UNITED NATIONS

ECONOMIC AND SOCIAL COUNCIL

Distr.
GENERAL

E/CN.4/Sub.2/1983/18
30 June 1983

ENGLISH
Original: FRENCH

COMMISSION ON HUMAN RIGHTS
Sub-Commission on Prevention of Discrimination and Protection of Minorities
Thirty-sixth session
Item 10 of the provisional agenda

Study of the relevant guidelines in the field of computerized personnel files

Final report prepared by Mr. Louis Joinet

GE.83-12398

TABLE OF CONTENTS

	Paragraphs	Page
Introduction	1 - 24	1
PART I		
The human rights affected by the computerization of personal data		
Chapter		
I. The right to protection of privacy	29 - 35	7
II. The use made of personal data files and the promotion of human rights	26 - 39	8
A. The right to use files as a condition for the exercise of certain collective rights	36 - 37	8
B. Computerized personnel files used by organizations specializing in the protection of human rights	38 - 39	9
PART II		
Review of measures taken by international organizations and regional agencies for States and their implementation in domestic legislation		
Chapter		
I. Measures taken at the international and regional levels	40 - 69	10
A. The first measures were taken by Western countries	40 - 47	10
B. Minimum protective rules embodied in the OECD recommendation and the Convention of the Council of Europe	48	11
C. Comparative analysis of these two instruments	49 - 62	11
1. Different backgrounds	50 - 55	11
2. Differences in scope	56 - 58	12
3. Differences in substantive provisions	59 - 62	13
D. Position of the developing or industrializing countries	63 - 69	13

TABLE OF CONTENTS (cont'd)

		Paragraphs	Page
II.	The establishment of minimum standards in national legislation	70-115	14
	A. Possible options in defining the scope of regulations	72- 84	15
	1. Should legislation cover public and private sector files, or the files of only one sector, and if so which sector?	73- 75	15
	2. Should files containing personal data on legal entities be protected?	76- 81	15
	3. Should legislation be extended to cover non-computerized files?	82- 84	16
	B. Possible options with respect to minimum desirable standards in national legislation	85-100	17
	1. Minimum standards generally admitted in national legislation	86- 99	17
	2. Extension of minimum standards by certain legislations	100	18
	C. Foreseeable exceptions	101-112	19
	1. Security files (police, defence, national security and intelligence service files)	102	19
	2. Medical files	103	19
	3. Files of political, trade-union, religious or philosophical organizations	104	19
	4. Files of press agencies and enterprises	105	19
	5. Files of statistical and research agencies	106	19
	D. The special case of transborder files	113-115	20
	PART III		
	Specific problems posed by the use of computerized personnel files by international, intergovernmental, regional and other organizations		
I.	Proposals	135-152	23
	A. The promotion of human rights in domestic law	135-148	23
	B. The files of international organizations and agencies	149-152	24
II.	Conclusion	153-154	25

INTRODUCTION

1. At its thirty-third session, the Sub-Commission on Prevention of Discrimination and Protection of Minorities expressed concern about the uses of data processing which might affect the rights of the person. 1/

2. The Sub-Commission emphasized that the increasingly frequent use of computerized personnel files entailed grave risks of interference with privacy and the exercise of freedoms, as had been pointed out in studies conducted in many countries. Since as a result of the increasingly widespread use of data processing virtually all regions of the world are now affected by this development, albeit to varying extents, the time has come to respond to it by means of appropriate action.

3. By resolution 12 (XXXIII) of 11 September 1980, the Sub-Commission accordingly requested that a study should be made of the relevant guidelines to be adopted in this field and a report submitted to it. The present study constitutes a response to that request.

Previous action relating to the effects of the use of computerized files containing personal data

4. Of the numerous resolutions and studies in this field emanating from the United Nations, reference will be made primarily to the following.

5. By resolution 2450 (XXIII) of 19 December 1968 the General Assembly, for the first time, specifically took up the problems arising in connection with human rights from the development of science and technology, in particular (see paragraph 1(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".

6. The General Assembly requested the Secretary-General to prepare, for submission to the Commission on Human Rights, a preliminary report comprising in particular a summary account of studies already made or in progress.

7. At its twenty-seventh session, the Commission examined this preliminary report (E/CN.4/1028 and Add.1-6) and on 18 March 1971 adopted resolution 10 (XXVII), in which it recognized the need to concentrate its attention in particular on "prevention of the use of scientific and technological achievements to restrict fundamental democratic rights and freedoms". The Commission accordingly requested the Secretary-General to continue his study in co-operation with Governments, the specialized agencies and non-governmental organizations and to submit to it one or more reports "which could be used as a basis for exploring the possibility of preparing international instruments designed to strengthen the protection of human rights".

8. Among these reports reference may be made to the following:

The report of 23 January 1973, prepared pursuant to paragraph 1(a) of the above-mentioned resolution 2450 (XXIII), relating to "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 and Corr.1, Add.1-3 and Add.3/Corr.1); and in particular

---

1/ See agenda item 9: "Human rights and scientific and technical developments" (E/CN.4/1413, E/CN.4/Sub.2/459, paras. 253 and 254).

The report requested in paragraph 1(c) of the above resolution and dated 31 January 1974, entitled "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" (E/CN.4/1142 and Corr.1, and Add.1 and 2), the first part of which is more particularly concerned with "computerized personal data systems".

9. General Assembly resolutions 3268 (XXIX) of 10 December 1974 and 3384 (XXX) of 10 November 1975, and resolutions 2(XXX) of 12 February 1974 and 11(XXXI) of 5 March 1975 of the Commission on Human Rights again emphasized the need for appropriate measures to be taken in this field.

10. By its decision of 10 November 1975, the General Assembly (at its thirtieth session), referring to the above-mentioned resolution 3268 (XXIX), decided to include in the provisional agenda for its thirty-fifth session the question of "Human rights and scientific and technological developments", and to consider it as a priority item. 2/

11. On 5 March 1976, the Commission on Human Rights adopted resolution 11 (XXXII), in which it expressed regret that it had been unable to make a thorough examination of the question of human rights and scientific and technological developments, and decided to include the item, on a priority basis, in the agenda for its thirty-third session.

12. Referring to General Assembly resolution 3384 (XXX) entitled "Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind", the Commission on Human Rights adopted at its thirty-third session resolution 10 B (XXXIII) on 11 March 1977. With the aim of encouraging Member States to take measures giving effect to the provisions and principles enunciated in the Declaration, the Commission invited the Sub-Commission to report to it on the question in the light of studies already carried out.

