COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

COMMITTEE OF MINISTERS

Strasbourg, 12 July 1973

Restricted
Addendum I to
CM (73) 110
CCJ (73) 23

EUROPEAN COMMITTEE ON LEGAL CO-OPERATION (CCJ)

Addendum I

to the report on the 19th meeting of the CCJ

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

(Texts drawn up by the Committee on the Protection of Privacy and revised by the CCJ at its 19th meeting)

31.068
05.2

CCJ (73) 23
Addendum I

PART I

DRAFT RESOLUTION

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

The Committee of Ministers,

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

Conscious of the already widespread and constantly increasing use of electronic data processing systems for records of personal data on individuals;

Recognising that, in order to prevent abuses in the storing, processing and dissemination of personal information by means of electronic data banks in the private sector, legislative measures may have to be taken in order to protect individuals;

Considering that it is urgent, pending the possible elaboration of an international agreement, at once to take steps to prevent further divergencies between the laws of member States in this field;

Having regard to Resolution No. 3 on the Protection of Privacy in view of the increasing compilation of personal data into computers, adopted by the Seventh Conference of European Ministers of Justice,

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 this 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 private sector.

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

1

The information stored should be accurate and should be kept up-to-date.

In general, information relating to the intimate private life of persons or information which might lead to unfair discrimination should not be recorded or, if recorded, should not be disseminated.

2

The information should be appropriate and relevant with regard to the purpose for which it has been stored.

3

The information should not be obtained by fraudulent or unfair means.

4

Rules should be laid down to specify the periods beyond which certain categories of information should no longer be kept or used.

5

Without appropriate authorisation, information should not be used for purposes other than those for which it has been stored, nor communicated to third parties.

6

As a general rule, the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information.

7

Every care should be taken to correct inaccurate information and to erase obsolete information or information obtained in an unlawful way.

8

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

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.

9

Access to the information stored should be confined to persons who have a valid reason to know it.

The operating staff of electronic data banks should be bound by rules of conduct aimed at preventing the misuse of data and, in particular, by rules of professional secrecy.

10

Statistical data should be released only in aggregate form and in such a way that it is impossible to link the information to a particular person.

CCJ (73) 23
Addendum I

PART II

DRAFT EXPLANATORY REPORT

Introduction

1. It is generally recognised that the development of modern science and technology, which enable man to attain an advanced standard of living, brings in its wake certain dangers threatening the rights of individuals.

This is the case, for instance, with the utilisation of new techniques for surveillance or observation of persons and for compiling and processing data pertaining to them.

2. A survey, conducted in 1968-70 by the Committee of Experts on Human Rights of the Council of Europe, on the legislation of the member States with regard to human rights and modern scientific and technological developments, has shown that the existing law does not provide sufficient protection for the citizen against intrusions on privacy by technical devices. Generally, the existing laws touch upon the protection of privacy only from a limited point of view, such as secrecy of correspondence and telecommunications, inviolability of the domicile, etc. Moreover, the ramifications of the concept of privacy have never been clearly established.

It is also doubtful whether the European Convention on Human Rights, Article 8 (1) of which guarantees to everyone "the right to respect for his private and family life, his home and his correspondence", offers satisfactory safeguards against technological intrusions into privacy. The Committee of Experts on Human Rights has noted, for example, that the Convention takes into account only interferences with private life by public authorities, not by private parties.

3. A particular new source of possible intrusion into privacy has been created by the rapid growth and popularization of computer technology. The purposes which computers are increasingly serving in the public and private sectors are by themselves not basically different from those served by more traditional forms of data storage and processing.

What is setting computers apart from the traditional means of data storage and processing is the extraordinary ease with which they have overcome at a stroke a whole series of problems raised by the management of information: the great volume of data, the techniques for their storage and retrieval, their transmission over large distances, their correct interpretation and, finally, the speed with which all these operations can be performed.

./.

CCJ (73) 23
Addendum I

Thus, computers permit the building up in the form of "data banks", of data collections or integrated networks of data collections. These data banks are capable of providing instantly and over large distances massive information on individuals.

