UNITED NATIONS

ECONOMIC AND SOCIAL COUNCIL

Distr.
GENERAL

E/CN.4/1142
31 January 1974

ORIGINAL: ENGLISH

COMMISSION ON HUMAN RIGHTS
Thirtieth session
Item 4 of the provisional agenda

HUMAN RIGHTS AND SCIENTIFIC AND TECHNOLOGICAL DEVELOPMENTS

Uses of electronics which may affect the rights of the person and the limits which should be placed on such uses in a democratic society

Report of the Secretary-General

CONTENTS

CONTENTS (continued)

/...

CONTENTS (continued)

/...

INTRODUCTION

1. In paragraph 1 of its resolution 2450 (XXIII) of 19 December 1968, on human rights and scientific and technological developments, the General Assembly invited the Secretary-General to undertake, with the assistance of the Advisory Committee on the Application of Science and Technology to Development among others, and in co-operation with the executive heads of the competent specialized agencies, a study of the problems in connexion with human rights arising from developments in science and technology, in particular from the following standpoints:

> "(a) Respect for the privacy of individuals and the integrity and sovereignty of nations in the light of advances in recording and other techniques;
>
> "(b) Protection of the human personality and its physical and intellectual integrity, in the light of advances in biology, medicine and biochemistry;
>
> "(c) Uses of electronics which may affect the rights of the person and the limits which should be placed on such uses in a democratic society;
>
> "(d) More generally, the balance which should be established between scientific and technological progress and the intellectual, spiritual, cultural and moral advancement of humanity."

2. The Assembly requested the Secretary-General to prepare, on a preliminary basis, a report comprising a summary account of studies already made or in progress on the aforementioned subjects, emanating in particular from governmental and intergovernmental sources, the specialized agencies and the competent non-governmental organizations; and a draft programme of work to be undertaken in fields in which subsequent surveys would be necessary for the attainment of the objectives of the resolution; and to submit that report to the Commission on Human Rights for consideration and transmittal, through the Economic and Social Council, to the General Assembly.

3. At its twenty-seventh session, the Commission considered the preliminary report (E/CN.4/1028 and Add.1-6 and Add.3/Corr.1 and 2) and adopted, on 18 March 1971, resolution 10 (XXVII).

4. In the preamble of the resolution, the Commission stated that the information and conclusions of the preliminary report of the Secretary-General

> "reveal that the protection of the rights proclaimed in article 12 of the Universal Declaration of Human Rights against arbitrary interference and attacks, which have already increased with the use of various recording techniques, electronics and data processing systems, has already been sufficiently studied for the United Nations to make a more detailed investigation of the various aspects of the subject".

5. In the operative part of the resolution, the Commission recognized the need during the Second United Nations Development Decade to concentrate its attention on the most important and basic problems of protecting human rights and fundamental freedoms in the context of scientific and technological progress, and in particular on:

> "(a) Protection of human rights in the economic, social and cultural fields in accordance with the structure and resources of States and the scientific and technological level they have reached, as well as protection of the right to work in conditions of the automation and mechanization of production;
>
> "(b) The use of scientific and technological developments to foster respect for human rights and the legitimate interests of other peoples and respect for generally recognized moral standards and standards of international law; and
>
> "(c) Prevention of the use of scientific and technological achievements to restrict fundamental democratic rights and freedoms."

6. The Commission requested the Secretary-General to continue his study of the consequences, for the observance of human rights, of current developments in science and technology, taking into account also the possibility of using them to improve living conditions and the enjoyment of economic, social and cultural rights.

7. It requested Governments to submit to the Secretary-General any material they might have on problems arising in connexion with the protection of human rights within the context of scientific and technological progress, including information on the problems mentioned in paragraph 5 above, and on the development of legislation, court decisions and national practice and any projects they had in view in connexion with the matters dealt with in the resolution. It moreover requested the specialized agencies and the International Atomic Energy Agency to submit to the Commission, through the Secretary-General, a report on the above-mentioned problems in relation to those human rights which fall within their competence; requested other intergovernmental organizations, especially regional organizations, to transmit to the Secretary-General their comments and observations on these problems; and requested the non-governmental organizations in consultative status with the Economic and Social Council to transmit any communications they considered relevant to these problems.

8. The Commission further requested the Secretary-General, bearing in mind the information received from Governments and in the light of the discussions at the Commission's twenty-seventh session, to supplement his studies so as to present a balanced picture of all basic problems arising in connexion with the exercise of human rights and fundamental freedoms in conditions of scientific and technological progress; and to submit to the Commission one or more reports, in fields where sufficient documentation and studies were available, which could be used "as a basis for exploring the possibility of preparing international

instruments designed to strengthen the protection of the human rights proclaimed in the Universal Declaration of Human Rights".

9. At the twenty-ninth session of the Commission, the Secretary-General submitted the first report in a series relating to the subjects mentioned in paragraph 1 of General Assembly resolution 2450 (XXIII). The report (E/CN.4/1116 and Add.1-3 and Add.3/Corr.1 1/) dealt with "respect for the privacy of individuals and the integrity and sovereignty of nations in the light of advances in recording and other techniques" (paragraph 1 (a) of General Assembly resolution 2450 (XXIII)).

10. Paragraphs 14-23 of document E/CN.4/1116 describe the response of Governments, specialized agencies, regional intergovernmental organs, certain other intergovernmental bodies, non-governmental organizations and other sources to the requests for information made in preparation for the preliminary report, E/CN.4/1028 and addenda, or in pursuance of Commission resolution 10 (XXVII). Some of the information received was used in preparing the present report.

11. This report, the second in the series mentioned above, was prepared by the Secretary-General in implementation of paragraph 1 (c) (on uses of electronics which may affect the rights of the person, quoted in paragraph 1 above) of General Assembly resolution 2450 (XXIII), keeping in mind Commission resolution 10 (XXVII). Various electronic devices have been referred to in document E/CN.4/1116, paragraphs 75-178, E/CN.4/1116/Add.1 and E/CN.4/1116/Add.3 (and Add.3/Corr.1), dealing with respect for the privacy for individuals and the integrity and sovereignty of nations in the light of advances in recording and other techniques. In the present report, attention is given mainly to various uses of the computer as a specific electronic device. Part one (E/CN.4/1142, paras. 1-320) of the report deals with "computerized personal data systems", that is, with the use of computers for storing, retrieving and disseminating information related to individuals. Part two (E/CN.4/1142/Add.1, paras. 1-92) deals with the use of computers in policy-making and management processes ("decision-making"), not based on storage of personal information, such as model building and certain direct monitoring operations. Part three (E/CN.4/1142/Add.1, paras. 93-102) and part four (E/CN.4/1142/Add.2) present further uses of computers and other electronic devices, which have an impact on human rights: electronic automation and electronic communications techniques.

12. In view of the preparation of the present report, the Secretary-General, on 8 December 1972, addressed a special request to Governments of States Members of the United Nations or of the specialized agencies for information concerning the use of computers in various fields of public and private activity and the various purposes for which computers were used. The Governments were further invited to communicate their views as to the benefits society might derive from the use of computers, the actual and possible threats to human rights arising from their use, and the legal, technical, professional or other existing or proposed safeguards to protect the rights of the individual. In this connexion, the Governments were also invited to transmit the text of laws, draft laws, implementing regulations, court rulings and model codes dealing with the use of computers.

1/ Addendum 4 of the report is before the Commission at its thirtieth session.

13. As of 30 November 1973, information had been received from the following Governments: Australia, Barbados, Belgium, Canada, Cyprus, Denmark, Gabon, Federal Republic of Germany, Italy, Jamaica, Khmer Republic, Kuwait, Philippines, Rwanda, Singapore, Sweden, Trinidad and Tobago, Ukrainian Soviet Socialist Republic, Union of Soviet Socialist Republics and United Kingdom of Great Britain and Northern Ireland.

14. Special requests for information and views were also sent, on 22 December 1972, to the International Labour Organisation, United Nations Educational, Scientific and Cultural Organization, World Health Organization and Universal Postal Union and, on 17 January 1973, to a number of non-governmental organizations. Information or views were supplied by the International Labour Organisation, the Universal Postal Union and the World Health Organization, and by the following non-governmental organizations in consultative status with the Economic and Social Council: Category II: Centro de Investigación para el Desarrollo Económico Social; Federation for the Respect of Man and Humanity; International Association of Penal Law; International Institute of Administrative Sciences and World Confederation of Organizations of the Teaching Profession; Roster: Battelle Memorial Institute and World Medical Association. Further material was collected for the present report by research independent of these requests.

PART ONE. COMPUTERIZED PERSONAL DATA SYSTEMS

I. THE NATURE OF COMPUTERIZED PERSONAL DATA SYSTEMS

15. In order to present more clearly the topics dealt with in this chapter, it is necessary briefly to describe computers and the definition and classification of computerized personal data systems.

A. Brief description of computers and the operations they perform

16. A computer is an electronic device intended to process information or data. By its utilization, the manual, mechanical and punched-card methods of data processing have been supplemented by electronic data-processing (EDP) or, in an equivalent terminology sometimes used, automated data-processing (ADP) methods.

17. There has been an attempt to give a legal definition of "data processing", in the draft bill on protection against the misuse of personal data in data processing (Federal Republic of Germany, 1972). 2/ According to the draft, "data processing" means in particular the storage, modification, communication and erasure of data. 3/

18. In order to perform the operations of data processing, the computer is provided with technical means of accepting information (input), 4/ of storing information (memory) and of processing the information (central processing unit or central processor) and with an output 5/ device. The equipment for performing these operations (that is, the physical or mechanical component parts of the computer) is called hardware. The major components of a computer system are: (a) input equipment: card readers, punched tape readers, keyboards document readers; (b) central processor: the unit that carries out the logical and arithmetical operations; (c) memory: devices for storing both data and instructions on how to process the data; magnetic cores, magnetic discs or magnetic tapes are examples;

2/ The text of the draft bill in German, and in English (Council of Europe, Information document of 26 January 1973, EXP/Prot.Priv./EDB13(73)2), was furnished by the Government of the Federal Republic of Germany on 14 March 1973. For details of the draft, see paragraph 195 below.

3/ According to one definition, "data processing" means "any operation or combination of operations on data to achieve a desired result" (Robert R. Arnold, Harold C. Hill, Aylmer V. Nichols, Modern Data Processing, (New York, John Willey and Sons, 1969), p. 361).

4/ "Input" is also used for "any information transferred into the internal storage of a data-processing system, including data to be processed or information to help to control the process" (ibid., p. 363).

5/ "Output" is also used for the "information transferred from the internal storage of a data-processing system to any device external to the system" and "also the results of operations performed on the data in data processing" (Ibid., p. 365).

(d) output equipment: line pointers, plotters or display devices. In contrast to hardware, the various general and specific sets of instructions specifying the sequence of operations to be performed (the computer's programme) are called software.

19. The continuous progress of computer technology led to the creation of a "time-sharing" system, by connecting several input-output terminals (consoles), 6/ to the same central processing unit and programming it in such a manner as to allow several users to utilize the system simultaneously or with imperceptible delays for performing various operations involving input, output and processing of data.

20. A further development in the same direction was the moving of the input-output terminals to remote locations, in the same or other countries and linking them with the computer by communications channels. This "remote access time-sharing system" produced, in many cases, a computer equivalent of a communications network.

21. The development of computer technology has thus permitted enormous increases, compared with the capacity of manual or other methods of data processing, in the quantities of data that can be processed, stored, retrieved, 7/ centralized and disseminated. The following has been said, summarizing the capabilities of computers in contrast with manual files:

> "Compared to manual files, computers offer greater storage capacity for data; greater speed of processing; lower processing cost per item of information; greater capacity for complex logical operation; simultaneous access to multiple records; ability to link data on the same person, place, or thing from different files; remote access to central facilities for input and output; and the ability to exchange information with other computer systems." 8/

22. The capacities of the computer are likely to grow even more as the result of

---

6/ A terminal or console is an input-output device intended for the user to interact directly with the computer (Stanley Roghman and Charles Nosmann, Computers and Society (Chicago, Science Research Associates, 1972), p. 325).

7/ "Information retrieval is the name applied to processes that recover or locate information in a large collection of data base" (ibid., p. 327).

8/ Alan F. Westin, "Civil liberties and computerized data systems", Computers, Communications and the Public Interest, Martin Greenberger, ed. (Baltimore and London, John Hopkins Press, 1971), p. 157.

new developments in data processing, hardware and software techniques. 9/ For example, the advances in integrated circuit technology are continuously reducing the cost and size per bit of storage capacities. Also, new programmes are continuously being developed based on more and more efficient algorithms, for sorting, merging and retrieval of information. As another example, the development of scanning devices for computerized information which will greatly enhance the possibility of selectivity in information retrieval could be mentioned.

23. With respect to the development of computerized record keeping in the United States, it has been estimated that there will be 500,000 computers (including minicomputers) at the close of the 1970s, compared to the 90,000 in use in 1971. 10/

B. Definition and classification of computerized personal data systems

24. The expression "computerized personal data system" is used in this report to include all forms of computer-based collections of personal data. The expression has been adopted because there is no generally accepted definition of "data banks", a term frequently used in relation to problems arising for human rights from the uses of computers. As had been remarked:

> "No standard definition exists of data banks. It has been used by organizational and civil liberties spokesmen to describe just about any large or small assemblage of data about people or things, sometimes in wholly manual form and sometimes computerized." 11/

9/ For detailed descritpions of further developments in computer technology, see Privacy and Computers, Report of a Task Force established jointly by the Department of Communications and the Department of Justice of the Federal Canadian Government (Ottawa, Information Canada, 1972), hereafter referred to as Canada, Privacy and Computers, p. 9 (The report was furnished by the Government of Canada on 23 January 1973); Arthur R. Miller, The Assault on Privacy: Computers, Data Banks and Dossiers, (Ann Arbor, University of Michigan Press, 1971), pp. 11-16; Databanks in a Free Society: Computers, Record Keeping and Privacy, Report of the Project on Computer Databanks of the Computer Science and Engineering Board, National Academy of Sciences, Alan F. Westin, Project Director, Michael A. Baker, Assistant Project Director (New York, Quadrangle Books, 1971) (hereafter referred to as "United States, Report of the National Academy of Sciences"), pp. 319, 324-330.

10/ United States, Report of the National Academy of Sciences, p. 330.

11/ United States, Report of the National Academy of Sciences, p. 229. See also Guy Braibant, La protection des droits individuels au regard du développement de l'informatique, report presented at the First Franco-Nordic Law Seminar (Uppsala-Stockholm, 24-27 October 1971), p. 4.

25. For the purposes of this report, the expression "computerized personal data systems" designates a collection of data, stored in computerized files (that is recorded on magnetic tape, magnetic disks etc.) and which relate to a specific individual, identifiable by name or other particular elements through which the name may be readily obtained. 12/

25a. The most common classification of personal data systems, whether computerized or not, divides them into three categories: statistical and research systems, administrative systems and intelligence systems. 12a/

25b. Certain statistical data systems operated by governmental agencies, such as those created in a population census or in sample surveys, contain personal data, gathered through a questionnaire or by other methods designed to assure the comparability of individual responses. The facts gathered are wide-ranging and include many categories of personal information that can be considered private. Although data output is in aggregate form only, and the identity of the individual is, in nearly all cases, either separated from the data in the files or is encoded to guard anonymity, data output can nevertheless in certain cases (see paragraphs 119-120 below) be related to the individual concerned. As statistical systems maintain data about individuals exclusively for statistical reporting, and not for regulatory or prosecuting purposes, they are not intended to be used in a manner which would affect any individual directly.

26. Similar to statistical systems, and therefore usually not considered as a distinct category, 13/ are the research systems, which also store data about identifiable individuals for purposes of research in social and biomedical sciences or for programme evaluation studies undertaken by governmental agencies.

27. Administrative systems are the most comprehensive category, as they are used both in the public and private sectors. These systems are often organized into "person" files or dossiers, to furnish reports about specific individuals and for

---

12/ See, for instance, Records, Computers and the Rights of Citizens, report of the Secretary's Advisory Committee on Automated Personal Data Systems, United States Department of Health, Education and Welfare, July 1973, (United States Government Printing Office, 1973) (hereafter referred to as "United States, HEW Report"), pp. 49-50; Canada, Privacy and Computers, p. 157. In the Data Act (Sweden 1973) the computerized files to which the law is applicable (see paragraph 195 below) are defined as any compilation of computer-processed personal data which can be referred to an individual.

12a/ For instance, Canada, Privacy and Computers, pp. 38-42; Records, Computers and the Rights of Citizens, report of Secretary's Advisory Committee on Automated Personal Data Systems, United States Department of Health, Education and Welfare (United States Government Printing Office 1973) (hereafter referred to as United States, HEW Report), pp. 5-6.

13/ In the report of the United States Department of Health, Education and Welfare the expression "statistical-reporting and research systems" was used (United States, HEW Report, pp. 89-106).

making determinations relating to their qualifications, characters, rights, opportunities and benefits. They encompass many public and private administrative activities in the economic, financial, business, educational, welfare and health fields. There is a great variety in the volume, sensitivity and purpose of the information gathered.

27a. It may be added that these systems may process data for their own internal purposes and/or for third parties, such as, for instance, authorities keeping drivers' records which can also be used by insurance companies 13a/ or information agencies, market and opinion research institutes and wage calculations centres. 13b/

28. Intelligence systems are used mainly by governmental agencies (Police, law enforcement, national security), but also by credit bureaux of the investigative type and by private investigators, primarily for potential employers, retail stores and insurance companies. These systems differ in practice from administrative records in the following ways: much of the information is hearsay; the existence of the file (and of the investigation) is usually unknown to the person investigated; the information is seldom made public, 14/ except as evidence in legal proceedings.

13a/ See paragraph 263 below for this example.

13b/ See, for instance, Provisional Explanatory Memorandum, attached to the draft bill on protection against the misuse of personal data in data processing (Federal Republic of Germany) (EXP/Prot.Priv./EDB(73)2, pp. 29 and 43).

14/ Canada, Privacy and Computers, p. 42.

II. BENEFICIAL USES OF COMPUTERIZED PERSONAL DATA SYSTEMS

29. It has been said that:

> "When historians come to write the story of our time, they may well characterize it as the Age of Cybernetics. Surely one of the most significant aspects of this period is the technological revolution centered around a species of machine we call 'the computer,' a revolution that is dramatically increasing man's capacity to accumulate, manipulate, retrieve, and transmit knowledge. Without this resource we would be unable to enjoy the fruits of contemporary society's information explosion or to reap the full benefits of our capacity to thrust a rocket to the moon and the planets beyond." 15/

30. In connexion with the increasing role of information, the opinion has been expressed that "the world is generally and steadily shifting from the industrialized society to the information society" and that "a revolutionary data processing centering on computers will be the motive power of transforming the industrialized society into an information society". 16/

31. It has been further pointed out that the computer is a vital tool in solving the new problems specific to modern society such as pollution of the environment, destruction of natural resources, road safety and noise and the old problems of crime, ignorance and chronic unemployment and poverty. The computer is the only means by which all relevant data may be adequately summated, studied and extrapolated, being also equipped to accept hypotheses for various solutions and to evaluate them rapidly enough for effective action to be taken. 17/

32. Benefits to be derived from computerized information processing systems have been described "in terms of effective planning, resource allocation and greater efficiency in various types of human activity" as "almost every activity depends upon a foundation of accurate, accessible information about both things and people". 18/

33. The Government of Italy has stated that computers facilitate the carrying out of social projects (such as projects relating to education, health, transportation, etc.) and improve administrative procedures. 19/

34. With regard to record keeping, the limitations of the manual filing systems have been stressed in the light of the use of these systems in contemporary conditions, when increasing complexity and expansion of government operations have created a need for information which has produced enormous quantities of paper

---

15/ Miller, op. cit., pp. 1-2.

16/ Japan Computer Usage Development Institute, The Plan for Information Society - A National Goal toward Year 2000 (May 1972), pp. 2 and 6.

17/ Malcolm Warner and Michael Stone, The Data Bank Society; Organizations, Computers and Social Freedom (London, George Allen and Unwin, 1970), p. 219.

18/ Canada, Privacy and Computers, p. 10.

19/ Information furnished by the Government of Italy on 13 July 1973.

records. Notwithstanding the increased allocation of manpower and resources to information-handling activities, the need for information had remained largely unsatisfied under the manual filing systems, because of their short-comings relating to file handling, retrieval, accuracy and storage of information. The substantial increase of the amount of stored information in each record and of the number of records had magnified these short-comings and diminished the utility of the manual system. 20/

35. The view has been also expressed that in the United States it is the increase in transactions that created the pressure to use computerized systems, more than failings intrinsic to manual record-keeping systems. 21/

36. The advantages of computerized record-keeping have been described as follows:

> "The use of computers is in many respects superior to manual systems, in particular as regards the quantities of data that can be processed and stored. Information can be centralized in databanks and, by means of developed techniques, processed and disseminated in a way that was impossible by means of older systems. This means that great benefits can be derived from the new information-processing systems. They make it easy to accumulate very large quantities of information about things and people, to keep the accumulated information accurate and to make it accessible in its original or processed form. Thus the computers can take over much of the routine tasks of an administration and set people free to carry out more qualified work. In addition, and even more important, the new information-processing systems can form the base for a faster and more effective planning and resource allocation and, in general, tend to diminish costs and strengthen the efficiency in various types of administrative work. Automatic data processing has made it possible to realize objectives which could not have been reached otherwise, in any case not for a long time." 22/

37. In the above-mentioned report of the National Academy of Sciences of the United States, one of the conclusions of a study of 55 of the most advanced organizations in the field of computerization of personal records in the United States was that:

> "computerization is definitely bringing some important increases in the efficiency of organizational record-keeping. The most important of these are

---

20/ "Computerization of Government files: what impact on the individual?" Research project, UCLA Law Review, vol. 15, No. 5 (1968) (hereinafter referred to as "UCLA Research", pp. 1380-1383).

21/ See United States Report of the National Academy of Sciences, pp. 222-228.

22/ The National Office of Organization and Management, Information Systems in the Administration (29.1. 1971) (furnished by the Government of Sweden on 21 August 1973). See also, Organisation for Economic Co-operation and Development (OECD), Digital Information and the Privacy Problem (Report of the Committee for Science Policy Computer Utilization in Member Countries, Paris, 1971) (hereinafter referred to as "OECD Report") paras. 17 and 20.

the production of more complete and up-to-date records; faster responses to inquiries; more extensive use of information already in the files; more extensive networks for interorganizational exchange of data; and the creation of some large data bases that would not have been feasible without computers. As a result, organizations are able to carry out record transactions more swiftly and effectively through computerized data systems." 23/

38. The above-mentioned advantages of computerized personal data systems explain their rapid and continuous expansion in an increased number of areas, depending upon circumstances specific to each country. The main areas where computerized personal data systems are applied are the following: government, public administration, law enforcement and justice, taxation, driver-licensing, social security and welfare, education, health, credit and banking, life, accident or casualty insurance and biomedical and social research.

39. The magnitude of computerized personal data systems applications should be envisaged also in the light of what has been called a basic dichotomy. One class of stored data may concern internal operations of the organization, including, among others, computerized files on the employees. Another class comprises personal information about the individuals who require the services of that organization. 24/

40. The existence of transnational computerized personal data systems storing data about citizens of foreign countries can be mentioned equally as another aspect of the expansion of data systems. Examples of areas where such transnational systems are operating are credit and banking, medical information for life insurance purposes and health information systems for patient treatment. 25/

41. The description of the applications of an integrated personnel administrative system could serve as an example of the variety of the purposes for which a computerized personal data system may be used. Such a system might include the following applications:

"Roster of applications

This application involves matching a file of currently available applicants against a file of vacant positions, taking into consideration the qualifications of applicants and requirements of the positions. The resulting report would identify the applicants that may qualify for certain positions and can be used to control and schedule recruitment, testing and selection.

23/ United States, Report of the National Academy of Sciences, p. 314.

24/ Cf. Edward F. R. Hearle, "Organization and management of data processing in Government", Report of the Interregional Seminar on Electronic Data Processing in Government: Volume I, Report and Technical Papers (Bratislava, Czechoslovakia, 22-30 November 1971, document ST/TAO/M/63), p. 53. "The basic dichotomy" applies also to private organizations. For instance, the Bank of America holds bank employees records and customer and "third party" files (prospective business customers) (United States, Report of the National Academy of Sciences, pp. 119-120).

25/ Canada, Privacy and Computers, pp. 56-57, 60, 63, 73 and 82.

"Applicant and employee testing

The computer can record requests to take entrance examinations, match candidate qualifications, schedule examinations, print notices for candidates, score examinations and print lists of qualified candidates.

"Personnel records

Personnel information by tradition and definition is qualitative and highly subjective. It is doubtful that such data will ever be fully computerized. However, basic personnel data, such as age, sex, employment dates and years of education can be coded for computer processing. The employee's personnel history as well as current position and pay data can also be successfully quantified and coded. Files developed for this application can be integrated with other files on position control, personnel actions, payroll, time, leave and retirement. The statistics and reports which can be produced from these files are too numerous to describe here.

"Position control and personnel actions

This application integrates data on the employee with the position he occupies. The position file contains a number for each position as well as its title, salary etc. This file can be used to prepare position requests for budget approval and formulation and for the analysis of vacancies, and it can serve as a basis for authorizing and controlling personnel actions.

"Payroll

This is probably the most common application of computers. The computer can compute gross pay, taxes, social security, insurance and pension premiums. It can print pay cheques, payroll journals, earnings ledgers for each employee and year-end statements of wages earned and so on.

"Time and leave records

The documents for time-keeping, which may be the basis for payroll can be used to record the accrual, use and balances of holidays and leave for employees. The printing of this information on pay cheques or statements can be a by-product of this processing.

"Skill inventories and manpower planning

The ideal of personnel administration is to place the best man in the right job at the right time. In recent years, considerable progress has been made in developing the coding and classification systems needed for the computer analysis of an individual's past, present and potential skills and capabilities so that career development and staffing plans may be prepared." 26/

26/ United Nations Secretariat, "Computer applications in government", in document ST/TAO/M/63, pp. 31-32.