13. By its resolution 12 (XXXIII) adopted on 11 September 1980, the Sub-Commission on Prevention of Discrimination and Protection of Minorities noted that one of the consequences of the use of computers was the increasingly frequent recourse to computerized personal files that the concentration of personal particulars in such files entailed grave risks of interference with the privacy of individuals and the exercise of their freedoms, and that, apart from States, international, intergovernmental and regional organizations were keeping an increasing number of computerized personal files. It requested the Chairman of the Sub-Commission to designate one of its members to undertake a study of the relevant guidelines in this area and requested the member so designated to submit his study and proposals to the Sub-Commission at its thirty-fourth session. The Chairman of the Sub-Commission designated Mrs. Questiaux for this task, on the understanding that it would be carried out by Mr. Joinet, her alternate. Mr. Joinet, who has in the meantime replaced Mrs. Nicole Questiaux as a member of the Sub-Commission, submitted an interim report in 1981. The present final report has also been prepared by Mr. Joinet.

2/ General Assembly, Official records: thirtieth session, Supplement No.34 (A/10034), P.100, item 69.

Previous action relating to the formulation of international standards

14. It will be recalled that in resolution 3268 (XXIX), paragraph 5, the General Assembly requested the Commission to draw up a programme of work with a view to undertaking, in particular, the formulation of standards in the areas which would appear to be sufficiently analysed.

15. In the preamble to resolution 2450 (XXIII), the General Assembly had declared that the studies envisaged on human rights and scientific and technological developments should serve as a basis for "drawing up appropriate standards to protect human rights and fundamental freedoms".

16. By resolution 10 (XXVII), the Commission requested the Secretary-General "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 human rights". The Commission renewed its proposal in resolution 2 (XXX), requesting information "in order to enable it to consider possible guidelines on standards which could be included in appropriate international instruments".

17. Lastly it will be recalled that in documents E/CN.4/1142, paragraph 320, and E/CN.4/1142/Corr.1 a number of principles relating in particular to "the protection of the rights of the individual against threats arising from the use of computerized personal data systems", were suggested for inclusion in a possible international instrument.

Sources

18. In addition to the above-mentioned documents, the following have also been taken into consideration:

(a) International and regional human rights instruments, in particular:

Article 12 of the Universal Declaration of Human Rights:

"No one shall be subjected to arbitrary interference with his privacy ... nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks";

Article 17 of the International Covenant on Civil and Political Rights, which has similar wording;

Article 11 of the American Convention on Human Rights:

"1. Everyone has the right to have his honour respected and his dignity recognized.

"2. No one may be the object of arbitrary or abusive interference with his private life ... or of unlawful attacks on his honour or reputation.

"3. Everyone has the right to the protection of the law against such interference or attacks";

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms:

"1. Everyone has the right to respect for his private ... life ...

"2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

(b) Relevant regional or intergovernmental instruments and resolutions relating to the protection of privacy in the light of the development of computerized personal data files

The final resolution of the Intergovernmental Conference on Strategies and Policies for Informatics, organized by UNESCO together with IBI 3/ in Torremolinos (Spain) in 1978. The relevant passages of the resolution read as follows:

"The Conference, ... concerned by the fact that the introduction of data-processing into a society may, in addition to its desired primary effects, also have negative secondary effects,

"Invites Governments to recognize the right of all persons to have access to recorded personal data about themselves and to have the possibility of having errors rectified ...".

The OECD recommendation concerning the guidelines for the protection of privacy and transborder flows of personal data of 23 September 1980;

Council of Europe resolutions (73) 22 of 26 September 1973 on data banks in the private sector and (74) 29 of 20 September 1974 on data banks in the public sector, which set out minimum guidelines for adoption by member States in their national legislation to ensure the privacy of individuals;

The Convention of the Council of Europe of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which, it should be pointed out, is the first binding international instrument in this field;

The resolution adopted by the Parliamentary Assembly of the Council of Europe on 28 January 1981;

The resolution adopted by the European Parliament on 9 March 1982 on the protection of the rights of the individual in the face of technical developments in data processing, which, in the form of a recommendation, brings to the attention of the Commission and Council of Ministers of the European Communities a list of the legal standards which should be taken into consideration by member States.

3/ The Intergovernmental Bureau for Informatics (IBI) consists mainly of developing or industrializing countries.

Various documents and proceedings of regional, intergovernmental, non-governmental or private organizations with competence in this sphere, namely:

Proceedings of the conference on the integration of African informatics held in Abidjan (Ivory Coast) from 22 to 30 November 1979;

Proceedings of the conference of Latin American informatics authorities held in Buenos Aires in 1979;

Proceedings of the first world conference on transborder data flow policies organized by IBI in Rome in June 1980;

Work of the specialized committee of the Nordic Council responsible for encouraging the harmonization among member States of legislation on informatics and freedoms;

Six studies by EEC dealing directly with the issues covered by this report:

(1) Qualitative and quantitative aspects of transborder data flows;

(2) Organization and methods of work of data protection authorities;

(3) Problems involved in distinguishing between data banks on natural persons and data banks on legal persons;

(4) International economic aspects of data protection;

(5) Technical aspects of the right of access;

(6) Inspection methods and data protection.

Report drawn up on behalf of the Legal Affairs Committee of the European Parliament on the protection of the rights of the individual in the face of technical developments in data processing;

Council of Europe: Summary of legislation of member States - 1973 (4.73.11); comparative study of methods concerning the protection of the privacy of individuals in relation to electronic data banks - 1975; Report prepared by M. Maisl, consulting expert, on the deontology of data-processing experts;

Recommendation No. R (81) 1 on Automated Medical Data Banks;

Proceedings of the tenth Colloquy on European Law, held in Liège in September 1980 by the Council of Europe, on the use of personal data for research purposes;

Proceedings of the OECD Symposium on Transborder Data Flows and the Protection of Privacy of Individuals, held in Vienna in September 1977;

The guiding principles adopted at Bellagio by the conference on privacy, confidentiality and the use of microdata of public administrations for statistical and research purposes;

The declaration on the protection of privacy and the use of personal data for research purposes adopted by the European Science Foundation; 4/

Comparative study of the International Commission of Jurists on the legal protection of privacy (1972) prepared for UNESCO;

Draft protocol No. 6 to the European Convention on Human Rights for the protection of privacy against the utilization and dangers of informatics and data banks, adopted by the International Association of Lawyers by its resolution of 14 September 1979;

Draft recommendation on the protection of personal data used for purposes of scientific research and statistics.