While few would deny the great advantages offered by the application of electronic data processing techniques. there is a growing concern among the public about the possibility of improper use being made of sensitive personal information stored electronically.

It is, for example, much more difficult for an individual to take steps to protect his personal interests vis-à-vis a computerised information system than it is with regard to a traditional data register. Moreover, data concerning him which are by themselves inoffensive may be correlated in such a way that their availability becomes a threat to his private interests.

4. Parliaments and governments, as well as private groups and associations, in several member States of the Council of Europe are now considering, and introducing, new legal principles and instruments with a view to resolving the difficulties arising in this field.

In addition to these efforts at the national level, initiatives at the international level have also been taken. These initiatives are based in the first place on the realisation that the problem is likely to present itself in more or less the same manner in different countries. Consultation between States at the international level will enable them to profit from each other's experiences. In the second place, certain aspects of the problem can only be satisfactorily solved by a concerted intergovernmental action (for example problems arising from the facility of transmission of data between computers and computer terminals installed in different States). Thirdly, it seems highly desirable that, whenever possible, common norms should be adopted in all member States, based on the idea of a "European public order".

The action taken at the European level

5. In 1971, a Sub-Committee of the European Committee on Legal Co-operation (CCJ) was charged with studying the civil law aspects of the right to privacy as affected by modern scientific and technical devices.

./.

This Sub-Committee took note, inter alia, of Recommendation 509 (1968) of the Consultative Assembly on Human Rights and Modern Scientific and Technological Developments. It also studied the report drawn up by the Committee of Experts on Human Rights mentioned in para. 2 above. It concluded that the protection of privacy vis-à-vis electronic data banks should be given priority. Acting in accordance with this advice, the Committee of Ministers set up a Committee on the Protection of Privacy vis-à-vis Electronic Data Banks, charged with taking appropriate action in this field.

6. This Committee held three meetings in 1972 at which it first examined the question whether the problem of data privacy could be dealt with at the level of the Council of Europe, taking into account that the technological and legal situation was quite different from one member State to another. In the big industrial States of Europe, electronic data banks are rapidly gaining in importance, while in the smaller, less industrialised States they play a minor role. The Committee recognised the importance of these differences but thought that their effect might be lessened by the elaboration of minimum standards which might serve as guidelines for the legislatures of the member States.

The Committee next discussed the priorities. It decided to give priority to the study of problems arising in the private sector, since it was of the opinion that this sector is distinctly international and that a lack of efficient national controls might weaken the position of individuals. In this respect, the Committee found itself supported by, and in complete agreement with, Resolution No. 3 of the Seventh Conference of European Ministers of Justice, held at Basle from 15 to 18 May 1972, on "Protection of privacy in view of the increasing compilation of personal data into computers".

The proposals of the Committee of Experts were examined by the CCJ, with the assistance of a Sub-Committee, at its 18th and 19th meetings (1972-73).

The current legal situation in Europe

7. The Committee reviewed the current legal situation in the various member States and was informed that in several countries, committees had been appointed to study the problem and to propose appropriate measures to the governments. The reports and materials published by these committees contain a wealth of information about the problem of data privacy and about suggested solutions. The Committee also received valuable information about the legal situation in the member States of the OECD.

./.

CCJ (73) 23
Addendum I

8. So far, very few member States of the Council of Europe have enacted legislation on data privacy. However, several important laws and bills, regulating the problem in whole or in part, provide an indication of possible solutions. Of particular interest are the Law on Data Protection enacted in 1970 by the Land of Hessen (Federal Republic of Germany), the Belgian Bill (1972) on Data Processing Control, and the Swedish Data Act (1973). The Committee's attention was also drawn to the United States Fair Credit Reporting Act of 1970, which provides an interesting model.

European principles concerning data processing

9. Basing itself on the study of these materials, the Committee elaborated a set of principles concerning the protection of the privacy of personal information vis-à-vis electronic data banks in the private sector which might be implemented in the national laws of member States.