42. With regard to the benefits derived from the design, programming and installation of a computer system for personnel administration, it has been pointed out that such a system would do much to:

> "(a) facilitate improved and uniform personnel policy and practices throughout the government, (b) streamline the recruitment process so that when qualified candidates become available they can be immediately employed, (c) ensure that timely and justified requests for filling positions are authorized within budgetary limits, (d) shorten the time-span between the initiation and the completion of all personnel transactions and add to their accuracy, (e) abstract personnel statistics and data as a by-product for personnel planning, training and career development, (f) develop and utilize personnel resources more effectively, (g) help to establish equitable compensation plans and employee benefits programmes based on accurate data, and (h) project manpower requirements upon which to base recruiting, training, career development and promotion policies." 27/

43. In information furnished by the Government of Belgium, benefits to be derived from the use of computers in certain public activities have been synthesized as follows:

> "Keeping staff size within reasonable bounds;
>
> "Speed of action and accuracy in execution;
>
> "Faster calculation and payment of staff wages and salaries, and faster introduction of changes in them;
>
> "Improved service to the public and significant benefits for the country's economy;
>
> "Accurate and full information facilitating decision-making, allowing more economical management of transport resources and simplifying negotiations for international agreements;
>
> "Speeding up of research in all fields of activity, in particular in legal matters;
>
> "More efficient supervision of vehicles in respect of technical matters, insurance and road taxation;
>
> "Safety of transport in general and especially of air transport." 28/

44. The information furnished by the same Government refers to, inter alia, the planned establishment of a computerized national register, with the purpose of

---

27/ Ibid., p. 33.

28/ Information furnished by the Government of Belgium on 22 February 1973.

storing and keeping up to date the basic elements (name, date of birth and sex) of identification of Belgians by using a national number (universal identifier). This system would provide the following advantages to central and local administration and to the population:

"(a) Advantages to central administration: The National Register will allow the automatic updating of files in the public sector concerning personal data of a general nature: surname, given names, address, civil status, makeup of the household. The National Register will also permit automatic exchanges of data between files, which are not possible at present because of the lack of a single identification number. The system will obviate the need to retranscribe data manually, thus eliminating a source of error, and will make it possible to reduce appreciably the time necessary for data transmission.

"(b) Advantages to local administration: Organs of local administration will have to report changes of residence by their inhabitants only once to the National Register, which will keep up to date other files kept by organs of public administration; at present, local authorities have to forward certain data to several different bodies.

"(c) Advantages to individuals in Belgium: Each individual will have a single registration number for the various public agencies. Accordingly, the risk of error due to the large number of references used at present will no longer exist. Furthermore, the individual will no longer be required to furnish many kinds of certificates, since the public agencies will be able to obtain such information from the National Register." 29/

45. The trend has developed in the United States for federal agencies other than those in charge of social security to use the social security number as a kind of standard universal identifier. 30/ In this connexion, the proponents of the general adoption of such an identifier have mentioned the following advantages: easier and more accurate updating, merging and linking of records about individuals for administrative, statistical and research purposes; a reduction of duplication and errors in record keeping; the simplification of the everyday dealings of the citizen with organizational record systems. 31/

46. In health care systems, the use of computers for handling administrative functions has been considered to present the advantage of reducing the clerical load not only of administrative personnel but also of doctors and nurses and of increasing the productivity of medical services. 32/

29/ Information forwarded by the Government of Belgium on 15 February 1973.

30/ See United States, HEW Report, p. 111.

31/ Ibid. and United States, Report of the National Academy of Sciences, p. 398.

32/ The Computer Impact, Irene Taviss ed. (Englewood Cliffs, New Jersey, Prentice-Hall, Inc., 1970), p.53.

47. By its speed in input and output, computerization of medical records has been described as enabling the physician or a nurse to determine the state of the patient more quickly and accurately than by using voluminous manual files and to obtain only the precise information needed. 33/

48. Computer-based medical records systems, by drawing together records kept in hospitals, pharmacies and laboratories could establish a comprehensive medical history of the patient. This would improve medical care as it would provide a more accurate picture of the patient's condition, which would contribute to a more accurate diagnosis. A comprehensive medical history of the patient would also lessen the possibility of error in diagnosis and treatment and avoid unnecessary testing which may be dangerous and expensive. 34/

49. Computerization of various tests would reduce the costs of preventive medicine in general. At the same time, a computer programme can select the problems requiring further examination, classify abnormal cases and suggest "provisional diagnosis". 35/

49a. In addition, the existence of computerized medical records presents the advantage that, in case of an accident, which has taken place at a distance from the residence of the victim, they could speedily offer complete information on his medical history, allowing the application of a more appropriate treatment. This is an important advantage in an epoch when people travel increasingly and the number of traffic accidents is rising.

50. It has been considered in general that medical computerized systems "may clearly provide information of direct benefit to the patient and may, therefore, prove essential for his treatment". 36/

51. The applications of computerized personal data systems in the fields of law enforcement and criminal justice have been estimated as being highly beneficial for society and for the protection of personal rights and freedoms.

52. Society benefits from the use of computerized systems in the above-mentioned

---

33/ Lorne Elkin Rozovsky, "Legal aspects of computerization in the health care system", paper presented at the 3rd World Congress on Medical Law, Ghent, Belgium 19-23 August 1973, pp. 1-2.

34/ Ibid., p. 2.

35/ The Computer Impact, p. 54. Examples of such applications of computers in a number of hospitals are given.

36/ J. de Moerloose, "A survey of international and national codes and legislation in selected areas", report presented at the Round Table Conference on Human Rights, organized by the Council for International Organizations of Medical Sciences (14-16 November 1973), p. 37 (furnished by WHO on 18 December 1973).

fields, because these systems are very effective tools in preventing and combating crime. 36a/

53. With regard to the benefits for the rights and freedoms of the individual, it has been pointed out that:

> "The ultimate goal of criminal justice is to nurture individual freedom; the system achieves its objectives by preserving ordered liberty, so that no man denies the freedom of his fellow man. Law enforcement and all the agencies of criminal justice are dedicated to preserving in dynamic equilibrium the delicate balance between individual liberty and community tranquility.
>
> ...
>
> "Computer systems should protect and enhance the freedom and civil liberties of the individual. Aside from the dividends of ordered liberty that will result from more effective administration of all the functions of criminal justice, there will ensue direct and very tangible immediate benefits. For surely justice can more readily be achieved, and constitutional protections better afforded when the accused is identified fully and all relevant facts pertaining to the case are rapidly available. A summons may be served in lieu of arrest in appropriate cases; bail or release on personal recognizance may be granted expeditiously, and immediate sentencing in appropriate cases may be based upon greater knowledge of the convicted person." 37/

54. For the illustration of the major new capabilities of a computerized personal data system used in law enforcement, the advantages of the New York State identification and intelligence system have been referred to as follows:

> "First, suspects from files of known criminals can be identified to a degree and a speed hitherto impossible. Second, outstanding open cases can be solved by automatic and comprehensive searches conducted on the basis of statewide information. Third, automatic abstracting, indexing, and retrieval of textual intelligence and *modus operandi* information can be used to conduct a comprehensive search of all documents stored in the system and a retrieval of only those documents that are relevant to the interests of the user, instead of the current time-consuming manual index-card files and bulky folder files.

36a/ Robert R. J. Galatti "Criminal justice: computers, related technology and the scientific method", *Police*, Sept.-Oct. 1968, pp. 25-26; Donald N. Michael, "Speculations on the relation of the computer to individual freedom and the right to privacy", *George Washington Law Review*, vol. 33, No. 1 (October 1964), p. 273, James Martin and Adrian L. D. Norman, *The Computerized Society* (Englewood Cliffs, N.J., USA, Prentice-Hall, 1970), pp. 100-101.

37/ Galatti, *loc. cit.*, p. 24.

"Finally, the system offers the tremendous potential of being able to perform research: a pattern analysis of data to assist in evaluating new trends in crime, in testing new approaches to the administration of criminal justice, and in discovering patterns of structure and activity of criminal and special organizations in order to discover relationships in vast bodies of facts that would be almost impossible to develop through standard manual techniques of file searching /47/.

"/47/ The Computer and Invasion of Privacy. Hearings before a subcommittee of the Committee on Government Operations. House of Representatives, 89th Congress, second session, July 26-28, 1966 (Washington, U.S. Government Printing Office, 1966), p. 159 and following." 38/

55. It has been further pointed out that the use of electronic data processing by law enforcement agencies, criminal justice and related agencies eliminates a great deal of wasted effort in the many operations related to the functions of these agencies and of criminal justice. 39/

56. An example of the benefits of a large electronic network in detecting crime relates to the United States Customs Automatic Data Processing Intelligence Network. The network's memory contains the names of more than 200,000 known or suspected smugglers, with identifying elements and information relating to their past criminal history. It is linked with computerized crime files of the Federal Bureau of Investigation, with other Federal law enforcement agencies and with customs representatives abroad as well as with the service's intelligence gathering headquarters in several important towns in the United States. The network is used for detecting smugglers entering the country from Mexico and Canada. In 1972, when its scope of operation was much smaller than it was in 1973, the network was credited with helping to bring about 446 smuggling arrests along the Mexican border along. 40/

56a. The Legal Affairs Committee of the Consultative Assembly of the Council of Europe presented to that Assembly a draft recommendation concerning the creation of a "Judicial Information Centre" which would centralize the information on foreigners, having been convicted under criminal law in one of the Member States of the Council of offences other than those of minor gravity. According to the explanatory memorandum appended to the draft, the Centre was envisaged to be wholly computerized. 40a/

38/ Martin and Norman, op. cit., pp. 115-116.

39/ Gallati, loc. cit., p. 19.

40/ Everett R. Holles, "Computers help detect smugglers at borders", The New York Times, 9 September 1973.

40a/ Council of Europe, Consultative Assembly, Twenty-First Ordinary Session (Third Part) 22-30 January 1970, Documents, Working Papers (Strasbourg 1970), pp. 2 and 5-6.

III. THREATS AND PROBLEMS FROM THE POINT OF VIEW OF HUMAN RIGHTS

A. Preliminary remarks

57. It has been maintained that the use of computers in the field of personal record-keeping has not brought any real new threat to human rights. Archives, files and police have existed since men have lived in society. Information about individuals had been gathered long before the advent of the computer and especially in modern times. Between the manual filing system and the computerized system, there was a transitional period when automated systems (punch-cards) were used, for instance, in statistics and personnel administration. The introduction of computerized personal data systems is said to be only a new technological stage in a constant and inevitable evolution of social life. 41/

58. In the report of the Committee on Privacy, appointed in the United Kingdom in 1970, 42/ it has been stated that "we cannot on the evidence before us conclude that the computer as used in the private sector is at present a threat to privacy, but we recognize that there is a possibility of such a threat becoming a reality in the future". 43/

59. It has been similarly stressed that neither the study of the Canadian Task Force nor others conducted in other countries have concluded that widespread invasions of privacy are actually happening. It has been pointed out, however, that "opportunities for such invasions exist" and that "the rapidity of technological progress is likely to broaden rather than restrict the potential for harm to individuals". 44/

60. It may be noted that in the report of the United States Department of Health, Education and Welfare it has been observed that "the application of computers to record-keeping has challenged traditional constraints on record-keeping practices," referring at the same time to "dangers latent in the spread of computer-based personal-data record-keeping". 45/

41/ This view has been summarized in Guy Braibant, "La protection des droits individuels au regard du développement de l'informatique", Revue internationale de droit comparé, 1971, No. 4 (furnished by the Government of France on 5 February 1973), pp. 796-797.

42/ United Kingdom, Report of the Committee on Privacy, Chairman: The Rt. Hon. Kenneth Younger, Cmnd. 5012 (London, HMSO), (hereafter referred to as "United Kingdom, Younger Report"), para. 619. For information relating to this report see paragraph 198 below.

43/ United Kingdom, Younger Report, para. 619.

44/ Canada, Privacy and Computers, p. 182.

45/ United States, HEW Report, pp. XIX and 12.

61. According to another view, the protection of the individual's rights in relation to information about him was much better before the age of computers, since:

> "(1) large quantities of information about individuals traditionally have not been collected and therefore have not been available to others; (2) the available information generally has been maintained on a decentralized basis and typically has been widely scattered; (3) the available information has been relatively superficial in character and often has been allowed to atrophy to the point of uselessness; (4) access to the available information has not been easy to secure; (5) people in a highly mobile society have been difficult to keep track of; and (6) most people have been unable to interpret and infer revealing information from the available data". 46/

62. The prevalent opinion seems, however, to be that, while any maintenance of personal data systems presents certain problems for and threats to human rights, the advent of computers has magnified some of these problems and has introduced others. In the report of the Commission on Publicity and Secrecy of Official Documents submitted to the Swedish Ministry of Justice in 1972, it was stated:

> "the ADP technique gives rise to quite new threats to personal privacy. Compared with information kept on documents, it is principally a matter of degree, but the difference is such that the situation has changed in a decisive way". 47/

One writer has observed:

> "computer techniques make such vast quantitative changes in the collection, processing and use of data that the result is a qualitative change: the elements which make up and characterize computer techniques are not new in themselves but are new by reason of their dimensions ...". 48/

63. The changes brought about by the computer in personal information systems which magnified their implications for human rights or added new ones have been described as follows:

> "The computer, which can be accessed through communications links, is a device whereby records about individuals (in varying but almost limitless quantities)

46/ Miller, op cit., p. 26. See also UCLA Research, p. 1411.

47/ Swedish Ministry of Justice, Computers and Privacy, Summary of report (SOU 1972: 47) and draft Data Act submitted by the Commission on Publicity and Secrecy of Official Documents, (furnished by the Government of Sweden on 21 August 1973), and hereafter referred to as "Sweden, Computers and Privacy"), p. 6.

48/ Braibant, loc. cit., p. 798. See also, for instance, United States, HEW Report, p. 49.

can be stored, retrieved and passed on to others, often without the consent or knowledge of the subject; where disparate bits of information can be centralized, correlated, and reorganized in possibly damaging ways; where mistakes can be compounded and their effects exacerbated; where the fallibilities of human memory are no longer a source of relief. Privacy-related questions are thus brought into play, and are intensified as the number of files on individuals grows constantly in a variety of fields from education to credit, from welfare to insurance, from taxation to criminal history." 49/

B. Human rights which may be affected

64. The use of computerized personal data systems may have the following adverse effects on the right to privacy, a right whose international recognition and whose scope have been explored in document E/CN.4/1116, paragraphs 27-49: (a) by gathering and storing a greater amount of data pertaining to the private life of the individual; 50/ (b) by disseminating the information to a wider audience than the individual consented to or anticipated when he originally surrendered the information, infringing thus upon its confidentiality. 51/

65. Computerization of personal files has been also viewed as having a specific impact, in organizational decision-making, on what is called in the Anglo-American legal systems the due-process tradition, 52/ as the data collected in these files are relied upon to determine rights, benefits or obligations of the individual. 53/

66. The concern has sometimes been expressed that the increased expansion of computerization of personal data may result in a "dossier society" which would have "dehumanizing" effects on the individual.

67. The following description of some such effects has been given:

"As the public becomes increasingly aware of the information orientation of modern life and that a substantial amount of personal data about them is being preserved 'on the record', it is understandable that people may begin to doubt whether they have any meaningful existence or identity apart from their profile stored in the electronic catacombs of a 'master' computer. Embedded in this fear of being stripped of individuality is the psychosis of the Computerized Man, popularly portrayed as a quasi-automaton whose functions have been standardized, whose status in the community has been determined for him, and whose financial condition is prescribed in immutable terms." 54/

49/ Canada, Privacy and Computers, p. 15.

50/ Canada, Privacy and Computers, p. 15.

51/ Miller, op. cit., p. 26.

52/ United States, Report of the National Academy of Sciences, p. 256.

53/ See further, paras. 111-117 below.

54/ Miller, op. cit., pp. 49-50.

68. The relative inflexibility of computer-based record-keeping resulting from the computer's having been designed to use certain pre-conceived categories (mentioned in paragraph 100 below), coupled with the constraints that some computerized systems put on the freedom of persons concerned to provide explanatory details in responding to questions have been considered as contributing to the dehumanizing effect of computerization. 55/

69. The use of the standard universal identifier (SUI), whose practical advantages were mentioned in paragraphs 44 and 45 above, in connexion with computerization, has recently raised fears and anxieties even in some European countries 56/ where such identifiers were introduced without opposition. Because of the introduction of SUIs, citizens "both feel a sense of alienation from their social institutions and resent the dehumanizing effects of a highly mechanized civilization". Such fears have been considered as justified because:

> "The bureaucratic apparatus needed to assign and administer an SUI would represent another imposition of government control on an already heavily burdened citizenry.
>
> "To realize all the supposed benefits of an SUI, mandatory personal identity cards would have to be presented whenever called for. Loss or theft of an SUI card would cause serious inconvenience, and the mere threat of official confiscation would be a powerful weapon of intimidation.
>
> "The national population register that an SUI implies could serve as the skeleton for a national dossier system to maintain information on every citizen from cradle to grave.
>
> "An unchangeable SUI used everywhere would make it much easier for an individual to be traced, and his behavior monitored and controlled, through the records maintained about him by a wide range of different institutions.
>
> "A permanent SUI issued at birth could create an incentive for institutions to pool or link their records, thereby making it possible to bring a lifetime of information to bear on any decision about a given individual.
>
> ...
>
> "a universally identified man might become a prisoner of his recorded past". 57/

55/ United States, HEW Report, p. 14.

56/ Sweden (1947), Norway (1964), Finland (1965) and Denmark (1968), (Canada, Privacy and Computers, p. 87).

57/ United States, HEW Report, pp. 111-112. Certain similar observations have been made in United States, Report of the National Academy of Sciences, pp. 398-399. Both reports recommend against introducing an SUI in the United States.

In addition, fear of loss of anonymity, and the suspicion that bureaucrats confronted by numbers will tend to forget that they represent real people, have been also mentioned as negative psychological effects of SUIs. 58/

70. The use of computerized personal data systems may have harmful effects on human rights in relation to inaccuracy and obsolescence of data, access to and sharing of data, accumulation of data and the record-keeping personnel. One or several of the human rights mentioned above may be adversely affected by one of these negative consequences. For example, inaccuracies in personal data, due to the use of computers, may affect the right to a fair and public hearing, if the computerized information is used as evidence in courts (see paragraphs 312-314 below) and, when it is employed for making decisions, other rights of the individual. For this reason, the threats and problems will be examined in paragraphs 71-110 below, without, in general, relating them to specific rights. The impact of the use of computerized files as a basis for making certain decisions about the rights and benefits of individuals presents, however, some specific special characteristics affecting issues of due process and therefore will be dealt with separately in paragraphs 111-117 below. In addition, paragraphs 118-120 below deal with a particular problem concerning privacy in relation to the use of statistical and research systems.

C. Inaccuracy and obsolescence of data

71. While the risk that careless or malicious administrators or information handlers will introduce inaccuracies into records containing personal data did exist before the use of EDP, the additional handling by computers, requiring the translation of data from alphabetic notation into a machine-readable computer input, magnifies the risk of inaccuracies in reporting, recording and indexing. There is also an increased likelihood of information distortion caused by human and machine malfunctioning, especially in remote-access time-sharing systems. 59/

72. Three basic ways in which inaccurate information on an individual may be recorded in a computer have been described:

> "(a) The input data may be wrong, either because an error was made in recording it, or because it has been wrongly transcribed. With incorrect data even perfect processing must give an incorrect result ...
>
> "(b) The computer's programme may be wrong, for example, because the programmer did not appreciate the full circumstances of the case, or because he made a logical mistake through faulty analysis, or because of copying or transcription errors in writing the programme down and preparing it for feeding into the computer.

58/ Ibid., p. 86. This report recommends against introducing an SUI in Canada.

59/ Miller, op. cit., p. 32.

"(c) The computer develops a mechanical or electrical fault which causes it to corrupt the data, the programme or the results." 60/

73. It has been said that, once in a file, information, however inaccurate, tends to remain there, and the nature of the computer strengthens this tendency, first because of the difficulty of finding errors among the mass of information that can be handled by a computer, and secondly because of the relative ease and economy of retaining the entire information gathered, as compared with an ordinary filing system. 61/

74. Individuals are vulnerable to the danger that subjective data - that is to say, evaluations based for instance on interviews - may be recorded in a computer and later treated as objective facts. 62/ This danger varies according to the quality of the source of information and of the personnel interpreting the computer's output.

75. Secondly, it has been maintained that erroneous information might result from a data-processing system as a consequence of faulty programming. Mistakes might enter the process between the preparation of programme and its installation as a set of instructions for the computers; but a more serious potential source of errors and distortions at this stage might be the programmer himself. 63/

76. Finally, erroneous information can result from a mechanical or electrical fault in the computer. The developing technique of time-sharing may present further possibilities for accidental malfunction:

"This /time-sharing/ means that while one user's finger is moving toward a control button on his computer control panel, another person is using the circuits he will be using a few seconds later. In the future, one computer user might accidentally gain access, through equipment malfunction, to another's information stored in memory banks." 64/

77. It has been further pointed out that computerized data may be easier to destroy than paper files or record books, as a simple magnet can be used to erase the information stored on a reel of magnetic tape. 65/ When the information is

---

60/ Joseph Jacob in (United Kingdom) National Council for Civil Liberties, NCCL News Release (26 June 1969), quoting from F. J. M. Laver, Introducing Computers (London, 1965).

61/ Jack Sawyer and Howard Schechter, "Computers, privacy, and the National Data Center: the responsibility of social scientists", American Psychologist, vol. 23, No. 11 (November 1968), p. 815.

62/ Ibid., p. 814.

63/ See, for instance, Miller, op. cit., p. 38.

64/ Donald N. Michael, loc. cit., p. 276.

65/ Miller, op. cit., p. 28.

moved from the files into the central processor of a time-sharing computer system, "a minor technical failure or variations in electric current - let alone a power failure - can result in data being lost, distorted or misdirected to an unauthorized recipient in a remote-access system". 66/

78. It may be felt that the Assembly for Human Rights, which met in Montreal, 22-27 March 1968, had the question of accuracy in mind when it stated: "non-governmental organizations of the legal profession should apprise themselves of the risk of computerized dossiers ...". 67/

79. The opinion has been expressed that accurate, but obsolete, information that may prevent the individual from exercising his right to "live down his past" also tends to be maintained in a computer's memory even more than it does in traditional files. 68/

80. According to the report of the National Academy of Sciences of the United States, a visit to 55 of the most advanced organizations in the field of computerization of personal records produced the following estimate regarding the accuracy problem:

> "Our two principal findings about accuracy of records can be summarized as follows: computerization has in many cases reduced omissions from standardized records and increased logical consistency and/or timeliness of the records that are converted to machine-readable form; many computerized operations keep their records more accurate in these respects by software and personnel supervision. But human and machine errors are still possible and present in computerized systems, with some kinds of mistakes capable of affecting very large numbers of individual records. Even when these mistakes are noticed, very important damage may have been done in the elapsed time to the rights and interests of those persons affected. And computerization has not affected the substantive correctness of the facts about people collected at the source. The conclusion we draw, therefore, is that society must assume that there can be inaccuracies in the records maintained in both manual and computerized systems." 69/

The same report further noted that in addition to carrying many of the same types of error as manual systems do, computerization also carries with it some kinds of errors unique to electronic data processing. 70/

66/ Ibid.

67/ Montreal Statement of the Assembly for Human Rights, (Montreal, 1968), sect. IX.

68/ See, for instance, Miller, op. cit., p. 50.

69/ United States, Report of the National Academy of Sciences, p. 302.

70/ Ibid., p. 435.

81. With respect to ensuring the accuracy of data by keeping them up to date, the opinion was expressed in the report that "the process of data conversion for computerized systems had led to the creation of more up-to-date individual records than these organizations achieved in the pre-computer area" and "that among the 55 organizations visited the policies about such matters as wiping out records after the passage of time have been carried forward rather than changed in the computerized systems." 71/

D. Access to and sharing and centralization of personal data

82. Unauthorized access to personal files, from within the organization maintaining them or from outside, can lead to unauthorized disclosure of the information they contain. Such a disclosure may occur by accident, or by deliberate efforts to infiltrate the system. The ways to achieve such infiltration have been described as follows:

> "Passive infiltration may be accomplished by wire-tapping or by electromagnetic pickup of the traffic at any point in the system. Although considerable effort has been applied to counter such threats to defense communications, nongovernmental approaches to information privacy usually assume that communication lines are secure, when in fact they are the most vulnerable part of the system. Techniques for penetrating communication networks may be borrowed from the well-developed art of listening in on voice conversations. (While the minimum investment in equipment is higher than that required to obtain a pair of headsets and a capacitor, it is still very low since a one-hundred-dollar tape recorder and a code conversion table suffice.) Clearly, digital transmission of information does not provide any more privacy than, for example, Morse code. Nevertheless, some users seem willing to entrust to digital systems valuable information that they would not communicate over a telephone.
>
> "Active infiltration - an attempt to enter the system to directly obtain or alter information in the files - can be overtly accomplished through normal access procedures by:
>
> Using legitimate access to a part of the system to ask unauthorized questions (e.g. requesting payroll information or trying to associate an individual with certain data), or to 'browse' in unauthorized files.
>
> 'Masquerading' as a legitimate user after having obtained proper identifications through wire-tapping or other means.
>
> Having access to the system by virtue of a position with the information center or the communication network but without a 'need to know' (e.g. system programmer, operator, maintenance, and management personnel).
>
> "Or an active infiltrator may attempt to enter the system covertly i.e., avoiding the control and protection programs) by:

71/ Ibid., p. 268.

Using entry points planted in the system by unscrupulous programmers or maintenance engineers, or probing for and discovering 'trap doors' which may exist by virtue of the combinatorial aspects of the many system control variables (similar to the search for 'new and useful' operation codes - a favorite pastime of machine-language programmers of the early digital computers).

Employing special terminals tapped into communication channels to effect:

- 'piggy back' entry into the system by selective interception of communications between a user and the processor, and then releasing these with modifications or substituting entirely new messages while returning an 'error' message;

- 'between lines' entry to the system when a legitimate user is inactive but still holds the communication channel;

- cancellation of the user's sign-off signals, so as to continue operating in his name.