Scope of the study

19. The Rapporteur's mandate under Sub-Commission resolution 12 (XXXIII) is confined to "a study of the relevant guidelines in this area". This wording calls for two comments.

20. It is in line with the most recent resolutions of both the General Assembly and the Commission on Human Rights, which have called for the drafting of guidelines in areas where sufficient documentation and studies exist to be taken into consideration, where appropriate, in international instruments.

21. The preceding remarks indicate that these conditions are largely met in the area of safeguarding the rights of individuals in the light of the development of computerized personal data files.

22. We shall therefore deal only briefly with the general analyses, and instead concentrate solely on highlighting recent steps and developments in this area.

23. Sub-Commission resolution 12 (XXXIII) specifies that the proposals should concern not only measures to be taken by States in their national legislation, but also rules for inclusion in the statutes of the international organizations of all kinds which are keeping an increasing number of computerized personal files for their own purposes.

24. In view of the specific problems raised by this second aspect of the Rapporteur's terms of reference, it will be the subject of a chapter in its own right. The study will therefore deal successively with:

The human rights affected by technical developments in the field of informatics;

A review of international co-operative measures taken for the benefit of States, and their implementation in domestic legislation;

The specific problems posed by the use of computerized personnel files by international, intergovernmental, regional and other organizations.

4/ The European Science Foundation is an organization in consultative status with the Council of Europe and comprises most European public research bodies.

Part I

THE HUMAN RIGHTS AFFECTED BY THE COMPUTERIZATION OF PERSONAL DATA

25. The following remarks could apply both to computerized personal data files and to purely manual filing systems. The fact that a Government records in any form whatsoever information on the political opinions of citizens, for example, creates a hypothetical risk of discrimination in the use that will be made of such information. Computerization merely increases this risk.

26. On the other hand, there are some rights whose exercise may be greatly facilitated by the use of data processing (right to vote, for example).

27. It would therefore be inappropriate to maintain that only computerized files are dangerous to privacy, or that data processing systematically threatens to narrow the enjoyment of freedoms.

28. In other words, while the use of manual (or a fortiori computerized) personal data files entails an obvious risk of violation of the privacy of individuals, there are cases where, on the contrary, the use of such files makes it possible to promote the effective enjoyment of certain human rights.

I. THE RIGHT TO PROTECTION OF PRIVACY

29. It would be pointless to insist on the need for a precise legal definition of the right to privacy as a precondition for drafting guidelines. While possible in sociology, 5/ where there is an abundant literature on the subject, a definition of this kind has apparently never been unanimously accepted by jurists.

30. Thus, the comparative legal study of the International Commission of Jurists 6/ points out that the legislation reviewed does not, strictly speaking, contain any legal definition of the right to protection of privacy.

31. In an OECD report of 1974, Professor Rodota stressed that, viewed in the historical context of its origins, the concept of privacy cannot be considered the expression of a need felt in the same way by the entire community.

32. He goes on to say that initially it is less a natural need felt by all individuals than a privilege acquired by a class. With the gradual politicization of society in all areas, however, this need for privacy ceases to be aristocratic and spreads throughout society. This change in motivation leads to a change in the content of the concept of privacy: respect for individual privacy is relegated to the background, in the cause of the exercise of public or private, political, economic or social collective freedoms.

33. This evolution is thought to explain why public opinion reacts more strongly, for example, to plans to introduce a national identification number, a national

---

5/ See A. Westin, Privacy and Freedom, New York, 1967.

6/ UNESCO, 1972, Report of the International Commission of Jurists, "The protection of privacy: a comparative study of 10 countries".

population register, links between police files and social surveillance files, census operations, etc., than to straightforward violation of personal privacy.

34. It is argued that respect for privacy to a great extent guarantees the power to exercise certain fundamental rights, particularly during periods when certain rights are being called in question, be it the right to one's own identity as a human being (right to deviate, to disagree, to non-discrimination on grounds of sexual proclivities), or the freedom to exercise in private the right of assembly or opinion, as well as their corollaries: inviolability of the home, mail, telephone conversations, and so forth.

35. In this connection, it is significant that the expression "data processing and privacy" in use during the 1960s has gradually been abandoned in favour of the expression "data processing and freedoms".

II. THE USE MADE OF PERSONAL DATA FILES AND THE PROMOTION OF HUMAN RIGHTS

A. The right to use files as a condition for the exercise of certain collective rights

36. In all regulations account should be taken of the fact that the establishment of personal data files may in some cases amount to a fundamental right on which the possibility of effectively exercising certain collective rights is predicated. Unless this is done, binding regulations, regardless of the good intentions underlying them, may become a cure worse than the disease.

37. The following are examples of such collective rights:

(a) Right of association,[7] in a broad sense

To deprive political parties, trade unions, churches and groups of like-minded persons of the possibility of keeping a register of their members would in fact be tantamount to preventing them from carrying out their activities and from performing their function. Likewise, any control by the authorities over their files would obviously involve a serious risk of violation of the right of association.

(b) Freedom of expression,[8] and in particular freedom of information

As is well known, in its most up-to-date version the principle of the free flow of information rests on three fundamental criteria: freedom to seek, disseminate and receive information and opinions. At the international level, the aim is to ensure the freest possible flow of information in the name of human rights, as referred to in the Helsinki agreements, with the aim of avoiding hatred among peoples. For this free flow to have real meaning, the developing countries have

---

7/ Universal Declaration of Human Rights (UDHR), art. 20; International Covenant on Civil and Political Rights (ICCPR), art. 22; American Convention on Human Rights (ACHR), art. 16; European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), art. 11.

8/ UDHR, art. 19; CCPR, art. 19; ACHR, art. 13; ECHR, art. 10.

furthermore stressed, during the work carried out within UNESCO "for a new international information order", that the flow of information must be not only free but "balanced". In setting forth guidelines, one must therefore take account of this new approach, and avoid any constraint likely to restrict the freedom to disseminate information. This concerns in particular subscription lists, newspaper data and documentation banks, and remote publishing processes.

(c) The right to participate in the management of public affairs

The exercise of this right presupposes the possibility of taking part in elections, the holding (and regularity) of which calls for the keeping of electoral rolls. The latter are also a condition for the exercise of many economic and social rights, particularly as regards professional, trade-union and association elections, and so forth.