The Committee emphasised that threats to privacy may arise not only from the use of computerised information systems, but also from other kinds of data collections. Consequently, it is likely that some member States will adopt new regulations applicable both to electronic and manual data collections. In any case, governments should take care that the introduction of new rules on electronic data processing should not have as a side effect that modernisation of administration becomes more difficult.

10. With regard to the legal instrument(s) to be adopted in this field, the Committee thought that preference should be given to a recommendation of the Committee of Ministers to the governments of the member States, since it is necessary to take into account both the rapid development of computer technology and the urgency for European action before new divergencies arise between the laws of the member States. To that end the present draft resolution has been drawn up.

At a later stage, an international Convention might possibly be concluded for a specific field where a binding uniform instrument is considered to be necessary. In the opinion of several experts, such a Convention might be a particularly efficient way of coping with the problem of transnational data banks.

Due note has been taken of the wish expressed by the representative of the OECD to the Committee, that the European instrument would be drawn up in such a form as not to exclude the accession to it by non-member States.

In the Committee's opinion, there should also be further consideration of the extent to which the principles contained in the present Resolution, or other principles, could be applicable to electronic data banks in the public sector.

Implementation of the Resolution by the member States

11. The Committee noted that the manner in which the general principles pertaining to electronic data banks might be implemented in member States would probably differ from one State to another. In some States, for example, a special law on computer privacy might see the light while in other States preference might be given to general legislation on the privacy of personal information. Likewise, supervision by the public authorities over the storing, processing and dissemination of computerised information might either take the form of a licensing system or a public register of data banks handling personal information.

For these reasons, it was felt prudent only to formulate general principles and to leave it to the discretion of member States to decide in which fields and in what manner these principles should be implemented.

Definitions and terminology

12. "This Resolution is concerned only with individuals (physical persons), not with legal persons (corporate bodies).

It is true that electronic data processing can be harmful not only to individuals but also to legal persons. However, the problem presents itself in the latter case differently and is less acute. For these reasons it was decided to restrict the scope of the present Resolution to individuals.

However, to the extent that governments might consider it useful, nothing will prevent them from drawing inspiration from the Resolution, or parts of it, for the protection of legal persons.

13. As the Resolution refers to electronic data banks which actually disseminate information (see paragraph 16), it will not normally apply to electronic data banks which are used only for internal purposes, such as a personnel administration. If, however, at a later stage, such a bank does disseminate information, it will be covered by the Resolution.

It is left to the discretion of the member States whether they wish to extend the principles set out in the Resolution to all electronic data banks, even to those which are used only for internal purposes.

14. The Resolution covers all data collections, irrespective of their size. It should be pointed out in this connection that computer technology makes it possible to link several small data banks into one big data bank.

./.

15. It seems useful to underline that the principles contained in the Resolution are addressed both to the authorities who are competent to regulate and supervise the data banks and the owners and users of the data banks.

Data banks themselves have no uniform legal status, but may be organised in different ways. The data processing equipment (hardware) and techniques (software) are usually sold or leased by the manufacturers to data processing centres which contain the data banks. Sometimes the user of the data banks is also the owner and operator of the centre. In most cases, however, the centre is managed by a separate organisation which has its own operating staff and provides computer facilities to several organisations with data banks. Those responsible for these data banks, referred to as users (credit bureaux, mailing list firms, etc.) may, in their turn, serve their own clients or members (e.g. a credit bureau selling information to banks).

16. The word 'handle' in this context covers both storage and processing.

'Dissemination' indicates any transfer of information by a user to a third party, for example by a credit bureau to a bank.

Although there might be slight nuances, 'information' and 'data' can be used as interchangeable words."

Stages of data processing

17. Data bank operations consist of the successive stages of storing, processing and disseminating the data.

Although the gathering of information prior to its recording does not form part of the actual data bank process, it is taken into consideration in principles 3 and 7.

Principle 1 - Quality of the information stored

18. Computerised information can give a semblance of special reliability. Mistakes may cause serious damage, because of the intensive use that can be made of the data.

19. Examples of information concerning a person's intimate private life are: information about his behaviour at home, his sexual life, his opinions, etc. An example of information which may lead to unfair discrimination is that about his state of health, or his past criminal record.