In all of these variations the legitimate user provides procedures for obtaining proper access. The infiltrator is limited, however, to the legitimate user's authorized files.

"More than an inexpensive tape recorder is required for active infiltration, since an appropriate terminal and entry into the communication link are essential. In fact, considerable equipment and know-how are required to launch sophisticated infiltration attempts.

"The objectives of infiltration attempts against information systems have been discussed by a number of authors from the point of view of potential payoff. We will merely indicate the types of activities that an infiltrator may wish to undertake:

Gaining access to desired information in the files, or discovering the information interests of a particular user.

Changing information in the files (including destruction of entire files).

Obtaining free computing time or use of proprietary programs.

"Depending on the nature of the filed information, a penetration attempt may cause no more damage than satisfying the curiosity of a potentially larcenous programmer. Or it may cause great damage and result in great payoffs; e.g., illicit 'change your dossier for a fee', or industrial espionage activities. ...

/...

"More sophisticated infiltration scenarios can be conceived as the stakes of penetration increase. The threat to information privacy should not be taken lightly or brushed aside by underestimating the resources and ingenuity of would-be infiltrators." 72/

83. The mere fact that remote terminals are used, enabling unauthorized persons deliberately to gain access to private information, has been described as giving rise to fears over privacy. 73/ It might be added that certain technological innovations are under way which portend to increase inter-computer access to such an extent as to operate computer networks similar to telephone networks. Some of these are: remote-access terminals, visual displays, linking computers via a satellite, and recent trends in miniaturization using very large scale integrated circuits, ion implantation and magnetic bubble technology.

84. The possibility of improper actions on the part of computer employees, by using their access for unauthorized disclosure, by enabling the outside intruder to bypass protective devices or by revealing their nature or even by directly "bugging" the machine, has been further mentioned. 74/ According to the report of the United States Department of Health, Education and Welfare, while there are technical possibilities to defend most systems against outside intrusion, the main question is to prevent abuses of authorized access, since most leakage of data from personal data systems, both computerized and manual, appears to result from such abuses. 75/ In the report of the National Academy of Sciences it has been emphasized that "in every instance of unauthorized access that we have been able to corroborate, there was use of inside information or co-operation by the organization's employee". The report states that: "/C/omputer software and system operations provide some significant barriers to unauthorized intrusion by those who do not know the procedure specific to a given system. Even a highly skilled expert in computer systems, unless he knows how a particular system operates and how its programmes have been set up, cannot simply step up to a terminal and get information out. He will have to probe to discover the rules of the system, to see what software modifications have been made specifically for that record-keeping operation, etc. When probes of this kind are made, they often disrupt things and will affect the system in ways that will alert its operators. Thus the element of customizing that is involved in each organization's arrangement of its computer system and software provides impediments to outside intruders that produce some important inhibiting effects." 75a/

85. Another adverse effect on privacy of computerization of personal data has been considered to be the fact that it facilitates access to data across boundaries normally separating organizations and various branches of government.

72/ H. E. Petersen and R. Turn, "System Implications of Information Privacy", American Federation of Information Processing Societies (AFIPS), Conference Proceedings, vol. 30, 1967 (Spring Joint Computer Conference April 18-20, 1967) pp. 291-292.

73/ Local Authorities Management Services and Computer Committee (LAMSAC), Computer Privacy: Notes of Guidance for Local Authorities (London 1972), (hereafter referred to as United Kingdom, LAMSAC, Computer Privacy), p. 5 (furnished by the Government of the United Kingdom on 28 August 1973).

74/ Miller, op. cit., p. 30.

75/ United States, HEW Report, p. 19.

75a/ United States, Report of the National Academy of Sciences, pp. 306-307.

86. The enhanced ability of computerized systems to gather, package and deliver information from one organization to another has been envisaged as leading to dissemination of information in circumstances where lines of authority and responsibility are overlapping or ambiguous. In addition, by different interpretation and use of data, the likelihood of unfair or inappropriate decisions about the individual to whom any file pertains may raise problems, and particularly whenever the files are incomplete or summarized. 76/ In the Report of the Canadian Task Force, the following broad conclusions have been presented:

"...

"There is probably more data interchange than is generally realized by the public. Information networks flourish in many situations where the exchange of personal data is beneficial to both parties involved. Because of the informality of the process, precise description of the data paths is practically impossible, though questionnaire returns did yield some information on the networks. To a greater or lesser extent, police, credit-reporting agencies, insurance companies, educational authorities, and welfare agencies are (amongst other categories) involved in such exchanges, which usually take place without the person involved being informed of the activity." 77/

87. In this context, the question has been raised: "Should the information collected for one purpose, for example by a government department, necessarily be made available for other purposes?". 78/ The Commission on Publicity and Secrecy of Official Documents, in its report on computers and privacy, submitted to the Swedish Ministry of Justice in 1972, taking as a starting point that all information about the conditions of individuals may concern privacy, stated that "the possibility of its use for different purposes may be felt as a threat or a violation.... On the other hand, for many important reasons - public and private - information of various kinds must be collected and used for different uses. From the point of view of the individual concerned it is a matter of significance whether the information is available only to a special authority, to persons who have connexions with him or to a wider circle, possibly to any one who asks for it it". 79/

88. In the report of the National Academy of Sciences of the United States it was stated, however, on the basis of visits to the 55 of the most advanced organizations, that:

76/ United States, HEW Report, p. 15.

77/ Canada, Privacy and Computers, pp. 29-31.

78/ World Council of Churches, Exploratory Conference on Technology and the Future of Man and Society, Geneva, 28 June-July 1970, report of Working Groups, p. 26.

79/ Sweden, Computers and Privacy, p. 5. See also United Kingdom, LAMSAC, Computer Privacy, p. 5.

"nothing in computerization itself has produced a sharing of identified information to a broader class of users within multibureau organizations or among organizations than before computers. Where changes in patterns of confidentiality have taken place among the organizations we studied, the cause was new legislation or administrative rule, prompted by basic programme changes or new social policies." 80/

89. The possibility of the centralization of personal data, by collecting it from various agencies and storing it in a central system, has been described as presenting human rights problems. In this connexion, the following comparison has been drawn between manual and computerized systems:

"First, the inconvenience of searching for a record in a manual filing system may cause a natural reluctance for authorized users to obtain information for others outside the collecting office or agency. If the information can be obtained instantly at the push of a button, however, requests for information from outsiders may be more readily accommodated. Secondly, the geographic distance between a person seeking information and an agency in whose files that information is contained may deter attempts to obtain the information. This geographic barrier could often be removed by a centralized system in which access to that information could be provided by any of the many agencies sharing the system. Furthermore, when the items of information desired are stored separately in the files of many different agencies, or when one does not know in which of many agencies the information is stored, each of those separate agencies must presently be contacted in order to obtain the information. The centralization or interconnexion of computer files could negate this restraint by making possible 'one-stop shopping' for all information about an individual. Such a system could provide a complete personal dossier on any individual which would include such information as welfare status and history, income (total and/or by sources), credit rating, grade average or class standing, recommendations and references, police record, security or other investigative reports, involvement in civil or criminal court action, medical history, psychiatric history, personality inventory, alcoholism or drug addiction, food purchases and consumption, and consumer preferences." 81/

90. A dual aspect of centralization has been described:

"centralization of private information and its preservation in computer memories may decrease illegitimate leaks of that information. Those who will have access to personel history will see much more of it than was usually the case when it was contained in printed records, but fewer curious eyes will have knowledge of any part of the private history of the individual." 82/

80/ United States, Report of the National Academy of Sciences, p. 255. This conclusion appears to be confirmed, in general, by the survey of managerial opinion of computerized systems in 14 fields of public and private activity (ibid., pp. 437-441).

81/ UCLA Research, p. 1441.

82/ Michael, loc. cit., p. 280.

91. The World Health Organization has stated the following in relation to the medical records of an individual:

> "In practice they tend to be distributed amongst various holders - but in the future, they will tend to be more centralised and computerised. Under such circumstances, they will constitute an area of special sensitivity, if access to them is not controlled and restricted. The sensitivity will perhaps be greatest where records of consultations with psychiatrists or psychoanalysts are entered in the file." 83/

92. On the same lines, attention has been drawn to the danger to the individual of allowing a governmental authority to have access to such a mass of information about him as can be contained in a computer, if the information is collected from all the official agencies that already have elements of such data. It has been claimed that:

> "even authorized use by the Government itself of this mass of data raises the specter of a government which knows all or which, having found that it does not know enough, devises further methods of obtaining the portion of the data which is still missing. One of the important features of a democratic government is the doctrine of the separation of powers which makes it difficult for any branch of the government to jeopardize the fundamental rights of the individuals. Certainly, at present, the multiplicity of agencies and procedures and the resulting red tape protect the individual against undue invasion of his privacy by making it more difficult for various government officials to know enough to cause real trouble. But if all the available data are integrated and stored in a computer in a way permitting instantaneous access to the record of each person, a sword of Damocles is going to hang all the time over the head of everybody." 84/

93. It has also been said that:

> "the centralization of information from widely divergent sources and on markedly different subjects, as often results from establishing large data banks, creates serious problems of contextual accuracy. A large corporate or welfare data bank may contain information on a person's education, military record, medical history, employment background, aptitude and psychological testing performance, as well as a number of subjective appraisals of his character and skills. Any of this information might be entirely accurate and sufficient when viewed from one perspective but be wholly incomplete and misleading when read in another." 85/

94. In the report of the United States Department of Health, Education and Welfare, it was estimated, however, that "the possibility of using a large computer to assembly a number of data banks into a master file" so that "a dossier on nearly everybody could then be extracted" is "currently remote" and that at present it

---

83/ A/8055/Add.1, para. 27.

84/ Commission to Study the Organization of Peace, The United Nations and Human Rights, Eighteenth Report (New York, 1967), pp. 41-43.

85/ Miller, op. cit., p. 33.

presents various problems "that few organizations, and probably no organization outside the Government, have the resources to solve". 86/ It has been stressed, nevertheless that:

> "public concern about such combinations of data through linkings and mergers of files is well founded since any compilation of records from other records can involve crossing functional as well as geographic and organizational boundaries. When data from an administrative record, for example, become part of an intelligence dossier, neither the data subject nor the new holder knows what purpose the data may some day serve. Moreover, the investigator may believe that no detail is too small to put into dossier, while the subject, for his part, can never know when some piece of trivia will close a noose of circumstantial evidence around him. Public sensitivity to the possibility of such situations argues strongly for preserving the functional distinctions between different classes of personal data systems." 87/

E. Accumulation of personal data

95. The capacity of the computer to accumulate more data, in comparison with traditional filing methods, presents two aspects. First, at the level of collection and storing of data, computerization allows the speedy gathering of a great number of facts, at the same time substantially reducing their storage-space. The computer memory is able to store large quantities of data and preserve them for a long time and, for these reasons, some data gathering, which under traditional methods did not pay, now becomes economically profitable. Secondly, the computer, by its capability of combining the information contained in various files, permits the users to acquire not only simultaneously certain information relating to one individual but to merge this information 88/ to obtain a more complete picture of his personality.

96. In the report of the Commission on Publicity and Secrecy of Official Documents submitted to the Swedish Ministry of Justice 1972, the Commission stated that:

> "automatic data processing makes it possible to collect and survey very large quantities of information. Information may cover a very large number of individuals and contain a great many things about each. The facts may be kept up to date and accessible to an extent that was quite impossible before the ADP technique. The information can be stored for a very long time and still

---

86/ United States, HEW Report, p. 21. A similar conclusion had been reached in the report of the National Academy of Sciences: "our survey findings about data integration support the notion that the kind of 'total' integration many civil libertarians fear has not yet occurred in most organizations, be they small and new to computers or the largest and most advanced computerizing institutions" (United States, Report of the National Academy of Sciences, p. 429).

87/ United States, HEW Report, pp. 21-22.

88/ Braibant, loc. cit., p. 798.

kept accessible. Registers can be centralized to a very high degree, which makes it much easier to find a certain fact." 89/

97. In the same report, it was also pointed out that if some information is of a specially sensitive character (such as facts about crimes, statements of opinions and attitude, evaluations and judgements or facts concerning the finances of individuals), "even the collection and compiling of large quantities of information, each item of which is trivial in itself, may affect the privacy of the individuals concerned". 90/

98. The development of scanning devices by their capacity for selecting in information retrieval and for reduction of the quantitative dimensions of information that may otherwise be too unwieldly to handle, would limit such protection as may be afforded by the volume of information and the difficulty in operating on it. For example, the following forecast has been made:

"On the horizon in technology is a laser scanning process that would enable a twenty-page dossier to be compiled on each of the 200 million citizens of the United States. Such information could be stored on a single plastic tape reel. Under such conditions, it might be cheaper to retain data than to discard it." 91/

99. The ability of computers to absorb large quantities of information has been viewed as encouraging the collection of more personal data, pertaining to the private sphere of the individual. It has been said in this connexion that "because information is now so easy to store in the various forms of computer memory, bureaucrats have an increasing temptation to ask more questions about the individual. 92/ It has also been said that "as capacity for information-handling increases, there is a tendency to engage in more extensive manipulation and analysis of recorded data, which, in turn, motivates the collection of data pertaining to a larger number of personal matters". 93/

89/ Sweden, Computers and Privacy, pp. 5-6.

90/ Ibid., p. 5.

91/ R. C. Brictson, "Computers and privacy - implications of a management tool" (Santa Monica, Cal., System Development Corp., 1968), doc. SP-2953/001/00, cited in Lance J. Hoffman, "Computers and privacy: a survey", Computing Surveys, vol. 1, No. 2 (June 1969), p. 87.

92/ R. V. Jones "Some threats of technology to privacy", paper prepared for the Third International Colloquy about the European Convention on Human Rights, held at Brussels from 30 September to 3 October 1970 on the topic of modern scientific developments and their consequences on the protection of the right to respect for a person's private and family life, his home and communications (H/Coll. (70) 2/2, p. 13).

93/ Arthur R. Miller, "A transparent society", International Herald Tribune, 6 August 1969.

100. The process of enlarging the capacity of an organization to process more information by computerization has been analysed from the point of view of economic incentive. The cost of setting up a computerized system tends to encourage a manager to spread the initial cost over as many fields of data-processing as possible. 94/ It has been further pointed out that:

> "An early incentive to concentrate on efficiency may also foster a tendency to behave as though data management were the primary goal of a computer-based record-keeping operation. When this occurs, unnecessary constraints may be placed on the gathering, processing, and output of data, with the result that the system becomes rigid and insensitive to the interests of data subjects. A commonly observed tendency in these situations is to make the data subject do as much of the data collection work as possible by forcing him to decide how to fit himself into a highly structured, but limited set of data categories (e.g., 'Please check one of the following boxes.').
>
> "This can be a way to cut down errors in transcribing data from one form of record to another, but when done solely in the interest of economy the system may well sacrifice flexibility and accuracy. It is true that data compression and 'shorthand' record entries did not originate with the computer; ill-adapted categorization has been the bane of bureaucracy for generations. However, manual record keeping can, at the stroke of a pen, take account of data that do not fit comfortably into pre-conceived categories, while a computer record is not usually amenable to any sort of annotation that was not expressly planned for in the design of the system." 95/

101. As modern organizations develop indicators of institutional performance and plan for the future, they are increasingly resorting to personal data not only for their administrative purposes, but also for statistical and research purposes. Thereby a new incentive for the accumulation of a larger amount of personal information comes into existence. While personal data collected for administrative purposes should be limited to data relevant to decision making about individuals, a substantial amount of such data "appear to be collected because at some point someone thought they might be 'useful to have', and found they could be easily and cheaply obtained on an application form, or some other record of an administrative transaction". 96/

102. The view that "once an organization purchases a giant computer it inevitably begins to collect more information about its employees, clients, members, taxpayers, or other persons in the interest of the organization" 97/ has however been contested after the investigation of the 55 most advanced organizations in the field of computerization of personal records in the United States; it was pointed out that

---

94/ United States, HEW Report, p. 13.

95/ Ibid., pp. 13-14.

96/ United States, HEW Report, p. 79.

97/ Alan F. Westin, op. cit., p. 161.

"the organizations that we visited have not extended the scope of their information collection about individuals as a direct result of computerization" 98/ but for other causes. 99/

103. Another aspect of the ability of computers to store, analyse and retrieve large amounts of personal data has been described as leading to its use as an instrument of surveillance 100/ or "cyberveillance", "to mean constant surveillance using the methods of cybernetics - computers monitoring a situation, processing data they collect, and taking action when they detect particular circumstances". 101/

104. In this connexion it has been said that:

> "Cyberveillance to spot tax-evasion, on the face of it, sounds like a good idea. Programs in computerized telephone exchanges for tracing malicious anonymous callers (a system currently in use in Sweden) are highly commendable. Computerized surveillance to help crime-detection appears to be potentially valuable. But how far should this be taken? Most citizens would react indignantly to the proposal that a computer monitor their bank account or credit transactions for unusual activity. How would we feel if we knew that a computer were analyzing all the telephone numbers we dial as an aid to national security, crime-detection, or for some obscure bureaucratic motive?" 102/

According to one writer:

> "The computer can and is being used to analyze seemingly unrelated data on large numbers of people to determine whether a particular individual's activities bear any relation to the conduct of other investigation subjects or groups." 103/

105. Attention has been drawn to the combined threat to human rights posed by the existence of new methods for the clandestine collection of information and the possibility of storing such information in computers (see E/CN.4/1116, paras. 128-130). In the report of the Canadian Task Force, it has been also pointed out that "surreptitious listening and watching devices have been identified as an especially harmful method" 104/ of collecting personal data. With respect to the same combination between computers and surveillance devices, the following question has been asked:

98/ United States, Report of the National Academy of Science, p. 249.

99/ Ibid., pp. 248-249.

100/ Miller, The Assault on Privacy, op. cit., pp. 38-46.

101/ Martin and Norman, op. cit., p. 354.

102/ Ibid., p. 355.

103/ Miller, op. cit., pp. 41-42.

104/ Canada, Privacy and Computers, p. 149.

"Will all that information, obtained clandestinely without the knowledge of the individual, be fed into computers in addition to information from official sources? Even if legislation has been enacted prohibiting such information from being fed into computers, will there not be parallel computers, just as there are 'parallel' departments, which will have information of that type?" 105/

106. With regard to transnational systems, mentioned in paragraph 45 above, it has been felt that the threats to privacy, presented by the large amount of data stored in these systems, much of which is sensitive, are less important than other human rights problems. In this connexion, the report of the Canadian Task Force, after mentioning that 13 computerized systems in the United States hold extensive data about Canadians, goes on to state:

"The principal problem, then, is not one of the privacy of Canadian data subjects being invaded by data about them stored in the United States. It is rather... /inter alia/ that data in United States databanks might be peremptorily withheld abroad for a variety of reasons, including security regulations, court injunctions, etc.; that United States laws might change and leave Canadians less well protected..." 106/

107. In addition, the observation has been made that the non-existence in certain countries of legislation protecting the rights of individuals against the threats and problems arising from the use of computerized personal data systems, or the existence of less strict regulations in this field, might induce agencies operating such systems to establish them in the territories of such countries, so as to evade stricter domestic requirements of their own countries. 107/ As one writer has put it:

"It would not be long before computer centres and data banks were set up in territories whose legislation was less strict, or even non-existent, near to large States which had adopted effective legislation, and the consequence might be a mushrooming of Renos or Las Vegases of the computer world." 108/

F. Computer personnel as a new category of record keepers

108. The dangers for human rights of the existence of specialized data-processing professionals in an organization resides partly in a possible trend to create a group therein whose interests are served by any increase in data use, without sufficient regard for the intrinsic value of the increased use, and to treat questions of record-keeping practice, which involve issues of social policy, as if they were little more than questions of efficient technique. 109/

105/ Pierre Juvigny, "Informatique et droits de l'homme", L'Informatique dans l'administration, published by the French Institute of Administrative Sciences, June 1969, p. 91.

106/ Canada, Privacy and Computers, p. 171.

107/ Ibid.

108/ Braibant, loc. cit., p. 817.

109/ United States, HEW Report, p. 23.

109. The position of the programmer, which gives him a key role in relation to the issue of privacy, has been considered to deserve special attention:

> "No one using the output from a computer needs to know as much about the data fed into it as does the programmer. Without intimate and extensive understanding of the data and the uses to be made of it, the programs which determine how the computer operates, and hence the quality of its output, will be crude. On the other hand, executive decisions often depend less on knowledge of details than on overall grasp of the situation. As a result, the programmer often will be the person with potentially the most intimate knowledge of the private lives of those whose data is processed. This potentiality need not result in his having specific knowledge about specific people, since a programmer is unlikely ever to see the materials which are input to the computer whose processes he has arranged. But given his deeper understanding of how the data are being processed, what assumptions are made about the relationships among the data, what constraints must be put on the data in order for the computer to use it, it is entirely possible that the programmer may be called upon in difficult cases to enrich the executive's basis for decision making. In this way, the programmer may become privy to very private information about specific individuals. There may then arise a demand for programmers with ethical standards which now are not considered prerequisites to their trade. Inevitably, of course, there will be corruptibles among this group who will leak private information." 110/

110. Writers have also stressed the danger of technocratic monopolization of power, which arises from the development of computers as also from certain other technological developments. According to one scholar:

> "Computer and information specialists are not simply white-collar mechanics. They have begun to perform many disparate roles and to assume managerial functions that range far beyond the activities we normally associate with people in technical positions. In the future programmers and systems operators will be given responsibilities that completely transcend the mundane tasks of collating and disseminating data or overseeing machine operations. With greater frequency they will be called upon to participate in information analysis and the decision-making process. Today's computer expert may emerge as tomorrow's information policy maker because the volume and variety of electronically processed data will be too great, the methods of storing and manipulating the information too complex, and the technical language too arcane to enable scientifically naive executives and public officials to maintain effective control over the activities of the information systems within their own institutions.
>
> "Eventually, the governance of data centers may fall into the hands of those we now jokingly refer to as 'computerniks', creating a danger that policy will be formulated by information managers who are so entranced with operating sophisticated machines and manipulating large masses of data that they will not be sufficiently sensitive to privacy considerations." 111/

110/ Michael, loc. cit., p. 279.

111/ Miller, op. cit., p. 253.

G. Decision-making on people based on computerized data and evaluations (due-process issues)

111. The making of decisions about the rights, benefits and privileges of individuals in various fields (such as employment, professional careers and education), based on computerized data and evaluations has been viewed as giving rise to threats to human rights.

112. From a procedural point of view (or procedural due process), it has been felt that the use of computerized data would lead to more decisions being made about individuals without their knowledge and without giving them the necessary opportunity for inspection or challenge. 112/ It has, however, been stated, on the basis of visits to the 55 of the most advanced organizations in the United States, that computerization of personal records had not modified the pre-existing rules of notification and access and that new legal rules of procedural due process have been followed equally well, or poorly, in computerized and manual file systems. In addition, the public debates over records and computerization have had the effect of increasing both public and individual awareness of the existence of files during the past decade. 113/

113. With respect to "substantive due process issues", fears have been frequently expressed that computer systems "will replace 'human judgement' with dangerous 'machine rigidities' and therefore introduce a new element of arbitrariness into decisions about individuals" and that decision makers would be inclined to treat "print-out" as the absolute truth and rely exclusively on it, instead of judging "the whole person". 114/ As one scholar has put it:

> "There remains the problem of the decision-making powers of governments as they involve citizens. Without entering the realm of science-fiction - as in Jean-Luc Godard's film 'Alphaville', in which people were condemned to death by a computer for illogical conduct - one may anticipate that as a result of the use of computers, decisions affecting the lives of individuals might be taken in an authoritarian and mechanical fashion, in such fields as counselling on school and university courses; one might also imagine the progress of staff member's career being entirely subject to the calculations of a computer." 115/

On the same lines, another writer pointed out that:

> "The convenience of referring to computer-stored evaluations and increased time pressures may lead decision-makers to abdicate their responsibility for making important judgments in a rational, thoughtful manner or to return to original sources to verify, update, and seek out more or better data. True, most information users insist that they understand that the computer's utility

---

112/ United States, Report of the National Academy of Sciences, p. 256.

113/ Ibid., p. 259.

114/ Ibid.

115/ Guy Braibant, "L'informatique dans l'administration", paper presented at the IXth Congress of the International Association of Democratic Jurists (Helsinki, 15-19 July 1970), p. 10.

and a data base's reliability necessarily are limited by the quality of the input, typically emphasizing their alleged awareness by reciting the maxim 'garbage in, garbage out' (GIGO). Nonetheless, the hypnotic effect of being able to manipulate enormous data bases is likely to encourage people to use the computer as an electronic security blanket and to view it as a device for quantifying the unquantifiable." 116/

114. As far as the above-mentioned threat is concerned, the report of the National Academy of Sciences of the United States mentioned three types of decision situations: situations where information to be weighed is essentially objective and fast action is needed; situations where the organization has more applicants for a given programme, service or benefit than it can accommodate and has developed certain objective minimum criteria for identifying individuals whom it wants to select (such as certain levels of salary or income, certain academic degrees); and situations where the organizations concerned could not work on the basis of standardized, objective criteria alone, but have also to weigh subjective characteristics and acquire direct knowledge of the person by interviews or self-descriptions by those being evaluated.

115. The report concluded that, in all these cases, no substantial changes had taken place in the organizations visited; in comparison with the previous situations under manual systems and that a strong awareness on the part of organizational personnel of the possible errors that hardware, software and operator failures could create in computer-generated output did exist. 117/ The report further emphasized that "our basic finding is that we did not find 'print-out' being used to sort and sift people in some automatic fashion in decision-making settings where more personalized and subjective decisions were typical in the manual era". 118/

116. The use of computer coding in organizational decisions about people (i.e., the use of data compression and "shorthand" record entries which was referred to in paragraph 100 above) would have a harmful effect on the decision process, "by causing organizational evaluations to 'force-fit' people into categories that do not reflect the subtleties that a narrative record might convey". 119/ It has been, however, contended, on the basis of the visits to the 55 of the most advanced organizations in the United States that although the computerization of records has in no way discouraged the use of code numbers and abbreviations or labels, as for instance, "troublemaker", "unruly child", "heavy drinker", "subversive", which can have harmful effects on decision making about individuals' careers, privileges and benefits, it did not appear, from the organizations visited, that this had led to any greater misuse of shorthand notations than was present in the manual systems. 120/

116/ Miller, op. cit., p. 37.