B. Computerized personal data files used by organizations specializing in the protection of human rights

38. These uses are of too recent date to enable any incontrovertible conclusions to be drawn from them.

39. Certain lessons may already be drawn from these developments. 9/ Provided specific protective measures are taken, they are of great interest in the following areas:

In obtaining up-to-date statistical data on certain forms of violation of human rights and assessing cases in which such violations are large-scale and systematic;

In ensuring better evaluation of the grounds of allegations concerning individual cases of violation; automatic processing of the data collected makes it easier to detect errors, people with the same name, cases already resolved, etc.;

In enhancing the effectiveness of measures to be taken in cases requiring "urgent action", by keeping files more up to date;

In resolving more efficiently certain administrative problems during the introduction and implementation of action programmes in support of refugees or displaced persons.

9/ See below, part III, paras. 116 et seq.

Part II

REVIEW OF MEASURES TAKEN BY INTERNATIONAL ORGANIZATIONS AND REGIONAL AGENCIES FOR STATES AND THEIR IMPLEMENTATION IN DOMESTIC LEGISLATION

I. MEASURES TAKEN AT THE INTERNATIONAL AND REGIONAL LEVELS

A. The first measures were taken by Western countries

40. The Nordic Council, a regional organization comprising the Scandinavian countries, played a vanguard role. As early as 1966, its council of ministers set up a special committee to promote the harmonization of legislation on data processing and freedoms in member States. With time, this committee has become an effective organ for co-operation among the national bodies responsible for the supervision of data files.

41. The European Economic Community (EEC) and the European Parliament have carried out studies or adopted resolutions aimed at helping member States to establish policies in this area.

42. The Council of Europe and its Consultative Assembly, followed by the Organisation for Economic Co-operation and Development (OECD), have played a predominant role in formulating rules in this area.

43. As far back as 1972, these two organizations envisaged the drafting of standard legislation which would ensure that individuals received strictly equivalent protection from one country to another. However, because of the appreciable differences which exist between the legal systems of member countries, it would have taken too long to bring about total reciprocity.

44. This idea was therefore replaced by a more limited project aimed at encouraging member States to harmonize their legislation, a move which would be supplemented by the introduction of regulations on the exchange of personal data between countries (transborder data flows), in order to make up for the margin of non-reciprocity which might continue to exist between States despite the efforts made to harmonize their legislation.

45. Two factors rarely found in comparative law facilitated a convergence of this kind:

Firstly, there was virtually no existing domestic legislation: consequently the legal differences which hinder the harmonization of existing legislation were not an obstacle in this particular case;

Secondly, taking advantage of this "legal limbo", the Council of Europe and OECD proposed for adoption by member States - in the form of resolutions, recommendations and even a convention - minimum rules, commonly known as the "hard core", which Governments should take into account in the rules they were drafting.

46. In the case of the Council of Europe, in addition to resolutions (73) 22 on private-sector files and (74) 29 on the public-sector files, special mention should be made of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the Committee of Ministers on 28 January 1981.

47. The OECD Council of Ministers adopted on 23 September 1980 a recommendation concerning guidelines on the protection of privacy and transborder flows of personal data.

B. Minimum protective rules embodied in the OECD recommendation and the Convention of the Council of Europe

48. These two texts have many points in common, in the form of minimum rules, which the parties undertake to respect in their domestic legislation, namely:

(a) Principle of fairness: information should not be collected or processed by unfair or unlawful means, such as wire-tapping which is not duly authorized;

(b) Principle of accuracy: those responsible for data files have an obligation to check the accuracy of the data recorded and to ensure that they are kept up to date;

(c) Principle of purpose specification: the purpose which justifies the creation of a file should be specified and known before it is set up, so that at any time it will be possible to check whether:

The data collected and recorded are in keeping with the purpose sought (principle of relevance);

The data are not used for a purpose other than that for which the file was set up (principle of non-misuse);

The data are stored for no longer than is normally required for the purpose for which they were collected (principle of the right to oblivion), unless the data are rendered anonymous;

(d) Principle of openness: a public record of computerized personal data files should be kept;

(e) Principle of individual access: everyone, whatever his nationality or place of residence, should have the right to know whether information concerning him has been computerized and, if so, to obtain a copy of it; the person having the right of access should be able to secure the rectification or erasure of data in the event of error, inaccuracy or unlawful recording;

(f) Principle of security: appropriate measures should be taken to ensure the physical security of files and security of access to them.

C. Comparative analysis of these two instruments

49. Despite their great similarity with regard to substantive rules, the differences between the two texts, as regards their background, scope and content amount to something more than shades of meaning.

1. Different backgrounds

50. The work of the OECD experts stemmed primarily from a desire to ensure that the new regulations relating to data processing and freedoms did not adversely affect transborder data flows as a whole, whether of personal data or not.

51. This concern to avoid hindrances in the form of legal obstacles is repeatedly stated in the preamble to the recommendation, in which it is recognized that transborder flows of personal data contribute to economic and social development, and that domestic rights with regard to the protection of privacy and transborder flows of personal data are liable to hinder those flows. Furthermore, the authors express their determination to encourage the free flow of information among member countries and to avoid the creation of unwarranted obstacles to the development of economic and social relations among those countries.

52. It was certainly fitting for OECD, an organization of developed countries with a primarily economic focus, to encourage this approach aimed at the free flow of information, while by no means neglecting the "human rights" aspect.

53. The Convention of the Council of Europe, on the other hand, is chiefly directed towards the protection of human rights. Right away in the preamble, the principle of "respect for ... human rights and fundamental freedoms" is affirmed before any other, and it is stressed that the purpose of the Convention is to extend the safeguards for everyone's rights and fundamental freedoms to respect for privacy, as provided for in article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

54. After the reaffirmation of the Council's commitment to freedom of information regardless of frontiers, in accordance with the spirit of article 10 of the European Convention at the very end of the preamble reference is made to the need to reconcile that approach with the principle of the free flow of information as affirmed in the OECD text.

55. In fact, from the same concept of the "free flow of information", OECD and the Council of Europe have followed different paths:

For the Couhcil, the main point is the "free flow of ideas and opinions", in other words, freedom of expression as recognized in international human rights theory;

For OECD, the main point is freedom of exchange of information and data because of their economic value; in other words, the application to a specific field of the principle of freedom of international trade.