The text of this principle makes a distinction between the keeping and the release of this kind of information. Even though in general it is not allowed to record such information, there may be exceptions to this rule, for example in the case of a counselling agency for alcoholics, or of a political party. In such cases the dissemination of the information is not allowed, however.

./.

Principle 2 - The purpose of the information

20. This rule implies, first of all, that computerised information should serve a specific purpose. However, it is not appropriate to lay down in an international instrument criteria as to what purposes should be permissible.

In general, a consequence of the freedom of the individual is that any purpose is allowed save when explicitly forbidden.

21. The principle laid down here applies both to the quantity and the quality of the information. The information should not be excessive in volume, i.e. more than is strictly necessary for the task.

A rule concerning the volume of the information is necessary in view of the capacity of electronic data banks to absorb an almost unlimited quantity of information, to preserve it indefinitely, to hand it out instantly and to link scattered information. By way of illustration it may be mentioned that currently the most popular form of storage, which will allow the retrieval of data in an average of 30/1000ths of a second, is on magnetic disk. Each disk contains 100 million characters, or 200 million numeric digits of information. The major banks in Britain hold approximately 25,000 million characters "on-line" on disks for essential overnight processing.

Users of electronic data banks have a material interest to store in one single operation the optimum amount of information, both information for immediate use and information for later use. Although normally electronic data banks contain only such amounts of information as are economically justifiable, it seems advisable to adopt a rule which would halt unbridled hoarding of data.

Principle 3 - Ways in which the information is obtained

22. It was deemed necessary to lay down a rule on the way in which the information may be gathered, in order to prevent the use of improper methods.

This safeguard is reinforced by principle 7.

Principle 4 - Period during which the data should be kept

23. Rules governing the period during which the information may be kept, in accordance with its character, may be laid down both by law or by the user of the data bank. In both cases, the computer can be so programmed as to erase the pertinent information automatically when the terminal date is reached.

./.

This principle is not intended to apply to certain categories of information, which remain indefinitely valid, such as names, birth dates, diplomas or other qualifications acquired by a person.

24. The Committee of Experts did not wish to go so far as to recognise a formal "right to oblivion". It is intended, however, to protect individuals from unreasonably long retention of data that could be harmful.

25. It was felt desirable to employ both words "kept" and "used". Retention of information even if not intended for use, presents a certain risk (for example, in case of accidental leaks.).

Principle 5 - Authorised use of information

26. This principle spells out the rule to be observed with regard to the use of information. There is a certain risk that the user of a data bank, in order to pay off the cost of storing data, might try to find new applications for which the data in his possession could be used. If such applications were to go beyond the original purposes for which the information had been compiled a violation of the right of the persons concerned to privacy might ensue.

27. It is to be observed that the word "authorisation" has a wide meaning in this context. It may include simply the consent of the persons involved but also a licence from a controlling authority, or a general permission granted by law.

28. The notion "third parties" is to be taken in the meaning it has in the national legal system concerned.

Principle 6-Informing the person concerned

29. This principle seeks to establish a balance between the legitimate interests of the individuals concerned and the general interests served by electronic data banks. It was drafted after due consideration of the following questions:

(a) whether an individual should have the right to be informed of the nature of the data stored on him;

(b) whether he should have the right to be informed of the actual data stored on him;

(c) whether he should have the right to be informed of the use of the data stored on him and, particularly, of any provision of information that has taken place;

(d) whether there should be any duty for those responsible for the data bank to keep an individual informed about the data held concerning him;

./.

30. The Committee thought that the questions at (a), (b) and (c) above should be answered, in principle, in the affirmative. Some provision for a person to learn what information is held about him was considered to be an essential minimum element in the protection of privacy. However, there are cases in which knowledge about certain kinds of information, such as a medical or psychiatric file, may be harmful to the individual.

31. The question posed under (d) has been answered in the negative. The Committee recognised that it would be appropriate to expect the individual to acquaint himself at the data bank about the information held concerning him.