117/ United States, Report of the National Academy of Sciences, pp. 260-263.

118/ Ibid., p. 264.

119/ Ibid. See also, United States, HEW Report, p. 14.

120/ United States, Report of the National Academy of Sciences, p. 266.

117. According to a general assessment made in the report of the National Academy of Sciences of the United States "most of the decisions about people are still being made with the aid of manual records today, and it is here the civil-liberties issues will remain heavily centred for several years to come", 121/ as "the more subjective information used by organizations to make judgements about people - in law enforcement intelligence, personnel work, medical diagnosis, educational advancement, etc. - is not yet being put into computers". 122/

H. Problems arising from the use of statistical and research computerized systems

118. As mentioned in paragraph 25b above, in statistical and research systems, the identity of the person concerned is eventually separated from the data in the record. It might be supposed therefore that threats to privacy, and mainly those related to unauthorized disclosure, could be reduced in these systems, by maintaining a strict separation between the person's identity and the data output in aggregate form.

119. However, it has been maintained by some writers that it is unrealistic and impractical to depend, for much of the statistical storage and calculation desired by governmental agencies and private organizations, on computers having only a limited capacity to identify the individual. Two basic reasons have been given for this. First, many of the advantages, such as economy and availability, accruing from a centralized computer system are said to be based on the desirability of the integration of information from diverse sources into individually identifiable records in order to correlate even purely statistical information to the fullest advantage. According to this view:

> "Even though no scientific interest exists in examining the response of a single individual, it is necessary, in order to compute the over-all relation between, for example, income and education, to match an individual's income with his years of education.
>
> "The requirement for matching means that each individual record in the data centre must be identified, as by a social security number or, better (for guarding privacy), a special code number. Thus is it always theoretically possible to extract from a data centre information referring to a particular individual. This is true whether the centre is characterized as a 'statistical data centre' or as an 'intelligence or dossier file'." 123/

121/ Ibid., p. 251.

122/ Ibid. The data from the survey of managerial opinions of 2,121 organizations in 14 fields contained in the Report of the National Academy of Sciences tend to confirm this estimation (ibid., pp. 924-927).

123/ Sawyer and Schechter, loc. cit., p. 815.

120. Secondly, the need to keep up to date the information even in a statistical data bank requires the use of individually identifiable records. This aspect has been described as follows:

> "The data bank is essentially a pool of information stored in a computer. It may be a static pool, that is, the result of a one-time collection of information, such as the census or a voter survey or the records of a particular social science experiment. This is not the central type of data bank with which we are concerned. Rather we are concerned with what has been called the dynamic data bank, a body of data which is constantly being updated and added to by further collections of data. ...
>
> "Typically, the output of a statistical data bank is data which does not contain identifying characteristics about any individual. However ... the need to keep such statistical data banks updated requires that identifying characteristics of the individual be retained in the system, so that new and additional data can be added to his file." 124/

124/ Alan F. Westin, "Discussion memorandum on legal aspects of privacy in computer data banks" (October 1968), pp. 3-9, a paper prepared for the Privacy Committee of the American Civil Liberties Union.

IV. EXISTING AND PROPOSED SAFEGUARDS

121. There is general agreement as to the need for an extensive set of safeguards to protect human rights against threats arising from the use of computerized personal data systems and to achieve a rational balance between the benefits which accrue from the use of these systems and the preservation of the rights of the person.

122. Provisions on safeguards are included in existing and draft legislation, in regulations governing the agencies operating computerized personal data systems and in codes of professional ethics. Certain safeguards are applied in practice by computing organizations. Various safeguards are also proposed in the "Principles concerning the protection of privacy with regard to electronic data banks in the private sector" contained in a draft resolution submitted in 1972 to the Council of Ministers of the Council of Europe 125/ and in the literature concerning the impact of computerized personal data systems on human rights.

123. Safeguards which are applied or suggested have been classified in the following main categories: physical security measures, technological safeguards, administrative (managerial or organizational) practices, professional safeguards and legal safeguards. 126/ It is, however, difficult to draw a precise line between administrative and legal safeguards, because both imply the establishment of rules prescribing a certain behaviour for those concerned. Therefore what are sometimes designated as "administrative safeguards" will be included below under the heading of legal safeguards (subsection 2, "Rules providing for safeguards relating to operational activities of computerized personal data system").

123a. Attention has been drawn - especially in the report of the National Academy of Sciences of the United States - to the fact that any forging of safeguards would involve a balancing process among competing human rights values and competing social values:

> "/G/iven the great diversity of record-keeping goals, practices, and content that we have shown to characterize organizational life; given the fact that not all record-keeping systems present the same issues of civil liberties; and given the fact that the social balance between individual privacy claims and organizational needs for information shifts markedly from one record-keeping area to another, and through different periods of national life, it appears clear to us that no single law, constitutional amendment, or court decision can cope with the tremendous diversity of issues and settings, and the uneven readiness for corrective action,

---

125/ The text of the draft resolution is reproduced in paragraph 319 below.

126/ See, for instance, OECD Report, paragraphs 31-81; Canada, Privacy and Computers, pp. 103-177; Miller, op. cit, pp. 169-258; Allan Campbell and Allan Woods, "Computers and Freedom", Law and Computer Technology, (June 1969), p. 6.

that make up the current data-bank problem. Such total solutions are not worth pursuing. There are some important policy actions covering broad segments of record-keeping that may be called for ... But a healthy skepticism toward all-at-once remedies is strongly suggested by our studies." 126a/

124. With regard to the extent of safeguards needed to protect the right to privacy it has been pointed out that the type of the computerized system has to be taken into account. Intelligence and other types of computerized personal data systems, storing sensitive information, would normally require a far more developed set of safeguards than the statistical systems. 127/ It has to be noted, however, that intelligence systems have been sometimes considered, for security reasons, to represent a special class which would normally be excluded from any general regulatory process 128/ or submitted to it with certain exceptions specifically sanctioned by the law. 129/ Such exceptions were explicitly provided in the Data Surveillance Bill (United Kingdom 1969) 130/ and in the draft bill on protection against the misuse of personal data in data processing (Federal Republic of Germany 1972). 131/

A. Physical security measures

125. Physical security measures have a wide range, from measures directed at the protection of the buildings or rooms where computers are installed to measures for the physical protection of files. 132/

126. Control over access to the buildings and rooms where computers are located is required to protect the equipment from destruction or theft or to prevent strangers from viewing data while being printed or displayed. The major security measures in this respect include locked doors to the computing centres, guards and identification measures (such as authorization badges). 133/

126a/ United States, Report of National Academy of Sciences, pp. 350-351.

127/ See, for instance, Alan F. Westin, "Legal safeguards to insure privacy in a computer society", Communications of the ACM (Association for Computing Machinery), vol. 10, No. 9, (September 1967), p. 536.

128/ Canada, Privacy and Computers, p. 158.

129/ United States, HEW Report, pp. 74-75.

130/ See paragraph 198, below.

131/ See paragraph 241, below.

132/ See Canada, Privacy and Computers, pp. 102, 106-107; United States, Report of the National Academy of Sciences, pp. 125-126; Martin and Norman, op. cit., p. 497.

133/ Other measures are alarm indicator panels, closed circuit television systems and, at central control points, bullet proof glass and guard stations with consoles controlling interlocked double-door entries and exits (United States, Report of the National Academy of Sciences, p. 126).

127. As to the physical protection of the files, of locked cabinets and vaults, some of the measures recommended or effectively applied are burglar proof tape stores, document shredders, and the storage of magnetic tapes containing sensitive data at remote locations. 134/

128. From official and unofficial surveys of computerized personal data systems in Canada and in the United States it appears that high priority has been given to the use of physical measures, in comparison with other safeguards. 135/

129. The "Notes of guidance for local authorities", issued in the United Kingdom, have recommended inter alia the following physical security measures: physical access to the computer room should be restricted to essential personnel, whose names should be placed on a list at the disposal of the reception staff; existing security systems should be alerted to the need for special attention to be paid to the computer room after normal service hours; terminals should be sited in offices to which unauthorized personnel cannot gain access; printers, terminals and consoles should be sited away from doors and windows; printed output from aborted runs should be made illegible before being disposed of. 136/

130. In the report of the United States Department of Health, Education and Welfare, it has been recommended that any organization maintaining administrative, statistical and research automated personal data systems should take reasonable precautions to protect data in the system from any anticipated threats or hazards to the security of the system. It was explained that the purpose of this requirement was to assure that these organizations take appropriate security precautions against unauthorized access to data in the system, including theft or malicious destruction. 137/

B. Technological safeguards

1. Definitions and purposes

131. Technological safeguards are the technical security means of protecting the accuracy of the data stored in a computer and of preventing any unauthorized alteration or modification and unauthorized outside or inside access. 138/

134/ Martin and Norman, op. cit., p. 497, United States, Report of the National Academy of Sciences, p. 126.

135/ In Canada, three quarters of the 1,268 organizations, which replied to the questionnaire of the Task Force, had controls over physical access to the equipment (Canada, Privacy and Computers, pp. 26, 34). See also, United States, Report of the National Academy of Sciences, pp. 309, 442-444.

136/ United Kingdom, LAMSAC, Computer Privacy, p. 10.

137/ United States, HEW Report, pp. 55 and 58.

138/ Cf. Reinturn and Norman Z. Shapiro, Privacy and Security in Data Banks Systems: Measures of Effectiveness: Costs and Protector-Intruder Interactions (Santa Monica, California, the Rand Corporation, July 1972), pp. 8-9.

132. It does not seem possible to put forward general criteria regarding the extent of technological safeguards needed for a given field of record-keeping or for particular organizations. The observation has been made that no minimum set of technological safeguards can be specified in the abstract for computerized files in all types of organizations, as the level of protection required depends on its particular characteristics. 139/ The fact that a large or complex system usually contains information of a differing degree of sensitivity may also render difficult the process of deciding how sophisticated a set of technological safeguards is necessary. In addition, it is often not possible to predict the character of future security problems at the initial stages of development of various systems, since they change their purposes and dimensions over the course of time. 140/

2. Various technological safeguards

(a) Integrity management

133. A vital technological safeguard has been considered to be the "integrity" of a computerized system, that is to say the means to ensure that it works as planned. For this purpose, the installation of the system must include a thorough initial testing of the hardware and software, followed by routine inspections. Standard procedures should be worked out for inspecting the system, particularly when modifications are introduced. 141/

134. The manufacturer should bear the responsibility of designing and providing a computer with appropriate technical capabilities to afford the necessary protection against exposure of private files or the opportunity of unauthorized access to them. The machine should be endowed, therefore, with certain features, some of which are already normal practice whereas others should be applied. For instance, a time-sharing computer must have absolute protection within the central processor so that no job can be inadvertently corrupted by any other operating at the same time. 142/ Therefore, "the operating system supplied by the computer manufacturer should be shown to contain precautions against programs in a multi-programming environment interfering with one another and against output appearing at a wrong point in the system". 143/

139/ United States, Report of the National Academy of Sciences, p. 393.

140/ Miller, op. cit., p. 241.

141/ OECD Report, para. 40; Petersen and Turn, loc. cit., p. 294.

142/ Warner and Stone, op. cit., pp. 198-199.

143/ United Kingdom, LAMSAC, Computer Privacy, p. 11.

(b) Technical means for the protection of the identity of the individual to whom the information relates

135. Threats to privacy from inside or outside intruders may be prevented or reduced if the access to the individual's identity to whom the information relates can be restricted. Such a protection has been recommended especially for statistical computerized systems, where the identity of the individual is not relevant for the use of the information they store.

136. One of the means to restrict access to an individual's identity is to ensure that files appear only with a special code number, not with the name or other easily identifiable indication of the individual. The code number and the name or other identifiable indication should be brought together only at the time of data input. Except when new data are being recorded the computer should prevent access to the code number. This might be accomplished by a time-lock, which would permit the operation to take place only at certain times. 144/

137. For statistical systems, it has been recommended that the data be put into the system in small aggregates, rather than in individualized units, thus protecting anonymity. In this way, no data on a single person could be traced with certainty. 145/ It has been also suggested that, for these systems, modern sampling techniques would make it possible to reach statistically valid results, without analysing everyone's responses. Therefore, a random sample could be used, thereby making it unlikely that a successful intrusion will yield a dossier on a particular person. 146/

138. The report of the Younger Committee has recommended the following principle: "In computerized systems handling information for statistical purposes, adequate provision should be made in their design and programmes for separating identities from the rest of the data." 147/

(c) Technical means to identify authorized users

139. In order to restrict the access to the information contained in a computerized personal data system only to authorized users, they should be duly identified. For this purpose various technical methods are used or suggested.

140. Physical keys, to be read by the machine before requests are honoured, may consist of badges, keys, plastic cards with punches, indicating the types and quantities of data to which the holder is entitled, or of magnetically coded identification cards, including cards designed to receive new invisible code numbers after each transmission. As such cards can be lost, stolen or mislaid, they do not

---

144/ Sawyer and Schechter, loc. cit., p. 816.

145/ Ibid.

146/ Ibid. See also Miller, op. cit., p. 251.

147/ United Kingdom, Younger Report, p. 183, para. 594.

seem to offer sufficient protection against unauthorized access to the computerized files. 148/

141. Passwords or code numbers can be allotted to each authorized user of a time-sharing system. Access to the system is made possible only by using the proper password. The computer provided with a monitor programme establishes automatically whether the password or code number is correct. Only after such verification may the user gain access to the system or to a particular file, depending on the extent of the authorization conferred by the password. 149/

142. To increase the level of security, passwords should be frequently changed. For the same purpose, the use of random numbers has been suggested. 150/

143. In the "Notes of guidance" issued in the United Kingdom for local authorities, it has been stressed that: "The protection afforded by the hardware and software will undoubtedly ensure that files, sub-files or records are only open to authorised enquirers who will be identified by a terminal number, and/or a password, and/or a key, and/or a badge. There may or may not be hardware or software features which inhibit the display of the password in a legible form, and there may or may not be features which permit an authorized user to open his files to another person without disclosing his password." 151/

144. It has been felt that the use of computer passwords and locks could make "adequately sure that only authorized persons can gain access to information in the register and only to the extent authorized". 152/

145. The use of keys and passwords in computerized personal data systems seems to be widespread. In Canada, for instance, of 475 organizations which, responding to the questionnaire sent by the Task Force, gave information about their security systems, 38 per cent used some kind of hardware/software security measures such as passwords. 153/ The Government of Belgium reported that a secret key is used in the computerized personal data system operated by the Régie des Postes et Régie des Télégraphes et les Téléphones 154/ and that one of the computers operated by the

---

148/ See UCLA Research, p. 1445; Miller, op. cit., p. 243. See also, for the various types of physical keys, Martin and Norman, op. cit., p. 485.

149/ Miller, op. cit., p. 243, Canada, Privacy and Computers, p. 103; Martin and Norman, op. cit., pp. 485, and 487-488.

150/ Warner and Stone, op. cit., p. 204.

151/ United Kingdom, LAMSAC, Computer Privacy, p. 8.

152/ Legal Aspects of the Protection of Privacy in View of the Increased Compilation of Personal Data into Computers and other Registers, report presented by K. Axel Nielsen, Minister of Justice of Denmark at the Seventh Conference of the European Ministers of Justice (Basle 15-18 May 1972), p. 5 (furnished by the Government of Denmark on 21 February 1973).

153/ Canada, Privacy and Computers, p. 103.

154/ Information furnished by the Government of Belgium of 22 February 1973.

Ministry of Justice, which is used also for centralizing data about individuals (for instance, persons being sought after) has been designed in such a manner that only the authorities which had previously possessed the information may have access to that information. 155/ The Government of Italy reported that in the system for computerization of central criminal records being installed at the Ministry of Mercy and Justice, access to the archives is possible only by the use of key words known only to authorized personnel, who are bound by the strictest official secrecy. 156/

146. It has been maintained, however, that passwords offer about the same level of security as the normal locking of a filing cabinet with a key, as passwords are subject to unauthorized disclosure or can be lost or stolen. They should be therefore combined with other technological safeguards which have sometimes been applied or suggested 157/ such as: an alphanumerical access code 158/ which would be known only to the recipient and could not be easily taken surreptitiously and could be also regularly changed; 159/ a "fail-safe" system, which requires several users to insert keys in a terminal before certain files are made available and is considered better than simple keys, because "the snooper is required to subvert a larger group of persons to gain access". 160/

147. Other methods of user identification have been further suggested: (a) visual identification of the user, by installing a closed circuit television channel between the terminal and the central processor; (b) fingerprint or voiceprint readers, requesting the user to place his finger on a special "reader" or speak into a microphone, so that the computer may translate the fingerprint or the voice onto a set of electronic signals which would be compared with those stored in the computer for that particular individual; (c) answer-back systems, which would require the user to respond to one or more randomly chosen questions, as a technique coupled with fingerprint or voiceprint reading. 161/ It seems, however, that the techniques of visual identification would be comparatively costly and cumbersome and would require constant monitoring. 162/ Fingerprint or voiceprint readers are either

---

155/ Information furnished by the Government of Belgium on 15 February 1973.

156/ Information furnished by the Government of Italy on 17 July 1973.

157/ Martin and Norman, op. cit., pp. 487-488.

158/ An alphanumerical code is a system in which either letters of the alphabet, numerals or symbols may be used (Arnold, Hill and Nichols, op. cit., p. 359).

159/ This type of access number is presently in use at the UCLA computer complex and is considered as both inexpensive and successful (UCLA Research, p. 1446).

160/ Miller, op. cit., p. 244. The author mentions that this system is applied in the banking industry.

161/ UCLA Research, p. 1445; Warner and Stone, op. cit., p. 295. In 1971, the Community Systems Foundation of Ann Arbor was testing a system that identifies users by a combination of physical characteristics and responses to questions asked to the user (Miller, op. cit., p. 323).

162/ Miller, op. cit., p. 244.

described as being used experimentally, but not publicly available 163/ or as presenting the defect that a person's voice may be easily recorded and replayed and fingerprint likewise obtained and duplicated. 164/ It has been said that the coupling of these devices with an "answer-back" system would afford a high enough level of security, as each safeguard would reinforce the others. 165/

(d) Technical means of preventing the infiltration of a computerized system and technical access restrictions

148. The information itself contained in a computerized personal data system should be protected by technological safeguards to prevent attempts of penetrating the system from outside and to restrict access to certain files.

149. For instance, for information which, by its sensitivity, may be thought to attract the use of electronic surveillance devices for eavesdropping on radiations from the equipment, the physical surroundings of the central processor and its remote terminals may be protected with shielding materials, such as metalized paper or by reducing the amount of radiation by circuit suppressors or filters. Procedures of this type are being used in, inter alia, communications centres around the world. 166/

150. It has been said that not all information stored in a computer may need the same degree of access restriction. Some refer to matters of public record, that are expected to be open to virtually everyone; others are of a confidential nature, thus having a limited usage; a third category consists of security information, given under the expectation of complete non-circulation, or obtained by physical and psychological surveillance. 167/

151. Taking into account the various levels of its sensitivity, it has been suggested that the information should be arranged and stored on an hierarchical basis and that mechanical controls should be built into the hardware and software of the central processor which could thus limit a particular user's ability to reach into certain computer files. 168/

152. Such mechanical controls (called also "programmed locks on data files") 169/ have been described as consisting in "partitioning" the working storage of a time-sharing system, so that each user and his working programme have access only to a

---

163/ Martin and Norman, op. cit., p. 485.

164/ UCLA Research, p. 1445.

165/ Miller, op. cit., p. 244.

166/ Miller, op. cit., p. 241.

167/ Westin, loc. cit., p. 536.

168/ Miller, op. cit., p. 242; Canada, Privacy and Computers, p. 105.

169/ Martin and Norman, op. cit., p. 487.

limited part of the computer's memory. This scheme can be reinforced by a monitor programme, built in the computer's software. Such a programme can be designed to include "privileged commands" or "privileged instructions", which limit access to ordinary users but are available for systems staffs and certain privileged programmes. 170/

153. The effectiveness of the monitor programme can be tested periodically by various technical means. Moreover, as a final safeguard, the monitor programme can be designed to clear the working memory of the computer, after each user has finished operating his programme, thereby eliminating the risk of data being left accessible to a subsequent user. 171/ It has been said, however, that because of the enormous complexity of modern computer operating systems, it is difficult to avoid entirely the occurrence of some chance "trap doors" that permit unauthorized data transfers between users. 172/

(e) Intrusion monitoring

154. The safeguards, mentioned in paragraphs 148-153 above, may be supplemented by technical means for the detecting of any breaches or violations of correct procedure in using the system. Such a means consists in automatic recording (monitoring) procedures built into the computer itself, which print the lists of the persons obtaining information and the nature thereof. 173/

155. This procedure called "audit log" or "audit trail" would not only record authorized users and the files each user had examined but also take note of any attempts to circumvent the security devices. It can analyse any suspicious events, such as incorrect passwords or attempts to get information from files to which the user had not an authorized access. If this analysis is done as the events take place, an alarm can be set off. The resulting protective file should be audited periodically by security experts for signs of violations and to evaluate the effectiveness of the technological safeguards which are used to protect the system. 174/

156. From 475 organizations which, in their replies to the Canadian Task Force have given information on security measures, 75 per cent used audit logs or some other monitoring methods. 175/

170/ Miller, op. cit., pp. 242-243; OECD Report, para. 44.

171/ Canada, Privacy and Computers, p. 105.

172/ Ibid., p. 106; Miller, op. cit., p. 245; Sawyer and Schechter, loc. cit., p. 816; Charles P. Lickson, "Protection of the privacy of data communications by contract: another case study on the impact of computer technology on law", Business Lawyer, vol. 23 (July 1968), p. 978; Warner and Stone, op. cit., pp. 203-204.

173/ Nielsen, op. cit., p. 5.

174/ OECD Report, para. 47.

175/ Canada, Privacy and Computers, p. 108. For the use of auditing procedures in the United States, see United States, Report of the National Academy of Sciences, pp. 83 and 125.

157. The keeping of a log of all persons entering the computer installation has been recommended in the Notes of Guidance for local authorities issued in the United Kingdom. 176/ In the same country the Data Surveillance Bill (1969) contained, in section 2 (2), provisions according to which the operator of each system covered by the bill "shall maintain a written record in which shall be recorded the date of each extraction of date therefrom, the identity of the person requesting the data, the nature of the data supplied and the purpose for which it was required". 177/

158. The draft bill on protection against the misuse of personal data in data processing (Federal Republic of Germany 1972), provided that: "In cases where personal data may be communicated by automatic devices ... a record of every such communication shall be kept stating the recipient, the type of data and the time of its communication." 178/

159. In the Report of the United States Department of Health, Education and Welfare, the rule has been suggested that organizations operating an administrative automated personal data system "maintain a complete and accurate record of every access to and use made of any data in the system, including the identity of all persons and organizations to which access has been given". 179/

160. In the Report of the Younger Committee it has been recommended, as one of the principles of handling information that "a monitoring system should be provided to facilitate the detection of any violation of the security system". 180/

(f) Transmission security

161. As mentioned in paragraph 121 above, in any remote access system, the communications lines between the central computer and the remote users are exposed to various means of infiltration. To protect the security of the data transmission, several technological safeguards are used or have been suggested.

162. One of these would involve the use of coaxial cables as transmissions lines. When the wiretapper draws power from the line, the interconnexion resistance is lowered by the tap. Moreover, because of the frequencies at which computer operations function, taps on the interconnecting coaxial cables would create discernible interruptions in the vibrations along the line which would be evident to proper equipment at the extremities. Both of those characteristics could be automatically monitored continuously by the computer for the detection of wiretappers. 181/

176/ OECD Report, para. 47.

177/ Warner and Stone, op. cit., p. 228, appendix I.

178/ Section 7 (3) of the Bill (Council of Europe, EXP/Prot.Priv./EDB (73) 2, pp. 3-4).

179/ United States, HEW Report, p. 56.

180/ United Kingdom, Younger Report, para. 597.

181/ UCLA Research, p. 1447.

163. The use of "scramblers" to garble data before transmission and installing complementary devices in the authorized terminals to reconstitute the signal have also been suggested. 182/ It has been thought, however, that scrambling methods being relatively simple, it is not difficult to translate a recording of what is sent into the correct data signals. This method, therefore, does not seem to provide a major degree of security. 183/

164. The use of cryptography has been considered as a very effective method to protect the confidentiality of sensitive data when transmitted or stored in removable files. Any minimal encoding of the data has been deemed to be a valuable deterrent against eavesdroppers. 184/ The use of certain types of codes (or ciphers), whose breaking would entail an enormous amount of work, would discourage any possible interception of the transmission. 185/ It has been maintained however that the high cost of implementation of this kind of protection would affect its application. 186/

165. It has been said that there is a "class of ciphers that one can prove to be indecipherable in an absolute sense". 187/ It consists in using random characters (or random key digits) which can be frequently changed, adding to each bit of message information one bit of key information which is in reality misinformation. Such key digits added at the sending end are "subtracted" at the receiving end. If a message is intercepted, it could not be decoded no matter how skilled the intercepter, unless he has access to the tapes of random digit keys; this could be effectively prevented, as, for instance, by sending the tapes to the legitimate receiver by guarded courrier. 188/

3. Problems and difficulties in the use of technological safeguards

166. One of the problems raised by the use of technological safeguards is that it entails substantial expense. 189/ It has been suggested therefore that before deciding to use technological safeguards "it is necessary to formulate appropriate

---

182/ Miller, op. cit., p. 241.

183/ Martin and Norman, op. cit., p. 493.

184/ Baran in The Computer and Invasion of Privacy, hearings before a Sub-Committee of the Committee on Government Operations, House of Representatives, 89th Congress, second session, July 26, 27 and 28, 1966.