2. Differences in scope

56. Both texts apply, as a minimum requirement, to the files of natural persons in the public and private sectors.

57. Beyond that minimum, one notes:

That the OECD recommendation applies without exception to manual files and in principle excludes consideration of the files of legal persons;

That the European Convention, on the other hand, provides for the possibility, for those contracting parties which wish to do so, of extending the Convention's scope to all or certain categories of files, either for example, by exercising the option of extending it to manual files or to the files of legal persons, or as laid down in the text, or by declaring as an exception at the time of ratification that the Convention will apply for example, only to those categories of files at present regulated by law (credit files, personnel files, customer files, etc.).

58. In other words, through the exercise of the options of extension and total or partial exclusion, the scope of the Convention of the Council of Europe is wider than that of the OECD recommendation, subject to the proviso that a contracting party may avail itself of these extensions to impose restrictions on another contracting party only in so far as it has itself put them into effect.

3. Differences in substantive provisions

59. The Council Convention above prohibits, unless appropriate safeguards are established, the processing of racial, political or religious data, data relating to health and sex life, and data concerning criminal convictions.

60. It has become apparent that in the case of intrinsically sensitive data, additional safeguards must be provided.

61. Such conditional prohibition is not, explicitly at least, embodied in the OECD text. The only provision made is the option whereby a member country may restrict flows of certain categories of personal data which are subject in its domestic law to specific regulations.

62. This summarizes the measures taken by the Western countries.

D. Position of the developing or industrializing countries

63. Until recently, these measures were viewed with some misgivings by the developing countries, which were quite legitimately concerned about the implementation of such regulations for the protection of human rights in the light of technological developments without direct consideration of the question of reducing the phenomena of technological dependence phenomena, which are themselves factors that impair human rights.

64. This attitude has eased considerably since 1977. The reasons are threefold:

The steady advance of data processing - albeit in varying degrees - in nearly all States Members of the United Nations, especially in public administrations and in private enterprises such as travel agencies and banks;

The progress in the North-South dialogue on the right to development as a human right and the work done within UNESCO in the cause of a new international information order;

The dialogue between developing and developed countries made possible by the joint initiatives of UNESCO and the Intergovernmental Bureau for Informatics (IBI).

65. The Intergovernmental Conference on Strategies and Policies for Informatics held at Torremolinos (Spain) in 1978 by these two organizations is evidence - as far as we know the first - of the awakening of this new sensitivity, the organizations being composed chiefly of developing or industrializing countries. In this connection, reference may be made to a few significant extracts from the final resolution:

"Conscious of the importance of informatics in the development of all countries ...;

"Concerned by the fact that the introduction of data-processing into a society may, in addition to its desired primary effects, also have negative secondary effects;

"The Conference invites Governments to recognize the right of all persons to have access to recorded personal data about themselves and to have the possibility of having errors rectified ...".

66. This new sensitivity is also apparent in Africa and Latin America.

67. At the Conference on the Integration of African Informatics, held in Abidjan (Ivory Coast) in 1979, some delegations suggested that an inter-State body should be set up within the Organization of African Unity to assist States in defining policy, inter alia by taking into account the problems of security and confidentiality of data.

68. At the World Conference on Transborder Data Flow Policies, organized in Rome in 1980 by IBI, an African delegate made the following statement:

"The creation of information networks can affect the lives and rights of individuals in third-world States ... . It is in countries still hesitating over the adoption of a democratic system that the accumulation of data on individuals will have an undoubted impact on the political orientation of the country concerned. Accumulated data concerning a certain individual can be used for political purposes, to the detriment of that individual. Collating extracts from various statements by an individual reveals his political opinions, which may give rise to positive or negative reactions on the part of those in authority. They can be used to force an individual to adopt a favourable attitude to a particular political regime".

69. The Latin American continent was also represented, inter alia through statements by experts from Brazil and Argentina, in the discussion at the IBI Conference in Rome. Elaborating on the ideas put forward at the Latin American Conference on Informatics held in Buenos Aires in 1979, the two delegates stressed the need for the Latin American countries to concern themselves with safeguards for the rights of individuals in that field, including international exchanges of personal data. The idea of a Latin American regional approach to these matters was mentioned.

II. THE ESTABLISHMENT OF MINIMUM STANDARDS IN NATIONAL LEGISLATION

70. Countries may be divided into three categories, according to the degree of advancement of their legislation:

Countries where legislation is already in force: Sweden (1973), United States of America (1974), Federal Republic of Germany (1977), France (1978), Denmark (1978), Norway (1978), Austria (1978), Luxembourg (1979), Hungary (1981), Iceland (1982), Israel (1982), Australia (1982).

Countries where draft legislation is at a more or less advanced state: Belgium, Canada, Finland, Italy, Netherlands, Portugal, United Kingdom, Switzerland.

Countries where preparatory work is in progress: Spain, Greece, Japan, New Zealand.

71. With the aim of assisting jurists and political leaders wishing to promulgate protective legislation, we have placed methodological aspects in the forefront in analysing the many reports, studies, laws and bills to which reference has been made, in order to bring out the basic options facing any country wishing to legislate in this field.

A. Possible options in defining the scope of regulations

72. Should account be taken of the differences in status between:

Files in the private sector and files in the public sector;

Files containing information on natural persons and those containing information on legal persons;

Computerized files and manual files?

1. Should legislation cover public and private sector files, or the files of only one sector, and if so which sector?

73. Most legislation has provided for regulation of both the public and private sectors, establishing separate rules and procedures tailored to each sector.

74. In France, for example, public files are subject to prior authorization, while only a prior declaration is required for private files. Conversely, in Sweden, private files are subject to prior authorization while public files are governed by less constrictive rules.

75. These differences, however, concern only the procedural regulations. The substantive regulations applicable to the two sectors are generally identical, as in the case, for example, of the obligation to rectify incorrect data, erase out-of-date information, recognize the right of access of the person to whom the information relates, etc. It is difficult to see how the obligation to rectify erroneous data could be imposed only on one sector and not the other.

2. Should files containing personal data on legal entities be protected?

76. It has sometimes been maintained that, since legal persons have no private existence, such protection is pointless. One notes, for example, that in most legal systems case-law admits the concept of "business secrecy", which is linked with the concept of confidentiality.

