy of such information depends on the individuals themselves and it generally makes little difference to an individual if statistical records relating to him are not entirely accurate or up-to-date. It should also be borne in mind that when the purpose of the system is to analyse a certain set of facts, thate will be no question of updating..

The third element of this principle is that a limit should be imposed on non-selective collection of data; only those data which are indispensable for the completion of the task entrusted to the data bank should be retained.

./.

17. The second paragraph, a corollary of the first, aims at the proper management of computerised data. While it goes without saying that the authority in charge of the data system has a professional interest in maintaining the good quality of the information that it is keeping, it was considered proper to lay down in this paragraph the explicit obligation to control at regular intervals and at all stages of processing the accuracy of the data stored and expunge from the system any data that do not meet the stipulated conditions.

Principle N° 3

18. Although the provisions of this principle should not be disregarded when non-sensitive information is being handled, the principle deals particularly with information which is inherently sensitive (for example because it relates to the individuals' conduct in his own home, his sexual life or his opinions) or becomes sensitive in the context in which it is used (for example, police or helath).

It has been emphasised that the processing of sensitive information should be governed by special rules in view of the damage which individuals might suffer in case of misuse. It was observed that the problem concerned could be solved by introducing, after the fashion of Article 8, second paragraph of the European Convention on Human Rights, the notion of legality.

It is understood that the object of this principle could also be met by s system in which data banks according to the law require a licence.

The text of paragraph (a) lays down the principle that the existence of any data bank for sensitive information should be provided for either by an act of parliament or, taking into account the peculiar nature of the legal system concerned, by an equivalent source, such as a s ecial regulation or, as for example in British practice, a statement before parliament, or any other document made public in conformity with the specific legal system.

19. According to paragraph (b) of this principle the provisions concerning the operations of the data banks should cover from the outset both the use of the data inside the s stem and their release to other branches of the administration or to other persons or bodies in the private sector.

The provisions also cover the transmission of data for purposes of improvement, control or verification between data systems which have been set up for different ends.

20. Paragraph (c) provides for the possibility of a departure from the rule that data may only be used for the stated purpose, provided that such an exception is surrounded by legal or administrative safeguards.

Principle N° 4

21. The first paragraph of this principle deals with the time-limits for keeping and using the information.

./.

In the public sector, just as in the private sector, individuals have a legitimate interest in seeing certain kinds of information concerning them, particularly that which is harmful to them, wiped off or rendered inoperative after a certain time has passed. The words "certain categories of information" indicate that not all information needs to be affected by time-limits. There are, in fact, certain kinds of information of a personal character, such as names, birth dates, diplomas obtained, etc, which remain indefinitely valid and the retention of which is not prejudicial to individuals. It is for every state to define which categories of information may be preserved indefinitely and which time-limits are to be observed in the case of certain other categories of information.

22. However, the second paragraph makes allowance for the necessity of certain exceptions in the interests of science and of historiography. States have a special duty to preserve certain information for posterity. In that case, the mission of the state as "guarantor of continuity" must be reconciled with the interests which citizens have against the preservation of data harmful to them. Therefore, if certain categories of information may, or even must, be preserved and used for purposes of statistics, scientific research or history, safeguards must be provided to prevent the possibility of such uses affecting the privacy of the persons concerned. The data should be preserved in such a way that the identities of the people on whom information is stored can only be ascertained by the specialists carrying out the research envisaged or, in the case of other people, after an adequate period of time has elapsed.

Principle No.5

23. The effective protection of an individual against intrusions into his privacy due to improper use of data stored about him hinges on his right to know the information. It is recognised that this right may have to undergo certain restrictions, for example for reasons of state security, public order or prevention of criminal offences or in the case of information which it might be harmful to the individual himself to know (the example of the psychiatric file has been cited). However, those exceptions (which may vary from one state to another) must be strictly defined.

24. It should be noted that the exercise of the right may be limited for purely administrative reasons, for example in the case of a procedure giving general access which might involve important material-and-cost problems.

./.

A further reason for imposing certain restrictions on the exercise of the right to know the information may be that this right may in turn degenerate into a source of unjust discrimination and be harmful to individuals (as has been the case in certain states where every citizen applying for a job must present to his employer a statement of good conduct delivered by the police authorities).

25. It should be stressed that any provisions concerning the costs to be charged to the individual or the minimum periodicity of communication of the information must avoid rendering the application of the principle inoperative or discriminatory.

Principle No. 6

26. This principle deals with the measures to prevent abuse or misuse of the information stored.

A great variety of staff are usually concerned with data bank operations. Apart from civil servants there are, for example, technical staff who, although employed by a government service, may not be civil servants. Moreover, data bank operations are sometimes carried out for the government by private firms whose personnel are not government employees. For this reason it will not be sufficient simply to refer to the rules of conduct applying to civil servants, but a special body of rules should be in force for all personnel concerned, irrespective of their status.

27. Paragraph (b) refers to the measures to be taken, within the bounds of existing technical possibilities, to safeguard the security of the information stored in a data bank.

The use of information technology by public administration offers in general satisfactory safeguards with regard to the risk of abuse or misuse. Yet it is desirable to provide expressly for the availability of technical arrangements guaranteeing the security of the information stored.

Computer manufacturers and managers of electronic data banks have underlined that the present stage of development allows for a much higher degree of security than can be obtained in the case of manual registers. However, they stress that it is in the final instance up to the users to specify the degree of security which they wish to see observed.

./.

Principle No. 7

28. This principle does not apply to "neutral" information which may circulate freely and to which consequently any person can have access.

As a matter of fact, the proper functioning of public services may call for the free circulation of certain categories of information such as that pertaining to the identification of persons.

However, the definition of personal identification elements is left to the discretion of the member States. It is recalled for example that an address, which is an identifier, is considered in certain countries as a sensitive item which for that reason cannot circulate freely.

29. Access to information which may not circulate freely should be restricted within the administration solely to those persons whose functions entitle them to take cognisance of it in order to carry out their duties. This rule contains a double safeguard: not only should the person be generally entitled to have access, but in every instance his access must be justified to the task he is carrying out.

Principle No. 8

30. Attention should be called to the fact that this principle also pertains to information concerning the intimate private life of persons and information which may be a source of discrimination.

31. One of the main objects of data banks is to provide public authorities with statistical information on which they may base their decisions. The release of statistical information is therefore one of the most prevalent uses of data banks.

Statistical information is usually released in a form that people can read, such as a printed page or a microfilm. However, statistical information stored in a computer can also be made available in a form (such as a magnetic tape or disc) which can only be read by a machine and needs further processing before it can be read by human-beings. The word "released" refers to both these situations.

32. Statistical information should normally be released only in aggregate form. If person by person information is released, for example for scientific or research purposes, it should be reduced to a level where it is impossible to identity the individuals.

33. With regard to the time-limit for preservation of data used for statistical purposes it is recalled that in conformity with Principle No. 4, second paragraph of the present resolution, special measures may be taken which constitute an exception to the first paragraph of the same principle.