185/ Canada, Privacy and Computers, p. 104.

186/ Warner and Stone, op. cit., p. 203.

187/ Horst Feistel, "Cryptography and computer privacy" Scientific American, vol. 228, No. 5 (May 1973), p. 17.

188/ Feistel, loc. cit., p. 18.

189/ Warner and Stone, op. cit., pp. 210-211; Miller, op. cit., p. 241; United Kingdom, Younger Report, para. 686.

analytical or empirical relationships among the value of information to the parties involved, the costs of protection and intrusion and the effectiveness of data security and intrusion techniques". 190/

167. Moreover, it has been generally estimated that any security system, including technological safeguards, can be broken and instances have been given in paragraphs 140, 146, 153 and 163 above. The degree of security has been said to depend on the relationship between the cost for the intruder of bypassing the technical security system and the value to him of obtaining the data. 191/ A profit-seeking intruder may, however, be deterred by raising the intrusion cost at a level that reduces his expected profits to an unacceptable level and effective technical access control may prevent the intrusion by persons not economically motivated. 192/ The risk of intrusion may be thus diminished by the cost and difficulty of any attempts to infiltrate the system. 193/

168. Another difficulty results from the proliferation of remote terminals, which complicates the setting up of a security programme. It has been said that "It is not uncommon for a company to have its computer in one centre, data transmission points in several different cities or states and assembly of final reports in still another location." 194/

169. Such difficulties might explain the fact that the use of technological safeguards is still limited. For instance, in Canada the Task Force on Privacy and Computers estimated that from approximately 1,268 organizations which replied to the questionnaire of the Task Force, and of which almost a half were from the public sector, only about 40 per cent had implemented hardware or software security measures, such as passwords, terminal identification coding or cryptographic coding. 195/ According to the report of the National Academy of Sciences of the United States, only a handful of the 55 of the most advanced organizations visited were using elaborate technological measures to safeguard information in their computerized files from unauthorized access. 196/

170. The use of technological safeguards seems however to be generally recommended, as a part of an extensive set of safeguards. If not absolutely effective by

---

190/ Turn and Shapiro, op. cit., p. 33. See also, UCLA Research, pp. 1452-1453. It has been said, however, that technological safeguards "are not highly expensive; the cost will vary with the measure of security needed, but a fairly elaborate set of safeguards might add perhaps 5 per cent to the overall cost of the system" (Martin and Norman, op. cit., p. 482).

191/ Canada, Privacy and Computers, p. 102.

192/ Turn and Shapiro, op. cit., p. 22.

193/ OECD Report, para. 42.

194/ Warner and Stone, op. cit., p. 206.

195/ Canada, Privacy and Computers, pp. 26 and 34.

196/ United States, Report of the National Academy of Sciences, p. 307.

themselves, technological safeguards are considered necessary, in combination with physical security measures and other safeguards.

171. On these lines, the Data Protection Act of the State of Hessen (Federal Republic of Germany) of 1970 197/ provided that "the records, data and results ... shall be obtained, transmitted and stored in such a way that they cannot be consulted, altered, extracted or destroyed by unauthorized persons. This shall be ensured by appropriate staff and technical arrangements." 198/

171a. The Swedish Data Act (1973) (see paragraph 195 below) provided that the regulations which may be issued by the Data Inspection Board concerning the operation of the computerized personal data systems under its supervision, should, in order to protect the right to privacy (see paragraph 289 below), contain instructions relating, among others, to the methods of ADP, the technical equipment which may be used, the type of automated processing which may be undertaken and the control and safety measures to be applied by these systems.

172. In the draft bill on protection against the misuse of personal data in data processing (Federal Republic of Germany, 1972), 199/ a provision has been included that any person processing personal data, to which the law would apply (see paragraph 196 below) "should take the requisite technical and organizational measures to prevent abuses in the course of such processing especially wrongful retrieval, communication, modification and erasure of data and their distortion and destination. Only those measures are required whose protective effects are in reasonable proportion to the cost involved." 200/

173. In the Notes of Guidance for local authorities, issued in the United Kingdom, which have placed much emphasis on security measures and technological safeguards, the local authorities have been asked formally to assign responsibility for over-all security to a designated chief officer, who in turn should designate an appropriate officer to be responsible for the security of specific terminals. 201/

174. In the Report of the Younger Committee, it has been recommended that "the level of security to be achieved by the system should be specified in advance by the user and should include precautions against the deliberate abuse or misuse of information". 202/

197/ See for details paragraph 196 below.

198/ Section 2, quoted from the International Social Science Journal, UNESCO, vol. XXIV, No. 3, 1972, p. 580.

199/ For details see paragraph 196 below.

200/ Section 4 (1) (Council of Europe EXP/Prof.Priv./EDB (73) 2), p. 2.

201/ United Kingdom, LAMSAC, Computer Privacy, p. 8.

202/ United Kingdom, Younger Report, para. 596. See for similar provisions principle No. 6 in the draft resolution submitted to the Committee of Ministers of the Council of Europe, reproduced in paragraph 319, below.

C. Professional safeguards

175. The protection of the rights of individuals against threats arising from the use of computerized personal data is considered to depend, to a great extent, upon the attitude and the behaviour of the computer profession. By their concern for the rights of the individual and by strictly applying technological and legal safeguards, the staff of computerized personal data systems have a key role in preserving data security and integrity and in eliminating actual or possible problems and threats to human rights. On the other hand, as even the most sophisticated set of technological safeguards and the observance of legal rules could be undermined by people working within the system, they could thus become a source of threats to the rights of the person to whom the information stored in the computer relates.

176. It has been often suggested, therefore, that the adoption of guidelines or enforceable codes of professional ethics for computer specialists, similar to those in existence for the medical or law professions, should be encouraged. 203/

177. The French Government, in a communication dated 21 January 1970 and concerning in particular the operation of postal and telecommunication systems 204/ stated, inter alia, that, "in particular and with the sole aim of avoiding any encroachment on personal freedom, a code of ethics might be prepared".

178. Some practical steps in this field have already been taken. In the United States, on 11 November 1966, the Council of the Association for Computing Machinery (ACM) adopted a set of guidelines for professional conduct in information processing. The guidelines refer to relations of the ACM members with the public, with employers and clients and with other professions. Directly relevant to the protection of privacy are the following guidelines:

> "1. An ACM member will have proper regard for the health, privacy, safety and general welfare of the public in the performance of his professional duties ...
>
> "2. An ACM member will act in professional matters as a faithful agent or trustee for each employer or client and will not disclose private information belonging to any present and former employee or client without his consent". 205/

203/ OECD Report, para. 37; Canada, Privacy and Computers, pp. 166 and 184; United Kingdom, Younger Report, para. 603; United States HEW Report, pp. 55 and 141; Miller, op. cit., pp. 254 and 257; Radu Filip, "Aspecte juridice ridicate de folosirea informaticii in domeniul fisierelor publice (Juridical problems raised by the use of informatics in the field of public files), Studiis; Cercetari Juridice No. 3 (Bucharest, 1973), p. 440.

204/ The full text has been reproduced in E/CN.4/1028/Add.5, para. 85.

205/ Warner and Stone, op. cit., p. 232-233 (appendix II, where the ACM code of professional conduct is reproduced).

179. In the United Kingdom, the Council of the British Computer Society (BCS) approved, on 17 February 1971, its Code of Conduct. 206/ As mentioned in paragraph 1.5 of section III of the Code, it does not deal specifically with the effect of computer-based systems on basic human rights. The following provisions seem to be relevant to this issue: principle 2 (under section II) which stated that a professional member of the BCS "will act with complete discretion when entrusted with confidential information"; and paragraph 2.6 (under section III) which provided that a member "should not disclose, or permit to be disclosed, or use to his own advantage, any confidential information relating to the affairs of his present or previous employers or clients, without their prior permission".

180. It may be noted that both codes mentioned above contain an identical provision requiring the prior consent of the individual for disclosure of data about him, a principle which appears also in existing and proposed legislation (see paragraphs 252, 256, 257 and 269 below).

181. Both codes also contain general ethical standards and rules of behaviour meant to enhance the sense of responsibility of the computer profession and to promote conduct based on integrity, honesty, good faith and a relationship of trust and confidence within the profession and with regard to the public.

182. In Canada, the Associated Credit Bureaus of Canada have adopted a code of ethics whereby many of the consumer rights provided for in the United States Fair Credit Reporting Act of 1971 (see paragraphs 209, 236 and 249 below) are included. 207/

183. Codes of ethics are also deemed necessary for behavioural research automated systems. An extensive code has been adopted in Canada by the Institute for Behavioural Research of York University. 208/

184. It has been said, however, that provisions of the type contained in the ACM Guidelines are self-evident and that they do not appear to be supported by enforcement mechanisms. It has been felt, moreover, that the climate in which computer specialists (who do not have direct contact with the individuals whose life histories they process) work, and the values of scientific quest and efficiency with which data managers are imbued, may raise difficulties in the application of self-regulatory methods in the computer profession. 209/ Difficulties resulting from a lack of congruence between the self interest of the computer profession and the public interest 210/ and from the lack of a common background or homogeneity of a profession which is a young one have also been mentioned. 211/

206/ Its text is reproduced in appendix N of the Report of the Younger Committee (United Kingdom, Younger Report, p. 331-337).

207/ Canada, Privacy and Computers, p. 63.

208/ Ibid., p. 50.

209/ Miller, op. cit., p. 255-256.

210/ Canada, Privacy and Computers, p. 165.

211/ Ibid. See also OECD Report, para. 33.

185. In the report of the Younger Committee, the following views have been expressed:

> "A system of control based on the ethical standards and technical skills of those responsible for programming and operating computers would depend on their organisation into a professional association or associations on the pattern of medicine or the law. On the same analogy there could be different disciplines and different levels of knowledge and skill. Assuming that the problem of recognising the status of persons already engaged in the various tasks could be overcome, the difficulty would be to identify the various disciplines and levels of competence in such a way that the appropriate degrees of skill and knowledge could be tested. Furthermore, the growth of computer technology is making the facilities of computers increasingly available to those not in the computer profession and this might make it more difficult to require observance of a professional code. Moreover the likely increase in the number of computers will, we imagine, be accompanied by an increase in the number of people connected with their use, including clerical and messengerial staff. It is now becoming easier to train programmers, who may, after a year or two, return to a former or transfer to a new occupation unconnected with computers."

The Report, though it applauds the efforts to give coherence to professional responsibility, concludes that "it would be premature to count on the successful establishment in the near future of effective voluntary professional discipline which could properly be endorsed by legislation". 212/

212/ United Kingdom, Younger Report, para. 603.

D. Legal safeguards

1. General review

186. In various countries legal safeguards, though not contained in laws concerning the protection of the individual's rights specifically against actual or possible threats arising from the use of computerized personal data systems, may be provided by existing law guaranteeing these rights in general fashion. In some countries, legislation which is explicitly or implicitly applicable to computerized personal data systems operating in certain fields such as post offices, census bureaux, credit reporting agencies, drivers' files, etc., has been enacted. In several other countries, legislation relating to computerized personal data systems in general has been enacted or has been proposed, or certain principles have been suggested.

(a) Existing law guaranteeing the rights of the person in a general fashion

187. The Government of the Union of Soviet Socialist Republics has reported as follows:

> "The use of computers and other new technologies in the Soviet Union is governed by Soviet legislation, including the USSR Constitution, the Fundamental Principles of the Labour Legislation of the USSR and the Union Republics, the Fundamental Principles of the Health Legislation of the USSR and the Union Republics (1970), the Labour Codes of the Union Republics and other such instruments.
>
> "Soviet law establishes responsibility for violations of the rules governing the use of computers and for the misuse of computer technology. Officials responsible for various forms of abuse involving the use of computers may be tried for a criminal offence under article 170 of the Criminal Code of the RSFSR ('Abuse of power or official position') or the corresponding articles of the Criminal Codes of the other Union Republics.
>
> "Similarly, officials who have failed to carry out or have improperly carried out their official duties in connexion with the use of a computer may be tried for a criminal offence under article 172 of the Criminal Code of the RSFSR ('Negligence') or the corresponding articles of the Criminal Codes of the other Union Republics.
>
> "Subject to various criteria, among which is the gravity of the consequences resulting from the act (including those connected with the improper applications of computer technology), the above-mentioned instruments lay down various penalties, which may go as far as imprisonment.
>
> "Soviet criminal legislation also contains rules establishing criminal responsibility for violations of the secrecy of correspondence (article 135 of the Criminal Code of the RSFSR) and for violations of the principle of the

inviolability of the home (article 136 of the Criminal Code of the RSFSR). These rules are also applicable to violations of personal rights which involve the use of electronic and other modern technologies." 213/

188. Similar references to existing general legislation as applicable to the uses of computers are reported by the Government of the Ukrainian Soviet Socialist Republic. 214/

188a. In 1970, the Organisation for Economic Co-operation and Development (OECD) circulated a questionnaire to member countries on computers and privacy and the existence of administrative and legal safeguards in this connexion. 215/ The replies to the question "Is the individual's right to privacy recognized or protected in the Constitution or the laws of your country?" indicated that the constitutions and general laws of the respective countries though not recognizing, in general, a right to privacy as such, do provide safeguards and remedies against specific invasions of privacy. Criminal law is commonly used to prevent disclosure of official secrets, eavesdropping and misuse of communication systems and to protect private information (for instance, information given in the periodic census enumerations). Civil law provides remedies for loss of privacy by attacks on honour or by the publishing of defamatory statements. The law imposes an obligation on officials to keep certain information confidential, and most replies show that this requirement is extended to certain professional groups. In Finland this obligation has been specifically extended to the staff of the Finnish Computer Centre, with regard to certain information concerning private persons. 216/

189. To the question "What legal safeguards or sanctions are provided at present to protect private information obtained or stored by the Government?" all the countries replying to the questionnaire reported that they had provisions within their legal systems for the protection of private information stored by the government. These laws are commonly embodied in a penal code, or other specific legislation, which imposes an obligation on a public servant to keep confidential material which is communicated to him by a private individual. The government, in its role as record-keeper, is considered to be acting as a trustee of information imparted in confidence, and it is an offence for an official to release this information without authority or as required by law. In some countries (particularly in Scandinavian countries), an official revealing information may not only be prosecuted for a criminal offence but also held liable in damages to the private individual whose confidence has been violated. 217/

213/ Information furnished by the Government of the Union of Soviet Socialist Republics on 27 March 1973.

214/ Information furnished by the Government of the Ukrainian Soviet Socialist Republic on 18 May 1973.

215/ For a summary of the replies to the questionnaire, see OECD Report, appendix I. The full texts of Member Government replies have been circulated in document DAS/SPR/70.10/01 of 25 September 1970.

216/ OECD Report, appendix I, pp. 42-43.

217/ OECD Report, pp. 44-45.

190. Regarding the question of the rights of redress of the individual in case of unauthorized disclosure of information stored about him in public or private computerized data bank systems, the replies showed that, though there are no specific remedies, in many cases redress can be obtained by normal operation of legal principles. Thus, in the case of public systems an individual can institute criminal proceedings against an official who improperly discloses stored information. And the normal provisions of civil law are available so that the law of defamation is relevant in certain circumstances: if an individual is defamed by false material published from a computerized system, he can sue for damages for libel. In some countries (Austria and France, among others), the member of the public defamed can require the publication of a correction at the expense of the defendant. In some member countries, the Parliamentary Ombudsman is available to investigate grievances. 218/

191. According to the report of the Younger Committee, in the United Kingdom:

> "The civil law on breach of confidence affords the same remedies in respect of confidential information processed by computers as it does in respect of any other confidential information; that is to say, the law provides a remedy for both the passing on and the anticipated passing on of the information." 219/

(b) Legislation applicable to computerized personal data systems operating in specific fields 220/

192. The report of the Younger Committee stated that in the United Kingdom there is no legislation dealing specifically with information held, processed, manipulated or disseminated in computerized form, except the Post Office (Data Processing Service Act) 1967. 221/ Certain provisions of the Civil Evidence Act 1968 regulated the admissibility of statements contained in a document produced by a computer.

193. In the United States, there are statutes and regulations that "collectively might be called the law of personal data record keeping", 222/ such as the Fair Credit Reporting Act and the Census Act. The agencies covered by this legislation rely heavily upon computers.

194. In France, a law was adopted in June 1970 on the centralization of documentation relating to road traffic. The provisions of this law (sometimes called the "law on

---

218/ Ibid., p. 77. On the Ombudsman, see paras. 293-295 below.

219/ United Kingdom, Younger Report, para. 584.

220/ Details concerning this legislation appear later in the present report.

221/ United Kingdom, Younger Report, para. 584.

222/ United States, HEW Report, p. 34.

the register of drivers") 223/ do not contain explicit references to computerized files. The computerization of the registers of drivers, established by the law, is, however, under study 224/ and the law was adopted with computerization in mind by the Parliament. 225/

(c) Existing or proposed legislation or principles relating to computerized personal data systems in general 226/

195. One statute relating to computerized personal data systems is the Swedish Data Act (which entered partially into force on 1 July 1973 and which will enter fully into force on 1 July 1974). 227/ The Act regulates computerized personal data systems both in the public and the private sectors. Such systems can be established or maintained only with the permission granted by a special authority, the Data Inspection Board. 228/ Only computerized systems whose creation is decided by the King in Council or the Riksdag are exempted from this rule. Both the King in Council and the Riksdag are obliged, however, to consult the Data Inspection Board, before such a decision is taken.

196. In the Federal Republic of Germany, the Land of Hessen adopted, on October 1970, a Data Protection Act. The scope of the data protection provided by this Act has been defined as follows: "Data protection shall cover all records prepared for purpose of automatic data processing, all stored data and the results of processing such records and data within the purview of the Land authorities and the public corporations, institutions and establishments under the jurisdiction of the Land." 229/ In the same country, the draft of a federal bill on protection against the misuse of personal data in data processing has been prepared. 230/ The

---

223/ Braibant, loc. cit., p. 801.

224/ Information furnished by the Government of France on 10 October 1973.

225/ Braibant, "La protection des droits individuels...", loc. cit., p. 802.

226/ Details concerning this legislation or principles appear later in the present report.

227/ An English translation of the draft of the Data Act annexed to the report of the Swedish Government of July 1972 on computers and privacy, and an article "The Swedish Data Act" by Jan Freese, published in Current Sweden (July 1973, No. 4), summarizing the Act as adopted by the Riksdag in April 1973, were furnished by the Government of Sweden on 21 August 1973. Further information concerning the changes brought to the 1972 draft furnished by the Government of Sweden on 24 January 1974 was also taken into account in this report.

228/ See for details on the Data Inspection Board, paragraphs 286-290 below.

229/ Section 1 quoted from International Science Journal, UNESCO, Volume XXIV, No. 3, 1972, p. 580.

230/ See paragraph 172, above.

draft bill contains rules to protect personal data stored in computerized systems or otherwise processed 231/ in public administrative offices or any other public establishments; in business undertakings or any other non-public establishments for their own purposes (that is for internal use) or for third parties in the normal course of business (such as inquiry and detective agencies, market and opinion research institutes, wage calculation centres, etc.), with the exception of the routine storage and communication of personal data for purposes of publication by press, radio and film enterprises and their auxiliary enterprises. 232/

197. In Belgium, a private bill relating to the protection of privacy and personality was placed before the Senate on 26 January 1972. The bill contained, inter alia, provisions on the information processed by electronic or other methods. In the same country provisions relating to safeguards have been included in a draft bill concerning the National Register. 233/

198. In the United Kingdom, two bills in this field were introduced which had only a first reading in Parliament: Mr. Kenneth Baker's Data Surveillance Bill 1969 and Mr. Leslie Huckfield's Control of Personal Information Bill 1971. The Data Surveillance Bill, to which reference was made in paragraph 124 above, was meant to apply to computerized personal data systems in both the public and the private sectors. 234/ It provided for the establishment of a register of the various computerized systems open to the inspection of the public and the press, with the exception of systems operated by the police, the security services and the armed forces, which would have had to be registered separately. 235/ The provisions of the bill, which had the purpose of protecting the rights of the individual and of establishing criminal and civil liability for their violation, 236/ would not have been applicable to computerized systems which do not contain personal information relating to identifiable persons, and to those operated by the police, by the security services and by the armed forces (section 2).

231/ Section 2 (2) and (3) and Section 3 (1) (Council of Europe Exp./Prot. Priv./EDB(73)2, p. 2). In the provisional explanatory memorandum accompanying the draft, it has been stressed that conventional methods will continue to have considerable importance in practice during the foreseeable future and cannot be excluded from the regulations. To limit the provisions to electronic data processing would lead to inequality of treatment and make possible and even encourage evasion of the Act (ibid., p. 28 (4.2.4)).

232/ Section 23, 3 (2) of the bill (ibid., p. 11).

233/ The texts of the two bills were furnished by the Government of Belgium on 15 February 1973.

234/ See the enumeration of these systems in paragraph 277 below.

235/ See paragraph 277 below.

236/ See paragraphs 238, 253, 300 and 307 below.

199. As already mentioned, in 1970 the Government appointed a Committee on Privacy under the chairmanship of Sir Kenneth Younger, with the following terms of reference: "To consider whether legislation is needed to give further protection to the individual citizen and to commercial and industrial interests against intrusions into privacy by private persons and organizations, or by companies and to make recommendations." The report of the Younger Committee, published in 1972, included principles for handling personal information by computers. 237/ The implementation of those principles was envisaged as not taking a legal form but rather the form of restrictions voluntarily agreed to by computer manufacturers, operators and users. The report further contained a proposal to adopt legislation concerning the establishment of governmental machinery for keeping under review the growth in and techniques of gathering personal information and processing it with the help of computers. 238/ The report of the Younger Committee was debated by the House of Commons in July 1973. 239/

200. The Government of Denmark has reported as follows:

> "/T/he Ministry of Justice, on 9 September 1970, set up a Committee to consider, in the light of technological developments, the protection of the privacy of the individual in connection with the establishment and use of public and private registers.
>
> "On the basis of a report submitted by the said Committee, the Danish Penal Code was amended by Act No. 89 of 29 March 1972." 240/

201. In Canada the Task Force on Privacy and Computers, established by the Department of Communications and Justice in 1971, with the purpose inter alia to examine and evaluate possible measures, whether juridical, regulatory, technical or professional, which might ensure observance of privacy rights and values, recommended in this respect that:

> "Government, as the principal collector and instigator of the collection of personal information, has a key role to play. Aside from such possible responses as a surveillance agency and an ombudsman, the Government could implement administrative rules, enforced by a central agency..." 241/

202. In the United States, proposals for the enactment of legislation establishing a "Code of fair information practice" for computerized personal data systems were made in a report of 1973 of the advisory committee of the Secretary of Health,

---

237/ United Kingdom, Younger Report, paras. 592-600.

238/ Ibid., para. 621.

239/ House of Commons, Official Report, 13 July 1973, cols. 1955-2058.

240/ Information furnished by the Government of Denmark on 21 February 1973.

241/ Canada, Privacy and Computers, p. 184.

Education and Welfare. The proposals contain recommendations of principles and safeguard requirements for administrative personal data systems, 242/ for statistical reporting and research uses of administrative data systems 243/ and for statistical reporting and research systems. 244/

2. Rules providing for safeguards relating to operational activities of computerized personal data systems

203. Various suggested or existing rules or requirements concern procedures or techniques applicable in general to the activities of computerized personal data systems in collecting, storing, using and disseminating identifiable personal data. The purpose of such rules or requirements is, in general, to prohibit certain practices considered intrusive upon privacy and related values, to prescribe certain procedures likely to protect such values and to establish the right of the individual to access to the computerized files which store information pertaining to him.

(a) Rules relating to collection of personal data

204. It has been pointed out that, as the computer data store is essentially a file, any information contained in it, irrespective of how extensive and effective the technological safeguards may be, would be liable to extraction or alteration. The most reliable safeguards have been considered, therefore, to be those which can be implemented before the personal data have been stored in the computer. 245/ Rules restricting the collection of personal data would thus hinder a large accumulation of sensitive information on matters which belong to the private life of individuals and of information not directly linked with the purposes for which it had to be gathered.

205. Prior requirements for collecting personal data. Collection of personal data for computerized files could be controlled and thereby restricted if as has been suggested before the establishing or enlarging of a computerized personal data system is envisaged, careful consideration is given to questions regarding its purposes, scope and utility. Formalized administrative procedures and requirements should be followed to ensure that such questions are raised and confronted before taking a decision in this respect. The public should also have the opportunity to comment on these systems before they are created. Rules regarding the collection of data which is likely to result from the creation or enlargement of computerized data systems should be established in advance, after the public has been given the opportunity to comment. 246/

242/ United States, HEW Report, pp. 50-64.

243/ Ibid., pp. 85-87.

244/ Ibid., pp. 95-102.

245/ Miller, "Personal privacy in the computer age", loc. cit., p. 1214.

246/ United States, HEW Report, pp. 51-52.

206. In the "Notes of guidance for local authorities" issued in the United Kingdom under the heading "Data Collection", the following recommendations have been made:

> "It should in no way be inferred that setting up data banks necessarily requires the collection of any additional information. If such information is requested it should be shewn that there is a legitimate use for it. Wherever possible the information to be included in the data bank should be assembled from existing records." 247/

207. Rights of the individual. The right of the individual at the stage of the collection of personal data requires that he should be informed of the reasons for which information is being sought and that his "informed consent" should be obtained. 248/

208. In this connexion, a rule has been proposed to the effect that the individual asked to supply personal data for administrative automated personal data systems and statistical reporting and research systems should be informed whether or not he is legally required to supply the data requested, and also of any specific consequences for him, which are known to the organization operating the respective system of providing or not providing such data. 249/ A somewhat similar principle has been recommended for personal data systems established for administrative purposes which use the data collected also for statistical reporting and research:

> "When personal data are collected for administrative purposes, individuals should under no circumstances be coerced into providing additional personal data that are to be used exclusively for statistical reporting and research. When application forms or other means of collecting personal data for an administrative data system are designed, the mandatory or voluntary character of an individual's responses should be made clear." 250/

209. According to the Fair Credit Reporting Act (United States 1971) the individual to whom the consumer reports relate has the right to be notified in advance by the

---

247/ United Kingdom, LAMSAC, Computer Privacy, p. 8.