77. Exclusion of the files of legal persons involves the risk of discrimination.

78. The vast majority of legal persons are small or medium-sized enterprises. It is generally large enterprises and banking establishments which keep files on small-scale enterprises (credit files, customer files, etc.) and therefore look askance at any legislation that would give small enterprises the right of access to such files. Since the interests to be protected are not the same in the two cases, the realk question is to determine which type of enterprise is most deserving of protection. We consider it our duty to pronounce in favour of the small and medium-sized enterprises, and consequently in favour of an extension of the law to the files of legal persons, as provided for in Danish, Austrian and Luxembourg law.

79. A further danger of discrimination should be emphasized. Craftsmen and small shopkeepers often pursue their activities as natural persons, but it also frequently happens that, for tax reasons in particular, they choose the status of legal person. In the former case, the shopkeeper as a natural person will enjoy the right of access to information concerning himself, while another shopkeeper pursuing an identical activity and having a similar clientele and turnover will not enjoy the same protection.

80. Lastly, a file on legal persons may contain information, sometimes of an intimate nature, on certain executives or directors. This applies particularly to credit files. It is outrageous to refuse persons in this category access to such highly personal information on the pretext that the file relates to legal persons, and thus to deprive them of the opportunity of rectifying tendentious or incorrect information which might do them serious harm.

81. For these various reasons, we consider that files on legal persons should also be protected. At the very least a compromise might be proposed on the following lines: recognition of the individual right of access to files on legal persons when the information recorded is used for the purpose of taking a decision detrimental to the person concerned, as in the case of refusal of credit or insurance. It should be emphasized, however, that this question does not appear to fall directly within the Sub-Commission's competence.

3. Should legislation be extended to cover manual files?

82. Such an extension is desirable as an ideal since certain manual files sometimes entail more serious risks than computerized files, but it poses formidable practical problems. Firstly, it is physically impossible to subject all manual files to control procedures. Secondly, the keeping of certain files is in itself an essential feature of the exercise of certain freedoms, as in the case of personal address books.

83. In the interests of balance and flexibility, it is suggested that:

Procedural regulations applicable to computerized files should not apply systematically to manual files;

Substantive regulations, such as those prohibiting the recording of discriminatory information, individual right of access, etc. should apply to both categories of file;

Computerized files should be assimilated to manual files;

Procedural regulations might exceptionally apply to certain categories of manual file of a particularly sensitive nature.

84. To conclude on consideration of this question, we would note that most recent trends are towards the broadest possible protection, with some reservations as to files relating to legal persons; a point is made to provide some flexibility in order to allow for the adaptations required by the diversity of situations.

B. Possible options with respect to minimum desirable standards in national legislation

85. Successive consideration will be given to the content of the minimum standards common to existing legislation, the possibilities of extending this "hard core" to include certain additional standards, the derogations provided for in respect of certain specific categories of file in the areas of public security, medicine, exercise of the right of association, the press and scientific research, and the problems posed by the transborder circulation of personnel files.

1. Minimum standards generally admitted in national legislation

86. On this point, except for a few slight differences, there is a perfect concordance between the minimum standards provided for in the international instruments analysed in paragraph 48 and the basic standards common to national laws.

87. We shall not revert to the principles of fairness (in data collection), accuracy (which implies an obligation to keep information up to date), or purpose specification, i.e. whether the information collected is adequate (principle of relevance), is not misused (principle of non-misuse) and is not kept for an excessive period (principle of the right to oblivion). Similarly, the principle of the physical security of data and security of access to them calls for no special comment.

88. We will focus, in particular, on the principles of the openness of, and access to, information (individual right of access).

89. The principle of openness: The effective exercise of the individual right of access implies the possibility of knowing of the existence of files. There are two possible options, depending on whether such access is by means of individual or general notification.

90. The individual notification procedure chosen by the Federal Republic of Germany consists in informing the person concerned at the time of the initial recording.

91. The general notification procedure is based on the keeping of a register of files, which is available to the public. In some countries, the register includes a brief description of the main characteristics of each file. Such a register can be kept only on condition that there is a minimum obligation to disclose the existence of the files (prior authorization is sometimes required). In addition to facilitating the exercise of the individual right of access, the general notification procedure makes it possible to gain an over-all idea of the development of filing processes. Most legislations have adopted this procedure.

92. The individual right of access, and the rider thereto, the right of rectification: With the exception of a few countries, including the United States of America, which limit this right to nationals or legal residents, the laws of practically all countries impose no conditions as to nationality or residence.

93. This option is in conformity with international human rights law which, not wishing paradoxically to establish forms of discrimination, provides for the protection of the individuals, i.e. every person, regardless of legal or geographical frontiers.

94. It is the responsibility of the person requesting information to give all necessary details concerning his identity and the nature of the information sought. One might have imagined that the holders of personal data should be obliged to organize their files systematically in order to permit an inquiry by name, or, if it exists, by national identity number. But the cure would have been worse than the disease, since it would have encouraged the generalized use of the national identity number, thus increasing opportunities for interconnections.

95. In order to avoid the abusive repetition of requests, certain conditions as to periodicity are generally laid down.

96. The data must conform to the recordings and be readily understandable.

97. If an item of information is proved to be inaccurate at the time of exercise of the right of access, the person responsible for the file is required to rectify it or even erase it. In some laws, such as the Fair Credit Reporting Act in the United States of America, the person concerned has the opportunity only of making his own observations in a brief memorandum, while the person responsible for the file maintains his own interpretation of the disputed information.

98. The right of rectification is sometimes supplemented by a "right of follow-up", which requires the holder of the file to make the error known to all persons responsible for files to whom incorrect information has been transmitted, for the purposes of rectification.

99. While some countries, such as Sweden, tend to provide in certain cases for right of access free of charge, most legislation provides for the payment of a variable fee. Experience acquired over the past 10 years shows that, contrary to what might be expected, the cost of the right of access is low or even negligible.

2. Extension of minimum standards by certain legislations

100. Extension beyond the minimum standards, which varies according to country, relates to the following points:

(a) Establishment of a collegiate (or "ombudsman" type) supervisory authority, acting independently or at least having some autonomy. Its task, in general, is to advise the users of files, to ensure that prior supervisory procedures (declarations or authorizations) are applied, and to ensure compliance with protective standards. A supervisory authority of this sort is envisaged in most enacted and draft legislation.

(b) An obligation, at the time of data collection, to inform the person concerned whether a reply is obligatory or not, and to state the purpose of the collection and the service through which the right of access may be exercised.

(c) Prohibition of the recording of certain sensitive data, such as data of a racial nature or data relating to political opinions, trade union affiliations, religious or other convictions, or sexual proclivities.