In many cases, a person will have very little interest in knowing what information is stored about him. Moreover the provision of automatic print-outs might harm the cause of privacy (e.g. because print-outs may get misdirected in the mail); finally, a general right of print-out might unreasonably hamper the development of data processing, for it could place a heavy burden on the users.

32. The principle is likely to be supplemented by national legislation. This legislation may lay down certain rules about the times at which information should be given to the persons concerned, and about the cost thereof.

Credit bureaux, for example, whose purpose it is to sell the information collected by them, may be allowed to charge a fee even in cases of obligatory release of information.

Principle 7 - Correction and erasing of the information

33. This principle is a corollary of principles 1, 3 and 4. It is addressed to the users of electronic data banks in the private sector. Normally, these have a commercial interest vis-à-vis their clients to have correct and up-to-date information in their possession. Nevertheless it was felt to be useful to confirm by this principle the duty of the data bank user to ensure the observance of these principles by checking regularly the state of the data in his possession. This control should be carried out at all stages of data processing.

With regard to the erasure of obsolete data, it was remarked that those responsible for data banks should pay attention not only to the ageing of data after their storage in the computer, but also to storage of data which were already obsolete from the outset.

Principle 8 - Measures to prevent abuse

34. The first paragraph lays down a general principle, applicable not only to the technical requirements of security, but also to other requirements, for example with regard to the organisation of the data bank and the selection of staff.

./.

35. The second paragraph deals in more detail with the technical safeguards. It is addressed mainly to the manufacturers of hardware and software and to the personnel of the computer centres. It refers to the technical facilities to be installed, within the limits of the present state of computer technology, in order to guarantee the security of the information stored in the data bank.

Computer manufacturers and data bank managers have stressed the fact that present computer technology provides an advanced degree of security which is much more effective than that obtained by manual data systems. However, they admit that in the final instance it is the users who determine the degree of security they wish to see observed.

Principle 9 - Access to the information

36. The first paragraph lays down in general terms which are the persons entitled to have access to the information. Those persons can be divided into two categories:

(a) the operating staff of the electronic data banks (programmers, systems analysts, etc.)

(b) the users and their clients.

With regard to category (a), the data bank personnel, it is generally recognised that they should be bound by a code of ethical professional conduct. This requirement has been set out in the second paragraph of the principle.

The way in which the relevant rules are elaborated may vary from country to country. In certain cases such rules may be laid down by law. In other cases they may be left to the private organisations concerned. It was noted that in several countries rules of professional conduct are already being formulated as the medium itself develops, both by individual data processing centres and by data processing societies.

With regard to category (b), the users and their clients, they should, in compliance with the rule set out in the first paragraph, take special care to guard against unauthorised access.

It is further noted that, under certain circumstances, a third category of persons may get access to the information, viz. the personnel working in the environment of the data banks (cleaning and maintenance staff, doormen, etc.). Their function, however, is not directly related to the operation of the data bank. For that reason the Committee thought it unnecessary to suggest that this category should be placed under special obligations. Damage resulting from their acts can be dealt with under the ordinary rules of law.

./.

Principle 10 - Statistical data

37. On this principle an advisory opinion was obtained from the International Statistical Institute.

One of the main purposes of the data bank is to provide managers with statistical information which will enable them to make executive decisions. Thus the production of statistical information from data banks is a common practice.

Normally, statistical data are diffused in published form. However, computerised statistics may also be made available unpublished, for example by transfer of tapes. Owing to the special facility of computers to trace correlations, the latter form of diffusion of statistical data may also create certain dangers to privacy. The word "released" covers all forms of diffusion.

Final Observations

38. In the framework of the examination of this draft Resolution the question arose whether there should be a separate principle providing for the creation of sanctions in either civil or penal law to ensure observance of the ten principles.

It was felt, however, that the possibility of laying down such provisions, in civil, penal or administrative law should be left to the discretion of member States. For this reason it was decided to draw up the operative part of the Resolution in flexible terms, which, while calling for compliance with the principles set out therein, leaves it to the member States to choose the manner of application which most conforms with their domestic situation.