248/ Canada, Privacy and Computers, p. 157.

249/ United States, HEW Report, pp. 59 and 161.

250/ Ibid., p. 85.

agency whenever an investigative report is to be prepared about him, unless the report is for employment for which the individual has applied. 251/

210. Another requirement generally suggested for restricting the collection of personal data is that such data be exclusively related to the functions which the collecting organization is legally entitled to perform. 252/

251/ The relevant provisions read as follows: "Disclosure of investigative consumer reports. (a) A person may not procure or cause to be prepared an investigative consumer report on any consumer unless -- (1) it is clearly and accurately disclosed to the consumer that an investigative consumer report including information as to his character, general reputation, personal characteristics, and mode of living, whichever are applicable, may be made, and such disclosure (A) is made in a writing mailed, or otherwise delivered, to the consumer, not later than three days after the date on which the report was first requested, and (B) includes a statement informing the consumer of his right to request the additional disclosures provided for under subsection (b) of this section; or (2) the report is to be used for employment purposes for which the consumer has not specifically applied. (b) Any person who procures or causes to be prepared an investigative consumer report on any consumer upon written request made by the consumer within a reasonable period of time after the receipt by him of the disclosure required by subsection (a) (1) of this section, shall make a complete and accurate disclosure of the nature and scope of the investigation requested. This disclosure shall be made in a writing mailed, or otherwise delivered, to the consumer not later than five days after the date on which the request for such disclosure was received from the consumer or such report was first requested, whichever is the later..." (United States Codes (1970 Edition) (Washington, Government Printing Office, 1971) (referred to hereafter as USC), title 15, para. 1681d).

In a bill to amend the Fair Credit Reporting Act, introduced in the Senate on 3 August 1973, it has been proposed to replace these provisions by the following:

> "A person may not procure or cause to be prepared an investigative consumer report on any consumer unless that consumer has given a specific, dated, and separately signed affirmative written indication of his authorization of such an investigative consumer report after receiving clear and conspicuous written disclosure to him of the methods and scope of the investigation. Such disclosure shall include --
>
> "(1) a list of all questions to be asked in the investigation and the likely sources to be contacted in the investigation; and
>
> "(2) a blank copy of any standard questionnaire or other similar form to be used in the investigation." (93rd Congress, 1st Session, S.2360, p. 2).

The Bill was read twice and referred to the Committee on Banking, Housing and Urban Affairs.

252/ United States, HEW Report, pp. 59, 161 and 85.

/...

211. According to the Swedish Data Act (1973), when issuing permission for the establishing or maintaining of computerized personal data systems, the Data Inspection Board should issue regulations (see paragraph 288 below) specifying, inter alia, the purpose of the system.

212. Provisions referring to the requirement that only data relevant to the purposes for which a computerized personal data system is operated should be stored therein have been included in the Data Surveillance Bill (United Kingdom 1969). 253/

213. In the report of the Younger Committee the following has been included among the suggested principles for handling information:

> "The amount of information collected and held should be the minimum necessary for the achievement of the specified purpose." 254/

214. The draft bill on protection against the misuse of personal data processing (Federal Republic of Germany, 1972) included a number of requirements to be observed for the storage of personal data for computerized files. Section 6 of the bill, relating to data processing by governmental administrative departments and other public offices, provided that the storage of personal data would be permitted only with the agreement of the person concerned, on the basis of a legal rule or as a part of the legitimate fulfilment of the tasks for which the storage unit is responsible. According to section 17, relating to data processing by non-official establishments for their own purposes, data storage would be allowed only with the agreement of the person concerned, on the basis of a legal provision and within the framework of existing contractual relations of trust, in so far as the person concerned had no overriding legitimate interests which stood in the way. 255/ Under section 24 (1) and (2), businesses, undertakings and other establishments which are not public-law corporations or entities owned by such corporations and which are processing data on behalf of third parties would be permitted to store personal data if the applicant gave credible proof that he had a legitimate interest in knowing such data and in so far as the person concerned had no overriding legitimate interests which stood in the way. 256/

215. Methods of collecting personal data. It has been said that the manner and methods adopted by organizations in collecting data to be stored in computers may be unnecessarily intrusive of personal privacy or may produce other harmful consequences. As mentioned in paragraphs 103-105 above, the collection of data by means of modern surveillance devices for computer storage has been considered

---

253/ Section 1, subsection 2, paragraph (f), and subsections 5 and 6 (Warner and Stone, op. cit., pp. 227-228).

254/ United Kingdom, Younger Report, para. 593. See also principle No. 2 in the draft resolution submitted to the Committee of Ministers of the Council of Europe, reproduced in paragraph 319 below.

255/ Council of Europe, EXP/Prot. Priv./EDB(73)2, pp. 3 and 17.

256/ Ibid., p. 11.

to be an especially harmful method. The report, "Respect for the privacy of individuals and the integrity and sovereignty of nations in the light of advances in recording and other techniques" (E/CN.4/1116), mentioned in its paragraph 130 that the potential use for storage, analysis and retrieval by governmental or private computer of information obtained by means of modern surveillance devices should be kept in mind in connexion with any discussion of the need to regulate the use of those devices.

216. It is clear that one of the means of preventing the input into a computer of personal information gathered through modern surveillance devices is to place certain limits on the use of these devices. 257/ The adoption by states of certain legislative provisions in this respect, suggested in the report mentioned above, under "Points for possible inclusion in draft international standards concerning respect for the privacy of the individual in the light of modern recording and other devices" (E/CN.4/1116, para. 177, points 3 (a) (i) and (ii) and 3 (g) especially) would represent a safeguard against the indiscriminate use of these devices for collecting personal data for computerized files.

217. Another safeguard which has been recommended is the prohibition of the storage in computerized files of personal information that has been surreptitiously gathered by surveillance devices, with the exception of information pertaining to certain areas such as law enforcement. 258/

217a. It might be mentioned that according to the Swedish Data Act (1973) (see paragraph 195 above) the regulations, which may be issued by the Data Inspection Board concerning the operation of the computerized personal data systems under its supervision should, in order to protect the right to privacy (see paragraph 289 below), contain instructions relating, among others, to the methods of collecting information.

218. Objectivity and accuracy of the personal data to be collected. It has been said that the information gathered should comply with high standards of accuracy and objectivity. Subjective and unverifiable information as well as ex parte or "hearsay" evaluations should be excluded. 259/

219. The type of information not to be collected. It has been generally recognized that, for the protection of the privacy of the individual, the collection of certain types of information considered as being extremely sensitive, should be prohibited.

257/ Canada, Privacy and Computers, p. 169.

258/ Ibid.

259/ See principle No. 8 in the draft resolution submitted to the Committee of Ministers of the Council of Europe, reproduced in paragraph 319 below. See also Sawyer and Schechter, loc. cit., p. 816; Miller, loc. cit., p. 1215; Martin and Norman, op. cit., p. 472.

Data concerning political and religious views, race and nationality, sexual behaviour (or intimate life) are usually included as types of data not to be collected. 260/ Reference has been also made to the general legal obligation not to store conviction records of persons pardoned by amnesty. 261/ It has been said, however, that the prohibition should be one of principle, allowing exceptions, under legally prescribed conditions and procedures. 262/

220. The Swedish Data Act (1973) contained provisions relating to certain categories of information which may be allowed by the Data Inspection Board (see paragraphs 286-290 below) to be recorded by specified authorities. The Act provided that the Data Inspection Board, unless there are special reasons, should not grant permission to a person other than an authority competent under law to record in computerized files personal information regarding: (a) suspicions relating to criminal activities, criminal convictions and compulsory measures taken in pursuance of certain laws (the Child Welfare Act and laws relating to psychiatric treatment of persons detained in special institutions, to antisocial behaviour dangerous to society and aliens); (b) the fact that a person had received medical attendance, social assistance, treatment for alcoholism and the like, or had been subjected to proceedings under the Child Welfare Act or the Alien Act. The Data Act further provided that permission to record political or religious views may be granted only where there are special reasons. This rule should not, however, prevent a political or religious association from keeping a record of its own members. In addition, according to the Act, the Data Inspection Board, when issuing permission for the establishing or maintaining of computerized personal data systems, is obliged to issue regulations (see paragraph 288 below) specifying, inter alia, the type of information which may be stored.

221. The law concerning centralization of documentation on road traffic (France 1970), which established two separate centralized files containing information on motor vehicle drivers, one storing administrative data and the other conviction records for criminal offences, restricted and enumerated the information which should be placed in these files. 263/

222. According to the Belgian draft bill on the national register (articles 1-5), the Crown must determine which of the information on physical and juristic persons, that was previously recorded in manual files, should be entered in the computerized files of this register.

260/ Canada, Privacy and Computers, p. 150; United States, Report of the National Academy of Sciences, p. 379; A. Miller, op. cit., p. 249.

261/ Braibant, loc. cit., p. 807.

262/ Ibid., p. 808; Canada, Privacy and Computers, p. 150.

263/ Braibant, loc. cit., p. 803.

223. Difficulties in establishing and implementing rules concerning collection of personal data. The opinion has been expressed that rules restricting the collection of personal data may hamper the ever-growing flow of information which is needed for the management and development of modern society. 264/

224. It has been remarked that "great care would have to be taken not to inhibit unduly or censor the flow of information and knowledge in society, especially since people who would not object to divulging certain information to some inquirers, such as pollsters or academics, might object to disclosing the same information to government or a private company." 265/

225. According to one writer, difficulties in defining a restrictive policy arise from the need for setting value priorities. There are certain values, such as the necessity to ensure a lawful and orderly existence of the community by comprehensive investigations of crime, which compete with the privacy value. 266/

226. It has been said that individuals are often in a poor position to dispute the relevance of particular information demanded of them, since giving the information is the necessary condition for receiving a benefit. The highly subjective nature of the alleged relevance of any particular item of information in a particular context would also make difficult the application of the principle that only data clearly relevant to the purpose in view should be gathered. 267/

(b) Rules relating to storage of personal data

227. To ensure the accuracy of the personal data stored in the computer and to protect it against accidental corruption, it has been suggested that rules be established providing for regular checking of the validity of the data: 268/ for controls over the accuracy of the circuit operation, the correct functioning of the system and protection against failure; 269/ and for removing of incorrect or incomplete data. 270/

228. According to the Swedish Data Act (1973), if there is reason to suspect that personal information stored in the computer is incorrect, the person responsible for the computerized system must check it, without delay, and, if needed, correct

---

264/ Cf. Miller, Assault on Privacy, p. 249.

265/ Canada, Privacy and Computers, pp. 150-151.

266/ U. Thomas, Computerized Data Banks in Public Administration (Paris, OECD Information Studies No. 1, 1971), p. 63.

267/ Canada, Privacy and Computers, p. 150.

268/ OECD Report, para. 51.

269/ Martin and Norman, op. cit., pp. 501-502.

270/ OECD Report, para. 51. See also principle No. 8 in the draft resolution submitted to the Committee of Ministers of the Council of Europe, reproduced in paragraph 319 below.

or remove it. If such information had been previously communicated to a third person, the individual to which the information relates may request the person responsible for the system to notify the recipient about the correction or removal of that information. When there are special reasons, the Data Inspection Board may, however, exempt the person responsible for the system from this obligation. The Act further provided that if the personal information which had to be stored in order to fulfil the purpose of the computerized system is incomplete or is lacking, the person responsible for the system should complete it or enter the missing information whenever such deficiencies may cause undue encroachment on privacy or risk of loss of rights.

229. The Fair Credit Reporting Act (United States 1971) imposed on consumer reporting agencies the obligation to follow "reasonable procedures to assure maximum possible accuracy of the information concerning the individual about whom the report relates". 271/ The Act provided in addition that:

> "Whenever a consumer reporting agency prepares an investigative consumer report, no adverse information in the consumer report (other than information which is a matter of public record) may be included in a subsequent consumer report unless such adverse information has been verified in the process of making such subsequent consumer report, or the adverse information was received within the three-month period preceding the date the subsequent report is furnished..." 272/

In a bill to amend the Fair Credit Reporting Act, it has been proposed to amend this above-quoted provision as follows:

> "(1) by inserting '(a)' before 'whenever'; and (2) by adding at the end thereof the following new subsection:
>
> "(b) Each investigative consumer report shall be in writing, shall identify the sources of all information contained therein, and shall be retained in the file of the consumer to whom it relates for a period of one year following its completion." 273/

230. To prevent the accumulation of out-of-date information, it has been generally recommended that a certain storage period be established, and that the obligation to review the content of computerized files periodically in order to remove data which has become obsolete be imposed. 274/

271/ USC, Title 15, para. 1681e (b).

272/ Ibid., para. 1681 1.

273/ 93rd Congress, 1st Session, S.2360, p. 5.

274/ OECD Report, para. 57; I. J. M. Laver, "Computers", Technological Injury, ed. J. Rose (Gordon and Breach, Science Publishers, London 1969), p. 143; UCLA Research, p. 1437. Martin and Norman (op. cit., p. 477) proposed as a rule that aged data should be removed. See also principles Nos. 7 and 8 in the draft resolution submitted to the Committee of Ministers of the Council of Europe, reproduced in paragraph 319 below.

230a. According to the Swedish Data Act (1973), the Data Inspection Board, in deciding to grant permission for the establishment or maintenance of computerized personal data systems (see paragraphs 195 above and 288 below), should pay special attention to the nature and the quantity of the personal data to be stored and to the attitude which those concerned can be expected to adopt towards the computerized system. The regulations which the Board may issue concerning the systems under its supervision should, in order to protect the right to privacy (see paragraph 289 below), include instructions relating, among others, to the question of how data are to be stored.

231. In the law concerning the centralization of documentation on road traffic (France 1970), it has been provided that information with regard to conviction records should be erased if the offence was pardoned by amnesty; measures of reprieve, rehabilitation and commutation of punishment should be included along with the convictions, and records of criminal and administrative penalties should be purged after a period of six years from the time they were imposed, if the person concerned was not subjected to new penalties during this period. 275/

232. The right of access of the individual to computerized files containing information about him has been considered to imply in general his right to know of the existence of such files, to see them on demand (i.e., to obtain a print-out) and to challenge any entry in the record as to its accuracy, completeness, current validity and relevance. 276/ In the report of the National Academy of Sciences it has been said that an individual should know of the existence of any general file kept by a government agency, with some exceptions for intelligence files and a right of inspection was advocated for most files, recognizing that some records would have to be exempted from such a right for reasons of confidentiality of sources and similar reasons. 276a/

233. In this connexion, in addition to the provision relating to the right of the individual mentioned in paragraph 228 above, the Swedish Data Act (1973) provided that the person responsible for the computerized system should inform once every year the person concerned, at his request and, as soon as possible, of the information stored about him. This information should be supplied, in general, free of charge. The Data Inspection Board may allow, however, in the case of special types of information, a fee to be charged. The right of the individual to obtain the information concerning him cannot be, nevertheless, exercised if that information, according to law or the decision of an authority, may not be

---

275/ Articles 4 and 8 of the law. See also Braibant, loc. cit., p. 804.

276/ See, for instance, Canada, Privacy and Computers, p. 155; Martin and Norman, op. cit., pp. 473-475; Miller, op. cit., pp. 246-247; Filip, loc. cit., p. 440. See also principle No. 5 in the draft resolution submitted to the Committee of Ministers of the Council of Europe, reproduced in paragraph 319 below.

276a/ United States, Report of the National Academy of Sciences, pp. 361-370.

delivered to him. The regulations which the Data Inspection Board may issue concerning the operation of the systems under its supervision should, in order to protect the right to privacy (see paragraph 289 below), contain instructions relating, among others, to the question whether the individual is to be informed of the processing of data concerning him.

234. Under the Data Protection Act of 7 October 1970 (State of Hessen, Federal Republic of Germany), "if stored data is incorrect, an aggrieved party may demand rectification" and "any person whose rights are infringed by unlawful access, alteration or destruction or by unlawful extraction may require that such action be discontinued, if there is danger of further infringement". 277/

235. In accordance with the law concerning the centralization of documentation on road traffic (France 1970), the individual has the right on request to know the information relating to him and to ask for its correction, following the procedure specified in the law. 278/

236. According to the Fair Credit Reporting Act (United States, 1971), the individual about whom a report is being prepared has the right on request to be informed by the agency about various aspects of the data relating to him, 279/ free of charge in certain circumstances or upon payment of a fee in others. He has further the right to be notified by the agency or by the user, according to a

---

277/ Section 2, quoted from the International Social Science Journal, UNESCO, vol. XXIV, No. 3, 1972, p. 582.

278/ Articles 4, 5 and 7 of the law. See also Braibant, loc. cit., pp. 803-804.

279/ The relevant provisions read as follows: "Disclosures to consumers. (a) Every consumer reporting agency shall, upon request and proper identification of any consumer, clearly and accurately disclose to the consumer:

"(1) The nature and substance of all information (except medical information) in its files on the consumer at the time of the quest.

"(2) The sources of the information; except that the sources of information acquired solely for use in preparing an investigative consumer report and actually used for no other purpose need not be disclosed: Provided, That in the event an action is brought under this subchapter, such sources shall be available to the plaintiff under appropriate discovery procedures in the court in which the action is brought.

"(3) The recipients of any consumer report on the consumer which it has furnished --

(A) for employment purposes within the two-year period preceding the request, and

(B) for any other purpose within the six-month period preceding the request." (USC, title 15, para. 1681 g).

/...

special procedure, when the reports on employment, credit and insurance are likely to have an adverse effect upon obtaining them. In this connexion, the following has been provided:

"A consumer reporting agency which furnishes a consumer report for employment purposes and which for that purpose compiles and reports items of information on consumers which are matters of public record and are likely to have an adverse effect upon a consumer's ability to obtain employment shall -

(1) at the time such public record information is reported to the user of such consumer report, notify the consumer of the fact that public record information is being reported by the consumer reporting agency, together with the name and address of the person to whom such information is being reported; or

(2) maintain strict procedures designed to insure that whenever public record information which is likely to have an adverse effect on a consumer's ability to obtain employment is reported it is complete and up to date. For purposes of this paragraph, items of public record relating to arrests, indictments, convictions, suits, tax liens, and outstanding judgments shall be considered up to date if the current public record status of the item at the time of the report is reported; 280/

279/ (continued)

In a bill to amend the Fair Credit Reporting Act it has been proposed to amend this provision as follows:

"(1) by striking out "The nature and substance of all" in subsection (a) (1) and inserting in lieu thereof "All";

"(2) by inserting before the period at the end of subsection (a) (1) a comma and the following: "except that the consumer shall be advised of the existence of any medical information withheld, and of his right to have such information furnished to a licensed physician of his choice";

"(3) by striking out the semicolon and all that follows it in subsection (a) (2) and inserting in lieu thereof "(including the sources of medical information)."; and

"(4) by adding at the end thereof the following new subsection:

"(c) Upon the request of the consumer to whom medical information withheld pursuant to subsection (a) (1) relates the consumer reporting agency shall furnish such information to a licensed physician designated by the consumer. Nothing in this Act shall be construed to prevent, or to authorize any consumer reporting agency to prevent such a physician from subsequently disclosing such information to the consumer to whom it relates." (93rd Congress, 1st Session, S. 2360, p. 3-4).

280/ USC, title 15, para. 1681 k.

/...

...

"(a) Adverse action based on reports of consumer reporting agencies.

Whenever credit or insurance for personal, family, or household purposes, or employment involving a consumer is denied or the charge for such credit or insurance is increased either wholly or partly because of information contained in a consumer report from a consumer reporting agency, the user of the consumer report shall so advise the consumer against whom such adverse action has been taken and supply the name and address of the consumer reporting agency making the report.

(b) Adverse action based on reports of persons other than consumer reporting agencies.

Whenever credit for personal, family, or household purposes involving a consumer is denied or the charge for such credit is increased either wholly or partly because of information obtained from a person other than a consumer reporting agency bearing upon the consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, the user of such information shall, within a reasonable period of time, upon the consumer's written request for the reasons for such adverse action received within sixty days after learning of such adverse action, disclose the nature of the information to the consumer. The user of such information shall clearly and accurately disclose to the consumer his right to make such written request at the time such adverse action is communicated to the consumer.

(c) Reasonable procedures to assure compliance.

No person shall be held liable for any violation of this section if he shows by a preponderance of the evidence that at the time of the alleged violation he maintained reasonable procedures to assure compliance with the provisions of subsections (a) and (b) of this section." 281/

In the bill to amend the Fair Credit Reporting Act, it has been proposed to amend paragraph 1681 m as follows:

"(a) Whenever any adverse action is taken either wholly or partly because of information contained in a consumer report from a consumer reporting agency, the user of the consumer report shall -

"(1) disclose in writing to the consumer against whom such adverse action has been taken (A) the reason for taking such adverse action,

---

281/ USC, title 15, para. 1681 m.

including reference to the particular item or items of information contained in the consumer report upon which such adverse action has been wholly or partly based; (B) the name, street address, and telephone number of the consumer reporting agency making the report; and (C) a statement of the fact that the consumer is entitled (i) to receive a copy of his file from the consumer reporting agency at nominal charge, or (ii) to inspect his file at the consumer reporting agency free of charge if visited within 30 days of receipt of the user's notification; and

"(2) furnish a copy of the consumer report if the consumer report was written, or furnish a copy of a summary if the consumer report was oral.

"(b) Whenever credit or insurance for personal, family, or household purposes, or employment involving a consumer is denied or the charge for such credit or insurance is increased either wholly or partly because of information obtained from a person other than a consumer reporting agency bearing upon the consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, the user of such information shall disclose in writing to the consumer at the time such action is taken the reason for such adverse action, and the nature of the information." 282/

237. The Act also provided for the right of the individual to dispute the accuracy of the information:

"(a) Dispute; reinvestigation.

If the completeness or accuracy of any item of information contained in his file is disputed by a consumer, and such dispute is directly conveyed to the consumer reporting agency by the consumer, the consumer reporting agency shall within a reasonable period of time reinvestigate and record the current status of that information unless it has reasonable grounds to believe that the dispute by the consumer is frivolous or irrelevant. If after such reinvestigation such information is found to be inaccurate or can no longer be verified, the consumer reporting agency shall promptly delete such information. The presence of contradictory information in the consumer's file does not in and of itself constitute reasonable grounds for believing the dispute is frivolous or irrelevant.

"(b) Statement of dispute.

If the reinvestigation does not resolve the dispute, the consumer may file a brief statement setting forth the nature of the dispute. The

---

282/ 93rd Congress, 1st Session, S. 2360, p. 5-6.

consumer reporting agency may limit such statements to not more than one hundred words if it provides the consumer with assistance in writing a clear summary of the dispute.

"(c) Notification of consumer dispute in subsequent consumer reports.

Whenever a statement of a dispute is filed, unless there is reasonable grounds to believe that it is frivolous or irrelevant, the consumer reporting agency shall, in any subsequent consumer report containing the information in question, clearly note that it is disputed by the consumer and provide either the consumer's statement or a clear and accurate codification or summary thereof.

"(d) Notification of deletion of disputed information.

Following any deletion of information which is found to be inaccurate or whose accuracy can no longer be verified or any notation as to disputed information, the consumer reporting agency shall, at the request of the consumer, furnish notification that the item has been deleted or the statement, codification or summary pursuant to subsection (b) or (c) of this section to any person specifically designated by the consumer who has within two years prior thereto received a consumer report for employment purposes, or within six months prior thereto received a consumer report for any other purpose, which contained the deleted or disputed information. The consumer reporting agency shall clearly and conspicuously disclose to the consumer his rights to make such a request. Such disclosure shall be made at or prior to the time the information is deleted or the consumer's statement regarding the disputed information is received." 283/

238. The Data Surveillance Bill (United Kingdom 1969) would have provided for the following rights of the person about whom information is stored in a computerized data system; the right to receive a print-out of all the data contained therein which relates to him, not later than two months after his name is first programmed into the system and, thereafter, at his request, upon payment of a fee; and the right to apply for amendment or expunging of data on the grounds that it is incorrect, unfair or out of date in the light of the purposes for which it has been stored in the system. 284/

239. In the draft of the bill relating to the protection of privacy and of the personality (Belgium 1972), it has been provided that the individual has the right of access to all information relating to him and to receive, free of charge, a complete copy, with the motives for which the information had been stored. In case

---

283/ USC, title 15, para. 1681 i.

284/ Sections 4 (1) and 5 (1), Warner and Stone, op. cit., p. 229, for the files which, according to the bill, are excepted from the right of access of the individual see para. 198 above.

of urgency he may request through a judiciary procedure, the correction or exclusion of all incorrect or useless information, or whose knowledge is not indispensable to the public good.

240. The draft bill on protection against the misuse of personal data in data processing (Federal Republic of Germany, 1972) contained a number of provisions relating to the safeguards which concern data storage and the rights of access of individuals.

241. As regards the personal data systems operated by governmental administrative departments or other public offices, the following would be provided: (a) immediately following the initial act of storage, the storage agency should announce publicly, in the official bulletin, what type of personal data is stored by it (with the exception of the offices for the protection of the Constitution, the Federal Intelligence Agency, the Military Counter Intelligence Service, the offices of the Public Prosecutor, the Police Department or the Taxation and Customs Prosecutions Department); 285/ (b) upon application, and upon payment of a fee, the person concerned should be supplied with information on stored data relating to him and the names of their recipients, except when that information was stored by the public authorities mentioned above and "where revelation of personal data would be prejudicial to public security or the public weal of the Federal Republic or of a Land, to the legitimate fulfilment of the tasks for which the storage agency is competent or to the overriding legitimate interest of a third party", and when "the request for extraction is patently ill-intentioned"; 286/ (c) personal data "should be corrected when they are incorrect" and "clarified when they are unclear"; if the accuracy of personal data is contested by the person concerned, without a substantiation of the alleged inaccuracy, an appropriate note should be included with the data whenever subsequently communicated; 287/ (d) personal data should be erased "when their storage is inadmissible or when they are no longer required by the storage unit for the legitimate fulfilment of its tasks and failure to erase them would harm the legitimate interests of the person concerned"; 288/ modification of data should be permissible "in order to further the legitimate fulfilment of the tasks for which the storage unit is competent". 289/

285/ Section 10 (Council of Europe EXP/Prot. Priv./EDB(73)2), p. 5.