(d) Specific regulations for the purpose of avoiding wrongful use of the national identity numbers of natural persons.

(e) Prohibition of decisions prejudicial to the person concerned taken by means of fully automated decision-taking processes (taking account of social background).

(f) Formulation of professional codes of conduct for computer specialists; this safeguard is of limited scope since most specialists are salaried workers and not members of a liberal profession.

C. Foreseeable exceptions

101. Certain data files, on account of their legal status (defence secrecy, medical secrecy) or because their purpose is related to the exercise of a fundamental freedom (press files, files of political or trade-union organizations), are covered by regulations which allow for some exceptions.

1. Security files (police, defence, national security and intelligence service files)

102. In certain cases, the exception is total; the law does not apply. There is a paradox here which gives rise to criticism since it concerns files which, by their very nature, involve the greatest risks for freedoms. A balance must be sought between the requirements of public order and the essential safeguarding of freedoms. In this sense, legislation may be instanced which provides for the restricted publicity of such files or the direct exercise of the individual right of access through the supervisory authority.

2. Medical files

103. Partial exceptions are frequently allowed; the individual right of access is not withheld but must be exercised indirectly, here again, by a doctor of the patient's choice.

3. Files of political, trade-union, religious or philosophical organizations

104. These files or at least files of their members, affiliates or sympathizers, deserve particular attention. Any regulations which allowed a supervisory authority to conduct investigations into such files, even with the object of protecting people's privacy, could amount to a cure worse than the disease. We would suggest that, in this case, freedom of association overrides the protection of privacy, which, in any event, remains protected by the direct exercise of the individual right of access.

4. Files of press agencies and enterprises

105. For reasons likewise obvious, we would suggest that the same situation should apply in regard to files of press agencies and enterprises; here again, freedom of opinion and its corollary, the right to information, must take precedence over the requirements of privacy (which remains protected by the individual right of access).

5. Files of statistical and research agencies

106. Statistical and scientific research work likewise calls for specific measures.

107. It has now been found, from experience, that the possible long-term consequences of new laws relating to data processing and freedoms for statistical and research work have been underestimated.

108. Thus, the obligation to rectify or erase inaccurate or erroneous data can have serious repercussions in the field of medicine; for example, the record of an error in diagnosis should be preserved not only in conformity with clinical discipline but in the interests of basic research.

109. The obligation not to keep data beyond the period necessary in order to attain the goal sought is contested - for obvious reasons - by some historians. For them, document archives constitute an indispensable tool. Similar reservations are expressed by research workers in the human sciences; when data have been compiled on a sample of persons for a particular study, there is no way of knowing in advance of what value they may be - say 10 years later - for a comparative study based on the same sample. Preserving such data may therefore be of scientific value.

110. Scientists are also concerned about the possible risks of "censorship" resulting from such legislation when it envisages a system of licensing or prior authorization involving an appraisal of the purpose of the research.

111. Because of its concern about this situation, the European Science Foundation, which comprises representatives of public research institutes, had drawn up a declaration 10/ aimed at reconciling the need to protect privacy and the requirements of research. A draft recommendation of a similar nature is at present being studied in the Council of Europe.

112. These proposals are reflected in the current legislation of most countries.

D. The special case of transborder files

113. In order to prevent the national legislation of certain countries from being evaded by remote consultation of files established in States lacking protective regulations (data havens), preservation measures are applied in most countries. For this purpose, transborder flows of personal data may be subject to prior control, amounting in some cases to the requirement of unconditional authorization or even refusal when the data flow is to or from a country which lacks any protective legislation or in which a significantly lower level of protection prevails.

114. In order to prevent these legal checks from being diverted from their real purpose and impairing the principle of the free flow of information, the OECD recommendation analysed above and the Convention of the Council of Europe propose suitable regulations of such flows.

10/ Declaration on the protection of privacy and the use of personal data for research purposes, adopted by the general assembly of the European Science Foundation on 12 November 1981.

115. The basis of the provisions envisaged in these international instruments may be summarized as follows:

The rule of the free flow of information remains the basic principle to which reference must be made;

Derogation from this principle is possible only when the protection of privacy and freedoms overrides the principle of the free flow of information. But the rule of free flow again becomes paramount as soon as the legislation of the parties to the instrument fully observes the minimum rules set forth therein; in this case it is in fact accepted that the bodies of legislation in question provide a virtually equivalent degree of reciprocal protection;

Derogations may, however, be permitted in a few particular instances; these derogations may not be made general and may be established only in restricted cases envisaged in legislation which must itself stipulate the forms and conditions of such derogations.

Part III

SPECIFIC PROBLEMS POSED BY THE USE OF COMPUTERIZED PERSONNEL FILES BY INTERNATIONAL, INTERGOVERNMENTAL, REGIONAL AND OTHER ORGANIZATIONS

116. On the basis of information obtained thanks to the spirit of co-operation shown by the directors of the international organizations and agencies consulted, files may be divided into two categories according to whether their purposes are internal or external;

The category of files for internal use comprises those relating to the organization's administrative procedures - for example, personnel management, wages and salaries, social security and retirement schemes, and to a lesser degree data on experts and consultants; likewise covered by this category, in our view, are certain files relating to persons outside the organization (subscribers, visitors, etc.) provided that suitable safeguards are envisaged;

The category of files for external use comprises those intended to enable the organization to achieve greater efficiency in carrying out its statutory tasks.

117. In this connection, certain particularly significant examples may be cited:

The file on refugees of the Office of the United Nations High Commissioner for Refugees;

The file, established in the United Nations by the Centre for Human Rights, on victims of enforced or involuntary disappearances;

Certain applications by the International Committee of the Red Cross (ICRC) or the non-governmental organization Amnesty International.

118. Apart from the files of Interpol - International Criminal Police Organization (ICPO), to which we shall refer later, only certain files in the first category have so far been the subject of protective measures. In fact, four cases have been brought to our attention: the United Nations, OECD, the World Health Organization (WHO) and, at the regional level, the Council of Europe have issued regulations for the benefit of their own personnel.

119. These internal measures relate to professional ethics rather than to standard-setting. However satisfactory they may be, their scope is limited.

120. The protective provisions are, in fact, limited solely to recognizing an individual right of access by the organization's staff members; there is no institutionalized supervisory body.

121. These initiatives were taken at a time when no national legislation on data processing and freedoms existed.

122. It will be recalled that an international organization is in principle subject to the territorial jurisdiction of the country of its headquarters, except where otherwise provided - as in the case of almost all organizations - by means of a headquarters agreement granting privileges and immunities, inter alia to endow it with a certain autonomy.