286/ Section 11 (ibid., p. 5-6).

287/ Section 12 (ibid., p. 6). An identical provision is contained in section 21 (1) applying to non-official establishments processing data for their own purposes and in section 27 (1) applying to agencies which store personal data in the normal course of their business for the purpose of communicating them to others and in fact do communicate them, (ibid., pp. 9 and 12).

288/ Section 12 (2) (ibid., p. 6).

289/ Section 9 (1) (ibid., p. 5).

242. With regard to non-official establishments (such as business undertakings) processing data for their own purposes, the bill provided that the person concerned would have the right to demand, upon payment of a fee, information on stored data concerning his own person and the names of the recipients. The individual concerned would not have the right to receive information where "the supply of personal data would seriously impair the functions of the place of storage and he has no overriding legitimate interests which stand in the way or when it would entail a risk to public security or order or to the public weal of the Federal Republic or of any Land or be prejudicial to any overriding legitimate interests of a third party". 290/ Data stored by such establishments might be erased "when they are no longer required in connexion with existing contractual relationships or quasi-contractual relationships of trust and the person concerned has no overriding interests which stand in the way". The data should be erased "when their storage is inadmissible" and "when they are no longer required in connexion with the contractual and quasi-contractual relationship of trust and the person concerned requests their erasure". 291/ Personal data might be modified "only in the context of existing contractual relations or quasi-contractual relations of trust in so far as the person concerned has no overriding legitimate interests which stand in the way". 292/

243. For non-public establishments which process data on behalf of third parties, in so far as the establishment in question stores personal data in systems in the normal course of business for the purpose of communicating them to others and in fact so communicate them, the bill provided that the person concerned should be notified whenever data relating to him have been communicated, and might demand, upon the payment of a fee, information concerning stored data relating to his own person. No information would be supplied "when knowledge of the personal data may be prejudicial to public security or order or the common weal of the Federation or any Land or to any overriding legitimate interests of a third party". 293/ Non-public establishments might erase stored data when "the person concerned would not have legitimate interests which would stand in the way," and should erase them when "their storage is inadmissible" or "after five years have elapsed from the time of their storage, if the person concerned so requests". 294/ Modification of the data would be permissible where the person concerned "has no overriding legitimate interests which stand in the way". 295/

244. Agencies which store personal data in the normal course of business for purposes of modification and communication, in so far as they modify them in such a way that the data neither refer to nor permit recognition of any particular

---

290/ Section 20 (ibid., p. 9).

291/ Section 21 (2) (ibid., p. 10).

292/ Section 19 (ibid., p. 9).

293/ Sections 23 (1) and 26, pp. 10-11 and 12.

294/ Sections 23 (1), 1 and 27 (3) (ibid., pp. 10-11 and 42).

295/ Section 25, ibid.

person and communicate data in that form (for instance, market and opinion research institutes), would, according to the Bill, have to erase these data "when they are no longer required for the purposes of storage and, at the latest, five years after storage". 296/

245. Agencies which store personal data and in any way whatsoever modify them (as, for instance, wage calculation centres), with the exception of those which are functionally part of public departments, 297/ should be allowed to erase or modify the data "only with the agreement of the persons and establishments on whose behalf the data are processed". 298/

246. In the Notes of Guidance for Local Authorities, issued in the United Kingdom, it has been pointed out that: "Every precaution should be taken to ensure the accuracy and the validity of recorded data ... the appropriate Chief Officer only should be responsible for the erasure from files of data which is considered to be obsolete ..." 299/

247. The following general rules concerning the safeguards aiming at ensuring the accuracy of data and the rights of the individual have been recommended in the U.S. Department of Health, Education and Welfare Report, to be applied to administrative automated personal data systems:

> "Maintain data in the system with such accuracy, completeness, timeliness and pertinence as is necessary to assure accuracy and fairness in any determination relating to an individual's qualifications, character, rights, opportunities, or benefits that may be made on the basis of such data ...
>
> "Eliminate data from computer-accessible files when data are no longer timely.
>
> ...
>
> "Inform an individual, upon his request, whether he is subject of data in the system and if so make such data fully available to the individual upon his request in a form comprehensible to him.
>
> ...
>
> "Maintain procedures that (i) allow an individual who is the subject of data in the system to contest their accuracy, completeness, pertinence,

---

296/ Section 28, 2 (ibid., p. 13).

297/ Section 23 (1), 3 (ibid., p. 11) and Provisional Explanatory Memorandum (ibid., p. 43).

298/ Section 29 (ibid., p. 13).

299/ United Kingdom, LAMSAC, Computer Privacy, p. 10.

and the necessity for retaining them; (ii) permit data to be corrected or amended when the individual to whom they pertain so requests; and (iii) assure, when there is disagreement with the individual about whether a correction or amendment should be made, that the individual's claim is noted and included in any subsequent disclosure or dissemination of the disputed data."

The same report further proposed that:

"Any organization maintaining an administrative automated personal data system shall give public notice of the existence and character of its system once each year. Any organization maintaining more than one system shall publish such annual notices for all its systems simultaneously. Any organization proposing to establish a new system, or to enlarge an existing system, shall give public notice long enough in advance of the initiation or enlargement of the system to assure individuals who may be affected by its operation a reasonable opportunity to comment. The public notice shall specify:

(1) The name of the system;

(2) The nature and purpose(s) of the system;

(3) The categories and number of persons on whom data are (to be) maintained;

(4) The categories of data (to be) maintained, indicating which categories are (to be) stored in computer-accessible files;

(5) The organization's policies and practices regarding data storage, duration of retention of data, and disposal thereof;

(6) The categories of data sources;

(7) A description of all types of use (to be) made of data, indicating those involving computer-accessible files, and including all classes of users and the organizational relationships among them;

(8) The procedures whereby an individual can (i) be informed if he is the subject of data in the system; (ii) gain access to such data; and (iii) contest their accuracy, completeness, pertinence, and the necessity for retaining them;

(9) The title, name, and address of the person immediately responsible for the system." 300/

248. In the Report of the Younger Committee, the following principles have been suggested:

"There should be arrangements whereby the subject could be told about the information held concerning him.

...

"In the design of information systems, periods should be specified beyond which the information should not be held.

"Data held should be accurate. There should be machinery for the correction of inaccuracy and updating of information." 301/

(c) Rules relating to the use of personal data

249. There are various existing and proposed rules aiming to ensure that personal data stored in a computer are used only for the purposes for which they were collected.

250. The purposes for which the personal information can be used may be established by a restrictive enumeration of the circumstances in which it can be furnished and the authorities or persons to whom it can be disclosed. In this connexion, the Fair Credit Reporting Act (United States) provided that:

"A consumer reporting agency may furnish a consumer report under the following circumstances and no other:

(1) In response to the order of a court having jurisdiction to issue such an order.

300/ United States, HEW Report, pp. 56-58, 59-63. For organizations maintaining an automated personal data system used exclusively for statistical reporting or research, the same requirement has been proposed with the following change and addition: "(8) The procedures whereby an individual, group or organization can gain access to data for independent analysis; ... "(10) A statement of the system's provisions for data confidentiality and the legal basis for them". (Ibid., p. 100.)

301/ United Kingdom, Younger Report, para. 595. For similar suggestions see also Norman and Martin, op. cit., p. 473-477.

(2) In accordance with the written instructions of the consumer to whom it relates.

(3) To a person which it has reason to believe -

(A) intends to use the information in connexion with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; or

(B) intends to use the information for employment purposes; or

(C) intends to use the information in connexion with the underwriting of insurance involving the consumer; or

(D) intends to use the information in connexion with a determination of the consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status; or

(E) otherwise has a legitimate business need for the information in connexion with a business transaction involving the consumer." 302/

The Act provided in addition that every consumer reporting agency should maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under the above-quoted section 1681 b. 303/

251. For statistical systems, the United States Census Act 304/ provided that the information may not be used for any other purposes than the statistical purposes for which it had been supplied.

252. In the Report of the Younger Committee, the following principle has been suggested: "Information should be held for a specific purpose and not be used, without appropriate authorization, for other purposes". 305/

253. The following provision of section 4 (2) of the Data Surveillance Bill (United Kingdom 1969) aimed at conferring on the individual to whom the data relates a power to restrict their use to the purposes for which they were supplied:

302/ USC, title 15, para. 1681 b.

303/ USC, title 15, para. 1681 e.

304/ USC, title 13, para. 9.

305/ United Kingdom, Younger Report, para. 592. See also principle No. 1 in the draft resolution submitted to the Committee of Ministers of the Council of Europe and reproduced in paragraph 319 below.

"Every print-out ... shall be accompanied by a statement giving the following information: (a) the purpose for which the data contained in the print-out is to be used ... (b) the purpose for which the said data has in fact been used since the last print-out, supplied in accordance with this section; (c) the names and addresses of all recipients of all or part of the said data since the last print-out supplied in accordance with this section." 306/

254. In the United States Department of Health, Education and Welfare report a rule has been suggested according to which organizations maintaining administrative automated data systems should:

"inform an individual, upon his request, about the uses made of data about him, including the identity of all persons and organizations involved and their relationship with the system;

"assure that no use of individually identifiable data is made that is not within the stated purposes of the system as reasonably understood by the individual, unless the informed consent of the individual has been explicitly obtained." 307/

255. The relevant provisions of the Data Protection Act (State of Hessen, Federal Republic of Germany 1970) read as follows:

"Section 3. Data secrecy

"1. Persons responsible for the preparation, transmission, storage or automatic processing of data shall be prohibited from communicating or making available to other persons any information concerning the records, data and results gained during the course of their duties and from enabling other persons to obtain such information except where authority exists by this virtue of the provisions of law or the consent of those entitled to exercise control over records, data and results.

"2. The prohibition in Subsection 1 shall not apply if the procedures described therein are necessary for the administrative or technical operations involved in data processing.

"3. The duty to maintain secrecy shall persist after the completion of the procedures referred to in Subsection 1.

306/ Warner and Stone, op. cit., p. 229. For the provisions of paragraph (1) of section 4 of the bill relating to the right of the individual to obtain the print-out referred to above, see paragraph 238 above.

307/ United States, HEW Report, pp. 62-63.

"4. The legal duty to provide information shall not be affected.

"Section 5. Data banks and information systems

"1. Records, data and results may be communicated for the constitution of data banks and information systems and for the statistical purposes of the establishments referred to in Section 1.

"2. In the case of data banks and information systems it must be ensured that none of the establishments referred to may consult or extract records, data and results other than those to which it is entitled.

"3. Data and stocks of data containing no individual details concerning natural or legal persons and permitting no such details to be inferred may be communicated and published when there is no legal prohibition against it nor any important public interest to prevent it. As a rule public interest shall not stand in the way of the Land Parliament's right to information (Section 6(1)).

"Section 6. Right of Land Parliament and local representative bodies to information

"1. The Hessen data processing centre, local district computer centres and the Land authorities operating data-processing installations shall be bound to give the Land Parliament, the Prime Minister of the Land Parliament and the parliamentary parties such information from the stored data as they are entitled to receive, provided the requirements of Section 5, Subsection 3 are satisfied and processing programmes exist.

"2. In respect of the Hessen data-processing centre, the relevant local district computer centre and other data-processing installations operated by Gemeinde and Landkreise, the right to information referred to in Subsection 1 shall be vested in district and local councils (Gemeindevertretungen and Kreistage) their political groups and appropriate bodies instituted by the corporations and establishments referred to in Section 1, each within its sphere of responsibility. Any application from the political groups shall be submitted through the Gemeinde authorities or the Kreis Council.

"3. In case of doubt the decision of the controlling authority shall be final." 308/

256. According to the Swedish Data Act (1973), the person responsible for the computerized personal data system, any person who has dealt with the register or

---

308/ Quoted from the International Social Science Journal, UNESCO, vol. XXIV, No. 3, 1972, pp. 580-581.

the lawful recipient of the information may not reveal without authorization what he has learnt from it about the personal circumstances of an individual.

257. Under the Post Office (Data Processing Service) Act (United Kingdom 1967), information obtained by any officer of the Post Office in the course of the provision by the Postmaster General for any person of services and facilities for the processing of data by computer should not, without the consent of that person, be disclosed by that officer, except for the purpose of performing his duties in relation to those services or facilities or in such cases as may be required by law.

258. According to the United States Census Act, the officials of the Census Bureau may not permit anyone other than the sworn officers to examine an individual report. 309/

259. The draft bill on protection against the misuse of personal data in data processing (Federal Republic of Germany 1972) contained the following provisions relevant to the issue of preventing unauthorized access to personal data when these are exchanged between public departments:

> "In cases where personal data may be communicated by automatic devices, steps shall be taken to ensure ... in particular that no unauthorized person can obtain such data." 310/

260. In the U.S. Department of Health, Education and Welfare Report, the following rule has been proposed for organizations maintaining administrative automated personal data systems:

> "Make no transfer of individually identifiable personal data to another system without (i) specifying requirements for security of the data, including limitations on access thereto, and (ii) determining that the conditions of the transfer provide substantial assurance that those requirements and limitations will be observed - except in instances when an individual specifically requests that data about himself be transferred to another system or organization;" 311/

A similar rule has been proposed for organizations maintaining automated personal data systems used exclusively for statistical reporting and research with the following modification of the last sentence: "... except in instances when each of the individuals about whom data are to be transferred has given his prior informed consent to the transfer". 312/

309/ USC, title 13, para. g (2) and (3).

310/ Section 7 (3) (Council of Europe, EXP/Prot. Priv./EDB (73) 2, p. 3-4).

311/ United States, HEW Report, p. 55.

312/ Ibid., p. 98.

261. In the Report of the Younger Committee, a suggested principle for handling personal information reads as follows: "Access to information should be confined to those authorized to have it for the purpose for which it was supplied." 313/

262. To prevent unauthorized disclosure or dissemination of information, various existing or suggested rules often expressly enumerate the authorities or persons to whom the data may be lawfully communicated.

263. According to the law on centralization of documentation relating to road traffic (France 1970), a complete print-out of the information can be transmitted exclusively to the person concerned, the judicial authorities and the prefect, in connexion with an offence which may imply the withdrawal of the driver's licence. Administrative and military authorities, for data concerning persons employed as drivers or persons applying for such employment and insurance companies, for data concerning their policy holders can obtain, at their request, only the information strictly related to the driver's licence and the category to which the driver, according to the danger which his behaviour presents, has been considered to belong. No individually identifiable information can be disclosed to any other person or authority (articles 4, 5 and 6 of the law).

264. In accordance with article 8 of the Belgian draft bill on a national register:

> "Paragraph 1: Information from the National Register may be divulged only by the department responsible for keeping the Register, or by any department designated by the King.
>
> "Paragraph 2: Such information may be obtained only:
>
> "1. By persons to whom it refers or by their legal representative, in so far as the information relates to them;
>
> "2. By third parties, subject to such conditions as the King may establish and in so far as the divulging of the requested information by the authority in possession of it would be permissible;
>
> "3. By governmental offices and other public agencies:
>
> "(a) In respect of information which they have supplied;
>
> "(b) In so far as the divulging of the information which they request is authorized by the relevant laws and regulations."

313/ United Kingdom, Younger Report, para. 592. With regard to the limitation of the access to the information, see also principle No. 3 in the draft resolution submitted to the Committee of Ministers of the Council of Europe, reproduced in para. 319.

265. The Swedish Data Act (1973) forbade the persons responsible for a computerized personal data system to supply information if they have reasons to suspect that it will be used for purposes contrary to the provisions of the Act. The Act further provided that in the regulations which the Data Inspection Board may issue concerning the operation of the systems under its supervision, should, in order to protect the right to privacy, 314/ contain instructions relating, among others, to the following questions: what data may be retrieved from the system, to whom the data may be delivered and how they may be used.

266. With regard to personal information used exclusively for statistical reporting and research, several United States statutes have provided various measures of protection against its unlawful disclosure.

267. According to the Census Act, personal data collected by the Bureau of the Census should not be made the object of "any publication whereby the data ... can be identified". 315/ This Act established hereby an absolute prohibition against disclosure.

268. The Fair Credit Reporting Act prohibited dissemination of obsolete information by its inclusion in consumer reports. Such information and the period of obsolescence have been specified in the Act as follows: bankruptcies - 14 years; suits and judgements - seven years; paid tax liens - seven years; accounts placed for collection or written off - seven years; records of arrest, indictment or conviction of crime - seven years; any other adverse information - seven years. Exceptions have been made for credit transactions and life insurance of $50,000 or more and for employment at an annual salary of $20,000 or more. 316/

269. Elaborate provisions concerning the regulation of dissemination of personal data have been also included in the draft bill on protection against the misuse of personal data in data processing (Federal Republic of Germany 1972). According to a provision of the draft, exchange of data by public departments would be allowed only with the personal agreement of the person concerned, on the basis of a legal provision or in order to further the legitimate fulfilment of tasks for which the recipient is competent (section 7 (1)). 317/ The same rule would apply, in general, to communication of data to third parties (section 8). 318/ Special rules referred to the circumstances under which non-official establishments which process personal

---

314/ See para. 289 below.

315/ USC, title 13, 9 a (2). See also principle No. 4 of the draft resolution submitted to the Committee of Ministers of the Council of Europe reproduced in paragraph 319 below.

316/ USC, title 15, para. 1681 c.

317/ Council of Europe, EXP/Prot. Priv/EDB(73)2, p. 3.

318/ Ibid., p. 4.

data for their own purposes or on behalf of third parties would be permitted to communicate or transmit such data (such as the agreement of the person concerned, the existence of a legal provision or of a contractural or quasi-contractual relationship, the legitimate interest of the applicant). 319/

270. In the United States Department of Health, Education and Welfare report, the following rules have been proposed for "organizations which maintain administrative personal data systems that publicly disseminate statistical reports or research findings based on personal data drawn from the system, or from administrative systems of other organizations":

> "Make such data publicly available for independent analysis, on reasonable terms ...
>
> "Take reasonable precautions to assure that no data made available for independent analysis will be used in a way that might reasonably be expected to prejudice judgements about any individual data subject's character, qualifications, rights, opportunities and benefits." 320/

319/ Section 18 (ibid., p. 8); section 24 (ibid., p. 11); sections 28 (1) and 29 (ibid., p. 13).

320/ United States, HEW Report, pp. 86-87.

3. Rules relating to administrative supervision and control

271. Various methods and mechanisms to be used for supervising the activities of computerized personal data systems and for implementing the safeguards dealt with under subsection (b) above, have been proposed or have sometimes been provided for in existing laws.

(a) Methods applicable within the organizations maintaining computerized personal data systems

272. The opinion has been expressed that compliance with safeguard requirements provided for by legislation could be assured without the establishment of new mechanisms or outside controls, 321/ since the establishment of independent bodies with a "watchdog role" might prove difficult in practice and could create obstacles to further development of electronic data processing technology which has already brought a variety of benefits to a wide range of people and institutions in modern society. 322/

273. Thus, the draft bill on protection against the misuse of personal data in data processing (Federal Republic of Germany, 1972) in section 14, entitled "Implementation of data protection in the Federal governmental departments", provided that:

> "The highest Federal authorities, the governing body of the German railways and any public-law corporations, institutions and foundations directly responsible to the Federal Government over which legal supervision alone is carried out by some senior Federal authority shall be each and severally required to ensure implementation of this Act and of any other legal provisions on data protection. They shall in particular ensure:
>
> "1. that a list is made of the type of personal data held in storage of the tasks for whose fulfilment a knowledge of the data is required, and of the regular recipients thereof, and
>
> "2. that the data processing programmes by means of which personal data are to be processed are checked for accuracy and for conformity with the regulations governing their use."

274. According to section 15 of the bill, the authorities specified in section 14 would have to issue administrative regulations for the application of the law, taking into account the circumstances peculiar to each area of activity. 323/

275. With regard to non-official establishments which process personal data for their own purposes, the bill (section 22) provided that they must engage "a data protection officer whose task will be to ensure that this Act and any other regulation on data protection are properly observed". The duties of this officer

---

321/ See, for instance, Filip, loc. cit., p. 443.

322/ See, for instance, United States, HEW Report, pp. 43-44.

323/ Council of Europe, EXP (Prot. Priv.) EDB (73), 2, p. 7. /...

would consist of supervising the type of data being stored; the purposes for which knowledge of such data is required, the recipients of such information and the accuracy and proper applications of personal data processing programmes; and of briefing the relevant staff on the provisions of the Act or any other relevant provisions. 324/

276. In the United States Department of Health, Education and Welfare report, it has been suggested, as a rule applicable to any organization maintaining an administrative automated personal data system or a system used exclusively for statistical reporting and research, that each organization should:

> "Identify one person immediately responsible for the system, and make any other organizational arrangements that are necessary to assure continuing attention to the fulfillment of the safeguard requirements;
>
> "Take affirmative action to inform each of its employees having any responsibility or function in the design, development, operation, or maintenance of the system, or the use of any data contained therein, about all the safeguard requirements and all the rules and procedures of the organization designed to assure compliance with them ...". 325/

(b) The establishment of a register of computerized personal data systems

277. As a mechanism of supervision and control with certain powers of decision, the establishment of a register for personal data banks has been suggested in the Data Surveillance Bill (United Kingdom 1969). The relevant provisions read as follows:

> "1. (1) A register shall be kept by the Registrar of Restrictive Trading Agreements (hereinafter in this Act referred to as 'the Registrar') of all data banks as hereinafter defined which are operated by or on behalf of any of the following:
>
> "(a) any agency of central or local government;
>
> "(b) any public corporation;
>
> "(c) any person exercising public authority;
>
> "(d) any person offering to supply information about any other person's credit-worthiness, whether to members of a particular trade or otherwise and irrespective of whether payment is made therefor;

324/ Ibid., p. 10.

325/ United States, HEW Report, pp. 59 and 97-98.

"(e) any private detective agency or other person undertaking to carry out investigations into any other person's character, abilities or conduct on behalf of third parties;

"(f) any person who offers for sale information stored in such data bank, whether to the general public or otherwise.

"(2) The register referred to in the foregoing sub-section shall contain the following information concerning each data bank:

"(a) the name and address of the owner of the data bank;

"(b) the name and address of the person responsible for its operation;

"(c) the location of the data bank;

"(d) such technical specifications relating to the data bank as may be required by the Registrar;

"(e) the nature of the data stored or to be stored therein;

"(f) the purpose for which data is stored therein;

"(g) the class of persons authorised to extract data therefrom.

"(3) The owner of the data bank shall be required to register the information referred to in paragraphs (a) to (c) of the foregoing sub-section. The person responsible for the operation of the data bank shall be required to register the information referred to in paragraphs (a) to (g) of the foregoing sub-section.

"(4) Any person responsible for registering information under this section shall be required to inform the Registrar of any alterations of, additions to, or deletions from the said information within four weeks of such alteration taking effect, subject to the provisions of sub-section (6) below.

"(5) If at any time the Registrar is of the opinion that in the circumstances the information given or sought to be given under paragraphs (f) or (g) of sub-section (2) above might result in the infliction of undue hardship upon any person or persons or be not in the interest of the public generally, he may order such entry to be expunged from or not entered in the register. In reaching a decision under this or the next following sub-section, the Registrar shall be guided by the principle that only data relevant to the purposes for which the data bank is operated should be stored therein, and that such data should only be disclosed for those same purposes.

"(6) An alteration to the register in respect of paragraphs (f) or (g) of sub-section (2) above shall be made by application to the Registrar who shall, not earlier than four weeks after receipt of such application, grant or reject the application giving his reasons in writing.

/...

"(7) The register together with applications submitted in accordance with the last foregoing sub-section shall be open to inspection by the public, including the press, during normal office hours:

Provided that entries relating to data banks operated by the police, the security services and the armed forces shall be kept in a separate part of the register which shall not be open to inspection by the public.

...

"3. (1) The Registrar shall submit annually to Parliament a report covering the previous calendar year in which he shall state the number of data banks entered on the register, the number of such data banks which fall within the terms of section 2(1)(a) and of section 2(1)(b) to (d) 326/ respectively and the number of instances in which he ordered entries to be amended under section 1(5) or refused an application to alter an entry under section 1(6).

"(2) The Registrar's report may contain such additional information statistical and otherwise, as the Registrar may think fit." 327/

278. Under the draft bill on protection against the misuse of personal data in data processing (Federal Republic of Germany 1972) a register of private establishments which process personal data for third parties, if such establishments store for communication and communicate these data on a professional basis (e.g., inquiry and detective agencies) would be established. The supervisory authority with which the registration would be made would watch over the implementation of the provisions of the proposed law which concern these establishments. 328/

279. Some writers have also proposed that a register of computerized personal data systems should be established. 329/

(c) The establishment of an independent centralized supervisory agency

280. The report of the Younger Committee, taking into account the opinion of its authors that the time was not ripe for detailed controls over computerized personal data systems made the following recommendation:

"that the Government should legislate to provide itself with machinery for keeping under review the growth in and techniques of gathering personal information and processing it with the help of computers". 330/

326/ For the provisions of section 2 (1) a - d, see paragraph 198 above.

327/ Warner and Stone, op. cit., pp. 227-228.

328/ Sections 30 and 31 of the bill (Council of Europe EXP/Prot. Priv. EDB (73)2, pp. 13-14).

329/ For instance, Martin and Norman, op. cit., pp. 471-472.

330/ United Kingdom, Younger Report, para. 621. A similar suggestion to be considered by the Younger Committee was made in March 1971 by the British Computer Society (see Submission of Evidence to the Committee on Privacy, March 1971, Prepared by the Privacy Committee of the British Computer Society, p. 24).

281. In France, some writers have suggested that any system of safeguards for protecting the right to privacy should provide for an agency called in various proposals "control commission" (Commission de contrôle) or "surveillance commission" (Commission de surveillance) or "safeguarding commission" (Commission de sauvegarde). In the annual report of the Conseil d'Etat for 1969-1970 on the consequences of the development of informatics on public and private liberties and on administrative decisions 331/ such an agency was called "the High Committee" (Haut Comité). 332/ Similar proposals have been made in the United States 333/ and Canada. 334/

282. In the proposals regarding the establishment of a supervisory agency in the field of computerized personal information, such a body was conceived as having an independent character par excellence. For this purpose, it should consist of "eminent personalities", experts in informatics and lawyers. 335/ According to the report of the Younger Committee, the machinery referred to in paragraph 280 above would take the form of an independent body (called a standing commission) with members drawn from both the computer world and outside. 336/

283. The functions of these proposed agencies would consist, in essence, of studying and surveying the computerized information stores and making recommendations concerning legislative or other controls for safeguarding the handling of information in such stores. It has been suggested further that such an agency should be invested with functions of the ombudsman type, that is, to receive complaints from the public, to investigate them and issue reports on its findings. 337/ Educational and public relations duties have been stressed by one writer. 338/

331/ See Braibant, La protection des droits individuels, Premières journées juridiques franco-nordiques (Upsala-Stockholm, 24-27 October 1971), p. 19.

332/ Ibid.

333/ Miller, op. cit., pp. 234-238; United States, HEW Report, p. 42.

334/ Canada, Privacy and Computers, op. cit., pp. 160-162.

335/ Braibant, loc. cit., p. 812; Miller (op. cit., p. 234) referred to people "who are versed in the relevant scientific and technical disciplines, the ways of the scientific community, the social sciences, the communications and computer industries and the law".

336/ United Kingdom, Younger Report, para. 621.

337/ United Kingdom, Younger Report, para. 622.

338/ Miller, op. cit., pp. 234-235.

284. Different opinions have been expressed regarding the advisability of investing the agency with rule-making powers or licensing authority. 339/

285. In the United States doubts have been expressed regarding the feasibility 340/ or the desirability of the establishment of a centralized and independent Federal agency to regulate the use of all computerized personal data systems. 341/

286. An authority with extensive powers of supervision, control and regulation of the activity of computerized personal data systems, the Data Inspection Board, has been established in Sweden by the Data Act (1973).

287. The Data Inspection Board has the duty to ensure that automated data processing does not cause undue encroachment on privacy. Supervision is to be carried out in such a way as to avoid unnecessary expenses or inconveniences.

288. The Board has been invested with the right to grant permission for the establishing and/or maintenance of personal computerized files (with the exceptions mentioned in paragraph 195 above), paying special attention to the criteria indicated in paragraph 231 above. Permission is to be granted if there is no reason to assume that undue encroachment could result with respect to the privacy of the individual about whom the information will be stored. It may be withdrawn in cases where, after the functioning of the respective system, such an encroachment could not have been avoided.

289. When granting permission, the Data Inspection Board is to issue regulations regarding the matters mentioned in paragraphs 211 and 220 above. In addition, it may issue regulations, if they are needed to avoid the danger of undue encroachment on privacy, concerning various measures to be taken to this effect, mentioned in paragraphs 171 (a), 217 (a), 223 and 265. Such regulations may be also issued by the Board if the King in Council or the Riksdag have not done so, in exercising their prerogative in establishing computerized personal data systems (see paragraph 195 above). The Board is further entitled to alter the existing regulations or issue new ones if undue encroachment on privacy arises or there are reasons to suppose that it might arise as a result of the functioning of the system.

290. In addition, the Data Inspection Board has the right to inspect computer centres and all their installations and documents and to obtain, from the person responsible for the centre, all information necessary to the purposes of the inspection.

339/ Ibid., p. 135; for different opinions, see Braibant, loc. cit., p. 812 and United States, HEW Report, pp. 42-43.

340/ Miller (op. cit., p. 234), though examining in detail the features of a Federal informational privacy agency, felt that it may never come into existence.

341/ United States, HEW Report, pp. 42-43.

(d) The establishment of an independent administrative tribunal

291. A number of proposals have envisaged the establishment of an administrative tribunal with large powers of supervising the practices of computerized systems as they affect privacy, implementing various safeguards (technological, administrative and legal), making decisions in particular cases, developing additional regulations, hearing individual complaints and licensing data banks. 342/ The establishment of such a tribunal having extensive powers regarding the licensing of computerized systems and equipped as a quasi-judicial body and backed by an inspectorate has been proposed in the Control of Personal Information Bill (United Kingdom 1971). 343/

292. In the Belgian draft bill on the protection of privacy and personality, the following judicial and administrative system has been proposed: (a) inferior courts would be competent to examine any suits relating to the collection, processing, reproduction or the use by any means of the personal information covered by the law; (b) a "Chamber for the control of electronics" (Chambre de contrôle de l'électronique) as a special court would be established by the Crown, to be presided over by a judge. This special Chamber would have the power to control all public or private computerized systems or centres of documentation, which would register with the Chamber and implement its injunctions (article 12 of the draft).

(e) The ombudsman

293. The institution of the ombudsman (a parliamentary commissioner, independent from the executive, whose tasks involve supervising the activities of the administration, receiving complaints from citizens and reporting to the legislature) is known in various countries. 344/

294. The Data Protection Act (Land Hessen 1970) has established an ombudsman with the title of Data Protection Commissioner. 345/ He is elected by the Land Parliament. The Commissioner is to ensure that the provisions of the Data Protection Act and other regulations governing the confidential handling of information provided by citizens and of records relating to individual citizens are observed in the course of automatic data processing in the establishments to which the Act is applicable. He is to inform the responsible control authorities of any infringements committed and initiate measures for improving data protection. The Commissioner has been empowered to receive complaints from any person who considers that his rights have been violated by the automatic data processing

---

342/ Canada, Privacy and Computers, pp. 159-160.

343/ United Kingdom, Younger Report, paras. 604. 607 and 608.

344/ For details, see Study of Equality in the Administration of Justice, (United Nations publication, Sales No. E.71.XIV.3), paras. 336-341.

345/ Sections 7 to 15 of the Act (reproduced in the International Social Science Journal, UNESCO, vol. XXIV, No. 3, 1972, pp. 581-583.

of personal records. At the request of the Land Parliament, of the President of the Land Parliament, of the parliamentary and of other representative bodies which, under the provisions of the Act, have a right to computerized information, the Data Protection Commissioner must investigate the reasons for which their requests for information have not been met or have not been fully satisfied. The Commissioner is entitled to obtain the information needed in the performance of his duties from the establishments covered by the Act. An annual report on the results of his activities is to be submitted by the Commissioner to the Land Parliament and to the Prime Minister.

295. Suggestions to establish an ombudsman for the activities of computerized personal data systems have been made in several countries, including Canada, 346/ the United Kingdom 347/ and the United States. 348/

4. Rules relating to civil liability

296. As has been pointed out, the use of computerized personal data systems gives rise to new problems relating to civil liability. Such problems may arise either from voluntary or involuntary errors in the data processing or from leakage of confidential information, since either could produce substantial damage. Even if judicial and administrative tribunals have developed a case law relating to violation of professional secrecy and to delivery of erroneous or misleading information, the difficulty of establishing who is liable for the damage (the owner of the automated system, the manager or the users) raises new problems of civil liability in connexion with the use of computers. 349/ The problem is even more complex in the case of time-sharing systems where the central system may belong to, be operated by or be used by, one person and the terminals by others.

297. Some of the existing and proposed legislation relating to computerized personal data systems contains provisions relating to civil liability for certain acts which violate the regulations governing the handling of information about individuals.

298. The Fair Credit Reporting Act (United States 1971) provided for civil liability of consumer reporting agencies or users of information for wilful or negligent non-compliance with its requirements which results in actual damage to the consumer. 350/

346/ Canada, Privacy and Computers, p. 181.

347/ Warner and Stone, op. cit., p. 190.

348/ Martin and Norman, op. cit., pp. 513-516; United States, Report of the National Academy of Sciences, p. 181; United States, HEW Report, p. 42 (expressing reservations as to the feasibility of such suggestions in the context of American legal, political and administrative traditions).

349/ Braibant, "La protection des droits individuels ...", Revue internationale de droit comparé (1971, No. 4), pp. 815-816.

350/ USC, title 15, para. 1681m and para. 1681o. In the case of wilful non-compliance, punitive damages may be collected by the court.

299. According to the Swedish Data Act of 1973, the person responsible for a personal computerized file shall pay compensation to the individual concerned for damage he may have suffered due to incorrect information being held in his file. In assessing the amount of damage, the suffering caused and circumstances of other than a purely pecuniary nature are to be taken into consideration.

300. The Data Surveillance Bill (United Kingdom 1969) provided that an operator of a computerized system (that is, the person responsible for its operation and for the introduction into and extraction from it of data), who causes or permits inaccurate personal data to be supplied would be held liable for damages to the person who had thus suffered loss (section 7). Civil liability to the person whose personal data is involved would also be incurred in cases where the operator, by non-wilful acts or omissions (a) failed or refused to send a print-out when under a duty so to do; or (b) permited data stored in the computerized system to be used for purposes other than those stated on the register; or (c) allowed access to the said data to persons other than those entered on the register as having authorized access; or (d) failed or refused to comply with a decision of the Registrar (section 6 (2)). 351/

301. The Code of Fair Information Practice for all Automated Personal Data Systems, proposed for enactment by the United States Department of Health, Education, and Welfare "should give individuals the right to bring suits for unfair information practice 352/ to recover actual, liquidated and punitive damages, in individual or class actions. It should also provide for recovery of reasonable attorney's fees and other costs of litigation incurred by individuals who bring successful suits. 353/

5. Rules relating to criminal liability

302. Existing and proposed legislation contains provisions making punishable, under penal law or sometimes under administrative law, acts or omissions violating their requirements.

303. In United States statutory law, there is a general provision making an offence the disclosure, by governmental officers and employees, of confidential information. 354/ According to the Census Act, an employee of the Census Bureau, who publishes or communicates, without the authorization required by the Act, information coming into his possession by reason of his employment commits an offence, punishable by fine, or imprisonment, or both. 355/

351/ Warner and Stone, op. cit., p. 230.

352/ "Unfair information practice" means violations of any safeguard requirement.

353/ United States, HEW Report, p. 150.

354/ USC, title 18, para. 1905.

355/ USC, title 13, para. 44.

304. Provisions for criminal penalties similar to those for violation of secrecy of conviction records are provided in the French law of centralization of documentation on road traffic (1970). 356/

305. The Data Protection Act of Hessen (1970) provided (section 16) that "whosoever intentionally or through negligence, contrary to section 3, 357/ contributes to making information covered by data protection available to unauthorized persons shall commit an offence". 358/

306. The Swedish Data Act (1973) provided that persons infringing certain of its provisions (such as those relating to the obligation to obtain a permission from the Data Inspection Board, communication of personal information, observing professional secret) or delivering incorrect information to the Data Inspection Board would incur the penalty of a fine or be sentenced to maximum one year of imprisonment. In addition, the Act established the crime of "data trespassing", stipulating that anybody unlawfully gaining access to a computerized file or unlawfully altering or erasing such a file may be fined or sentenced to a maximum of two years' imprisonment if the offence is not punishable under the Penal Code. A money penalty may be imposed on the person responsible for a computerized personal data system, if access has been denied to the Board to the premises or to the documents of the system and if the person refused to give the necessary information (see paragraph 290 above) or has not fulfilled its duties mentioned in paragraphs 228 and 233 above.

307. According to the Data Surveillance Bill (United Kingdom 1969), if the operator of a computerized personal data system had wilfully committed the acts or omissions mentioned in paragraph 300 above, he would have been liable on summary conviction to a fine and on conviction on indictment to a fine or imprisonment or both. The bill also considered a criminal offence the failure of the person who owns the computer or of the operator thereof to register it in accordance with the relevant provisions of the Act. 359/

308. Under the Bill, a person who aided, abetted, counselled, or procured the commission of one of the above-mentioned offences or who, with knowledge of its wrongful acquisition, received, used, handled, sold or otherwise disposed of information obtained as a result of such an offence would be likewise considered guilty. 360/

356/ Articles 8-10 of the law; see also Braibant, loc. cit., p. 804.

357/ For the provisions of this section, see paragraph 255 above.

358/ Text quoted from the International Social Science Journal, UNESCO, (vol. XXIV, No. 3, 1972), p. 583.

359/ Section 6 (2) (Warner and Stone, op. cit., p. 230).

360/ Section 6 (3) (ibid., p. 230).

309. The draft bill on protection against the misuse of personal data in data processing (Federal Republic of Germany 1972) contained provisions declaring a criminal offence unauthorized disclosure by any person of data stored in the establishments covered by the bill and declaring administrative offences violations by any person of certain requirements of the draft. 361/

310. According to the Belgian draft bill on the national register (article 5), offences violating the provisions of article 8 (quoted in paragraph 261 above) would be punishable under article 458 of the Penal Code. 362/

311. It has been proposed that the Code of Fair Information Practice for all Automated Personal Data Systems, whose enactment has been suggested in the United States Department of Health, Education, and Welfare report, should prohibit violation of any safeguard requirement as an "unfair information practice"; any such violation would be subject to both civil and criminal penalties. The issuance of injunctions to prevent violation of any safeguard requirements has also been suggested. 363/

6. Safeguards relating to the use of computerized data as evidence in civil proceedings

312. In United States legal literature it has been said that, though the use of computers raises many interesting questions concerning the admissibility of evidence and techniques of proof, because computer systems involve records that differ from traditional records significantly in appearance, format, and content, no rules are needed to render computerized records admissible. 364/ Nevertheless, a statute of the state of Delaware (the Delaware General Corporation Law, section 224), included provisions relating to the admissibility as evidence of computerized data. 365/

361/ See sections 32 and 33 of the bill (Council of Europe, EXP/Prot.Priv./EDB 73 (2), p. 15-1).

362/ Article 458 of the Belgian Penal Code reads as follows:

> "Doctors, surgeons, medical practitioners, chemists, midwives, and any other person who, by position or occupation are the recipients of confidential information and who, except when called upon to give evidence in legal proceedings or when required by law to disclose such confidential information, divulge the same shall be liable for imprisonment for eight days to six months and a fine of B.Frs. 100 to B.Frs. 500" (OECD, Directorate for Scientific Affairs, Group of Experts on Computer Utilization, Computer Utilization and the Privacy Problem, Belgian Reply to the Questionnaire (Paris, August 1970), p. 7).

363/ United States, HEW Report, p. 50.

364/ Computers and the Law: An Introductory Handbook, Robert P. Bigelow, ed., Second Edition, (Chicago, Commerce Clearing House), 1969, pp. 139-140.

365/ Ibid., pp. 140-143.

313. In the United Kingdom, the Civil Evidence Act 1968 included provisions regarding the "admissibility of statements produced by computers" in civil proceedings. The act established, inter alia, the following requirements to be met by such evidence in order to ensure its probative value and the procedural rights of the individual:

"5. (1) In any civil proceedings a statement contained in a document produced by a computer shall, subject to rules of court, be admissible as evidence of any fact stated therein of which direct oral evidence would be admissible, if it is shown that the conditions mentioned in subsection (2) are satisfied in relation to the statement and computer in question.

"(2) The said conditions are -

"(a) that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period, whether for profit or not, by any body, whether corporate or not, or by any individual;

"(b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained in the statement or of the kind from which the information so contained is derived;

"(c) that throughout the material part of that period the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents; and

"(d) that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.

"(3) Where over a period the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in subsection (2) (a) above was regularly performed by computers, whether -

"(a) by a combination of computers operating over that period; or

"(b) by different computers operating in succession over that period; or

"(c) by different combinations of computers operating in succession over that period; or

"(d) in any other manner involving the successive operation over that period, in whatever order, of one or more combinations of computers,

/...

all the computers used for that purpose during that period shall be treated for the purposes of this Part as constituting a single computer; and references in this Part to a computer shall be construed accordingly.

"(4) In any civil proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say -

"(a) identifying the document containing the statement and describing the manner in which it was produced;

"(b) giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer;

"(c) dealing with any of the matters to which the conditions mentioned in subsection (2) above relate,

and purporting to be signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

"(5) For the purposes of this Part of this Act -

"(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

"(b) where, in the course of activities carried on by any individual or body, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

"(c) a document shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

"(6) Subject to subsection (3) above, in this Part of this Act 'computer' means any device for storing and processing information, and any reference to information being derived from other information is a reference to its being derived therefrom by calculation, comparison or any other process."

314. The Government of Trinidad and Tobago has reported as follows:

> "As a direct consequence of the use of computers and electronic devices Parliament has seen it fit to enact legislation to permit the use of information derived and accumulated by computer to be given in evidence in a court of law.
>
> The Evidence (Amendment) Bill, 1973 which should be assented to and proclaimed shortly, recognizes the age of computerization and electronic devices, as an integral part of the development of Society and makes provision for the reception of evidence and consequent protection of human rights." 366/

7. Safeguards against threats posed by transnational computerized personal data systems

315. According to the Swedish Data Act (1973), data to be used abroad for automated processing can be communicated only with the permission of the Data Inspection Board; such permission may be given only if it may be assumed that the communication would not cause undue encroachment on privacy.

316. In the report of the Canadian Task Force, several proposals for government policies in relation to the storage in the United States of personal information about Canadians have been discussed. According to one proposal, reliance on United States law for protection would be sufficient. Such a course of action would present the disadvantage of relying upon laws over which Canada has no control. Another proposal envisaged requiring companies in Canada storing data in foreign computerized systems to register with the appropriate Canadian authority. Such a procedure, however, was considered as cumbersome. The same objection was formulated against the proposal to require that a complete set of duplicate files be kept in Canada, which would be in addition a more expensive procedure. According to a fourth proposal, the storage abroad of data about Canadians should be entirely prevented, an option deemed undesirable since it would hamper the flow of information and be nearly impossible to enforce. 367/

317. One writer has pointed out the advisability of adopting international safeguards against the threats to human rights arising from transnational computerized systems, stating that:

> "It would be pointless to adopt national legislation to protect rights and liberties against the threats posed by computers unless they were speedily supplemented and strengthened by international agreements. As a result of technological progress, data transmission and processing take

---

366/ Information furnished by the Government of Trinidad and Tobago on 27 July 1973, including a copy of the bill, which contains provisions similar to those reproduced in paragraph 313 above.

367/ Canada, Privacy and Computers, pp. 171-172.

place without regard to national frontiers; files of small bulk can be easily transported from one country to another, and remote data techniques make it possible to process files relating to citizens of another country, as is shown by the example of relations between Canada and the United States ...

"The problem requires a solution at the international level, which could be sought both in the field of international conventions on human rights and in that of telecommunications agreements." 368/

368/ Braibant, loc. cit., p. 817.

V. SUGGESTED INTERNATIONAL STANDARDS

A. Existing proposals for international conventions or standards

318. The idea of the adoption of a multilateral international convention which would embody a set of model rules for the protection of persons about whom data is stored and recognize also the international implications of the question of computers and privacy has been advocated in the report of the Canadian Task Force. 369/

319. On 14 June 1972 the Committee on the protection of privacy against electronic data banks submitted to the Committee of Ministers of the Council of Europe the following draft resolution, relating only to computerized systems in private sectors:

"The Committee of Ministers,

"Considering that the objective of the Council of Europe is closer union among its member States,

"Aware of the increasing development of data processing,

"Aware that, in order to prevent abuses during the gathering, processing and dissemination of data of a personal nature by electronic data banks in the private sector, legal guarantees for the protection of physical or juridical persons may become necessary,

"Convinced of the desirability of proceeding at once, pending the possible drafting of an international agreement, to take measures designed to avoid new discrepancies between the legal systems of member States in this matter,

"Recalling 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, 370/

"Recommends that Governments of member States should:

"(a) Take the principles appended to this resolution into account when drafting national laws;

"(b) Keep the Committee of Ministers informed of steps taken in this field.

369/ Canada, Privacy and Computers, pp. 173-174.

370/ Resolution No.3, on the protection of privacy in view of the increasing compilation of personal data into computers, recommended "to the Committee of Ministers to pay fullest attention to this work and to invite the Committee of Experts to examine the possibility of elaborating a draft international convention in this field".

"Principles for the protection of privacy in relation to electronic data banks */ in the private sector

"1. Personal data may not, without appropriate authorization, be used for purposes other than those for which they were gathered, nor may they be communicated to third parties.

"2. The set of data must not contain unsuitable data or data in excess of those needed for the desired purposes.

"3. Access to the data should be restricted to persons who can give proof of a legitimate interest in them.

"4. Statistical data may be published only in aggregated form and in such a way as to make it impossible to reconstitute information from which persons could be identified.

"5. Measures are needed to enable the person concerned to ascertain the nature of the data gathered relating to that person, the uses planned for it and, if possible, to whom any such data have been divulged.

"6. Precautions should be taken to prevent any abuse or misuse of the data.

"For that purpose, security systems should be installed before the electronic data banks are put into operation.

"They should make it possible to prevent or detect both intentional and unintentional misuse.

"7. For each data-handling system, a fixed period should be set beyond which the data may no longer be kept or used.

"8. The data must be legitimate, accurate and still valid. Provision should be made for the greatest possible care in correcting erroneous data and keeping data up to date.

"9. States should take the necessary steps to prevent any infringement of the principles set out above." 371/

---

*/ For the purposes of the work of the Committee concerning the problem of electronic data banks in the private sector, "electronic data banks" shall be taken to mean any electronic data processing system designed for personal data management which is capable of distributing such data.

371/ Council of Europe, Exp/Prot. Priv./EDB (72) Misc. 5.

B. Points for possible inclusion in draft international standards for the protection of the rights of the individual against threats arising from the use of computerized personal data systems

320. In the light of the existing and proposed safeguards dealt with this present report, it is suggested that the following points be taken into account in the drafting of international standards relating to the protection of the rights of the individual against threats arising from the use of computerized personal data systems:

(i) The States which have not yet done so should adopt appropriate legislation containing rules relating to computerized personal data systems in both the public and the private sectors. As far as possible, legislation should be adopted concerning all types of computerized personal data systems (statistical and research systems, administrative systems and intelligence systems), but may vary according to the nature of those types of systems.

(ii) The following minimum standards should be followed in drawing up national legislation:

(a) only the personal information strictly necessary for the purposes of the respective system should be collected;

(b) the individual should be notified that information is being gathered about him and his agreement should be obtained before the information is stored: provided that information may be gathered without such knowledge and agreement in areas related to national security, law enforcement and criminal justice, and in other areas for which the law has established that such knowledge and agreement are not required due to the purpose of the gathering of information, subject to appropriate safeguards for human rights which should include those suggested in points 3 (a) (i) and (iii) and 3 (b) appearing in paragraph 177 of document E/CN.4/1116. 372/

372/ These read as follows:

3. States shall, in particular, take the following minimum steps:

(a) Penal Codes should designate as offences and provide for penalties of fine, imprisonment or both, for:

(i) the clandestine monitoring or recording of conversations except, possibly, by participants to the conversations, and except by judicial or ministerial order, and in accordance with that order, in countries which permit monitoring or recording in criminal investigation or for reasons of national security;

372/ (continued)

...

(iii) the clandestine viewing, photographing, filming or televising of members of households and their guests in their dwellings, except by judicial or ministerial order, and in accordance with that order, in countries which permit such actions in criminal investigations or for reasons of national security;

(b) States which permit the utilization by their own agencies of modern recording and other techniques in the investigation of crimes or for reasons of national security shall make provision to restrict the use of these techniques to cases of the most serious crimes or the most serious threats to national security. They shall lay down by law the conditions for their use, which conditions shall include:

(i) prior authorization in each case by a judicial authority (or by an official of Ministerial rank), upon a showing of "probable cause" or its equivalent and a showing that alternative methods of surveillance are not available or not effective in the particular case;

(ii) specification, in the authorization, of the person to be monitored, the suspected offence, the person who is to do the monitoring, and the length of the period of surveillance. States shall make provision to ensure that such authorizations are not issued in a routine manner or by delegation of authority;

(iii) specification of the extent to which use may be made in criminal proceedings of information gained;

(c) the collection and storage of hearsay and other subjective material should be avoided;

(d) data concerning political and religious views, race and ethnic origin and intimate life should not be collected and stored, except under conditions explicitly provided by the law;

(e) all necessary measures, including technical procedures, should be taken to maintain the accuracy, completeness and pertinence of the stored information, and to remove or update obsolete information;

(f) legal responsibility should rest upon computer manufacturers and/or software developers, who with knowledge or through gross negligence fail to install basic safeguards for confidentiality and security of information;

(g) the individual should have the right, through special procedures laid down by the law, to receive a copy, intelligible to him, of stored information relating to him, to challenge it, to add explanations to it, and to obtain the correction or removal of inaccurate, obsolete or unverifiable data about him;

372/ (*continued*)

(h) the stored information should be disclosed or otherwise used only for the purposes for which it has been collected and disclosed only to legally authorized authorities or persons;

(i) all necessary measures, including technical procedures, to protect the confidentiality of the data and prevent their unauthorized disclosure and dissemination should be taken;

(j) any damage suffered by the individual in his rights, by the misuse of computerized data concerning him, should be compensated;

(k) violations of laws aiming at protecting the rights of the person to whom the stored information relates should be made punishable;

(l) the legality of decisions about individuals based on computerized personal data systems and their judicial control should be ensured.

(iii) The use as evidence of information stored in computerized systems should be regulated by special legislation.

(iv) Rules should protect the rights of the person whenever information about him is stored in computerized systems operating in countries other than his own.

(v) The establishment of a supervisory body in the field of operation of computerized personal data systems should be considered. Its functions might include:

(a) registering existing computerized personal data systems;

(b) supervising the observance of existing laws protecting human rights against the abuse of such systems;

(c) following developments in the field affecting human rights and drawing the attention of the legislature, the executive and the public to the effects of such developments upon human rights and to possible further required safeguards.

(vi) The establishment of professional associations for computer personnel should be promoted and such associations should be encouraged to adopt codes of ethics which should contain minimum rules aiming at regulating the professional conduct of such personnel in such a manner as to prevent infringements of human rights.

(vii) Professional associations for computer personnel might be given some jurisdiction over the professional education and the selection of such personnel and the power to apply disciplinary measures for non-compliance with the code of ethics mentioned above.