123. The existing headquarters agreements did not, however, foresee the emergence of these new legislative provisions relating to data processing and freedoms.

124. In this connection, the case of ICPO deserves special study inasmuch as its situation applies to the majority of international organizations and agencies. ICPO is established in France under a headquarters agreement dating from 1972, when the supervision of files had not yet come so much to the fore in domestic legislation; consequently, no provision on this point was made by the negotiators at the time.

125. When subsequently (in 1978) France enacted a law on data processing and freedoms, the National Commission on Data Processing and Freedoms (Commission Nationale de l'Informatique et des Libertés - (CNIL) took the view that, in the absence of specific exemptions in the 1972 agreement, French law applied to the ICPO files, subject to renegotiation of the headquarters agreement to take account of the new legislation.

126. This was the solution which eventually prevailed.

127. Three bodies of rules (headquarters agreement, exchange of letters, internal regulations) make up the juridical framework of the supervisory measures in force.

128. The principle of the supervision of files is incorporated in article 8 of the headquarters agreement proper; this article provides that files are subject to internal supervision by the organization under the general rules established through an exchange of letters with the Government of the French Republic.

129. Through this exchange of letters provision is made for the establishment of a supervisory commission for data files made up of five members of different nationalities, namely:

> Three persons appointed, either for their independence and competence in the field of data protection, or by virtue of the high judicial office they hold or have held; one is chosen by the French Government, another by ICPO and the third, who acts as chairman, by joint agreement of the first two. In the absence of such agreement, the Chairman is appointed by the Secretary-General of the Permanent Court of Arbitration;
>
> A member of the ICPO Executive Committee; and
>
> A data-processing expert appointed by the Chairman of the Commission from a list drawn up by the organization.

130. The five members of the Commission each have an alternate appointed on the same basis.

131. The Commission has two functions. Firstly, it ensures that the personal data contained in the ICPO files are accurate, recorded for specified purposes, and obtained and processed in accordance with the organization's statutes, article 3 of which states that any activity or interference relating to matters or cases of a political, military, religious or racial nature is strictly forbidden as far as the organization is concerned. The Commission also keeps a list of files at the disposal of any citizen or resident of a State member of the organization, and such persons also have indirect right to access to information concerning them. This right is exercised through the supervisory commission, which, on application by the person concerned, carries out the necessary checks and makes the requisite corrections.

132. Rules giving effect to the principles of fairness, purpose specification, accuracy, duration, conservation, and destruction of obsolete data, and practical arrangements to give effect to supervisory rules are laid down in ICPO's internal regulations.

133. Some have taken the view that the protection arrangements are inadequate. They do, however, mark a major advance as far as the citizens of the overwhelming majority of ICPO member countries are concerned. Few of them have adequate domestic legislation, with the paradoxical result that many persons who do not enjoy rights of access - even indirect rights - to the police records of their own countries will be enabled partly to exercise such rights at the international level.

134. It may therefore be considered that, subject to some adaptations or improvements, these arrangements constitute a valuable precedent and may serve as a framework of reference.

I. PROPOSALS

A. The promotion of human rights in domestic law

135. In order, firstly, to encourage States to promote protective regulations in their domestic legislation, and secondly, to avoid excessive discrepancies between one legislation and another, guidelines should be proposed for adoption by the competent United Nations bodies, possibly in the form of a recommendation.

136. The recommendation might be on the following lines.

137. States should take steps to give effect to the following basic principles in their domestic legislation.

138. Principle of fairness: information about persons should not be collected or processed in unfair or unlawful ways.

139. Principle of accuracy: persons responsible for data files should be obliged to check the accuracy of the data recorded and to ensure that they are kept up to date.

140. Principle of purpose specification: the main purpose which a file is to serve should be known before it is established in order to make it possible subsequently to check whether: (a) the personal data collected and recorded are

relevant to the purpose to be served; (b) the personal data are not used for purposes other than those for which the file was intended; and (c) the period for which the personal data are kept does not exceed that which would enable the objective for which they were recorded to be achieved.

141. Principle of openness: measures should be taken to ensure that any person may be in a position to know of the existence of a personal data file.

142. Principle of individual access: any person, irrespective of nationality or place of residence, should have the right:

To know whether information concerning him is being processed;

If the need arises, to have such information communicated to him in an intelligible form, without excessive delay or expense;

To have appropriate rectifications or erasures made in the case of erroneous, unlawful or inaccurate entries.

143. Principle of security: appropriate measures should be taken to ensure the essential security of data files and of access to restricted information.

144. Departures from the application of one or other of these principles might be admitted in regulations concerning security files (police, defence, courts, intelligence), medical records, scientific and statistical data, and press files, provided that the limits of the exceptions were specified and they were embodied in laws or special regulations promulgated in accordance with the juridical system of each State.

145. Information on racial origin, sexual proclivities, political opinions, religious or philosophical convictions, or trade-union membership should not be recorded. Departures from these prohibitions should not be authorized except by law and should be subject to more rigorous safeguards.

146. A supervisory body should be established with adequate guarantees of impartiality both for the purpose of advising the persons affected by these new legislative measures and in order to ensure that the above principles are complied with.

147. The above principles and rules should, at the very least, be applied to public or private computerized files containing data relating to natural persons.

148. Particular provision might be made to extend the application of these provisions to manual data systems.

B. The files of international organizations and agencies

149. The international organizations and agencies using computerized personnel files should be recommended to take appropriate protective measures unless they accept local jurisdiction where such exists.

150. The internal statutes and rules of international organizations and agencies should make provision, as concerns their own files, for the application of the aforementioned principles of fairness, accuracy, purpose specification, openness, individual access and security.

151. A supervisory authority, either of a collegiate or "ombudsman" type, set up under a procedure offering adequate guarantees of impartiality, should be appointed within each organization or agency.

152. Its task would be to advise those responsible for the operation of data files and to ensure effective enforcement of internal regulations.

II. CONCLUSION

153. The Sub-Commission on Prevention of Discrimination and Protection of Minorities might prepare a resolution embodying in some appropriate way the twofold proposal made above for submission to the Commission on Human Rights.

154. As an immediate step, it is suggested that, as far as United Nations computerized files are concerned, one of the members of the Sub-Commission should be appointed to study draft internal regulations with the assistance of the Secretariat.