DATA PROTECTION: INTERNATIONAL TRENDS AND THE AUSTRIAN EXAMPLE

Gerhard Stadler
Thomas Herzog

May 1982
CP-82-22

Presented at a Guest Seminar at the International Institute for Applied Systems Analysis, Laxenburg, Austria, May 18, 1981.

INTERNATIONAL INSTITUTE FOR APPLIED SYSTEMS ANALYSIS
2361 Laxenburg, Austria

AUTHORS

Until 1980 Gerhard STADLER was Head of Department in the Austrian Chancellor's Office, chairman or member of various expert groups in the Council of Europe and in the OECD, and former managing member of the Austrian Data Protection Commission. Since 1981, Deputy Director of EFTA in Geneva.

Thomas HERZOG is an assistant professor at the University of Vienna and a member of the Legal Services of the Chancellor's Office in Vienna.

PREFACE

On May 18, 1981 a Guest Seminar on Data Protection was held at IIASA. Special emphasis was placed on the Austrian data protection law, a typical European data law and one which has major relevance to IIASA's data processing and computer communications activities, our Institute being a registered Austrian "Verein". Drs. Stadler and Herzog were both closely involved from the very beginning in the activities of the Austrian data protection scene as members of the Office of the Chancellor of Austria. Not only were they present when the law was created but they were then able to report on its first impacts.

CONTENTS

DATA PROTECTION: INTERNATIONAL TRENDS AND THE AUSTRIAN EXAMPLE

Gerhard Stadler and Thomas Herzog

INTRODUCTION

Issues of this Paper

Ensuring personal privacy in today's computerized-information society seems to be a common goal among the member states of the OECD. In this paper an attempt is made to summarize the discussions at the political and law-making level, both nationally and internationally within the framework of the OECD member countries.

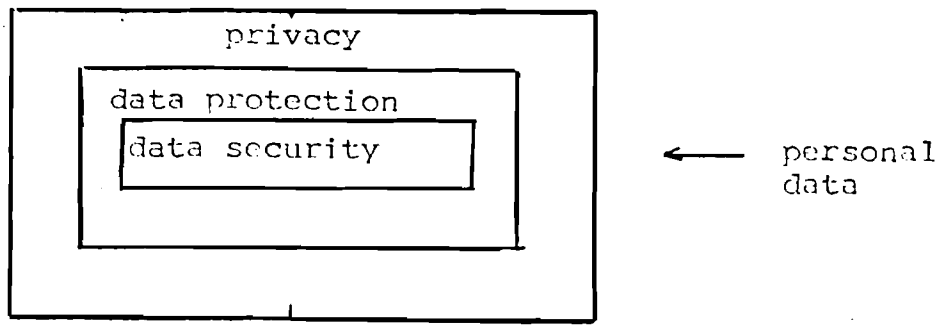
From the concrete outcome of these discussions, i.e., the data protection acts adopted and yet in force, the Austrian situation has been chosen as example (Annex 1).

Some Definitions

PRIVACY =	The right to privacy is the right of the individual to decide for himself how much he will share with others his thoughts, his feelings, and the facts of his personal life. "The right to be let alone".
DATA PROTECTION =	The sum of regulations and instructions dictating when, by whom, how, and to what extent information may be collected and communicated.

DATA SECURITY = The sum of all measures affecting organizations, personnel, technology, or construction taken to ensure that data processing is undertaken in an orderly fashion and that data are not unlawfully disclosed or brought to the knowledge of third parties or revealed to, processed by, or disclosed by unauthorized persons. (In light of the type of data, economic feasibility, and technical possibilities).

PERSONAL DATA = Any data that identify or describe a characteristic of an individual (whether identified or likely to be identified or similarly data on legal entities). This term implies any symbol, number or character, or address by which the individual is indexed in a file or retrievable from it.



DATA PROTECTION AS A PROBLEM OF THE "INFORMATIZATION" OF SOCIETY

Changes in Information Behavior

It is a fact that in modern society, records mediate the relationship between individuals and organizations, thus affecting the individual more easily, more broadly, and often more unfairly than was possible in the past.

For centuries, keeping records about individuals were relatively limited and local in nature. The most complete records was probably kept by churches, who recorded births, baptisms, marriages, and deaths. Town officials and county courts kept records of similar activities. Merchants and bankers maintained financial accounts for their customers, and when they extended credit, it was on the basis of their personal knowledge of the borrower's circumstances. Few persons had insurance of any kind. A patient's medical record very likely existed only in the doctor's memory. Records about individuals rarely circulated beyond the

place they were made.

The last three decades have changed all this, mainly as a consequence of changes in the social, economic and political environment. Most Americans and Europeans now do at least some of their buying on credit, and most have some form of life, health, property, or liability insurance. Institutionalized medical service is almost universally available. Government social services programs and development plans now reach into the population along with government licensing of occupations and professions, and taxation of individuals, and government regulation of business and labor union affairs. Today governments regulate and support large areas of economic and social life through some of the nations' largest bureaucratic organizations, many of which deal directly with individuals.

A significant consequence of this marked change in the variety and concentration of institutional relationships with individuals is that record keeping about individuals now covers almost everyone and influences everyone's life, from the business executive applying for a personal loan to the school teacher applying for a credit card; from a person seeking check-guarantee privileges from the local bank to the young married couple trying to finance furniture for its first home. All will have their credit worthiness evaluated on the basis of recorded information in the files of one or more organizations. The same is true of insurance, medical care, employment, education, and social services. Each of these relationships requires the individual to divulge information about himself, and each usually leads to his being evaluated on the basis of information about him that some other record keeper has compiled.

The substitution of records for face-to-face contact in these relationships is what makes the situation today dramatically different from the way it was even as recently as 30 years ago. It is now commonplace for an individual to be asked to divulge information about himself for use by unseen strangers who make decisions about him that directly affect his everyday life. Furthermore, because so many of the services offered by organizations are or have come to be considered necessities, an individual has little choice but to submit to whatever demands for information about him an organization may make. Organizations must have some substitute for personal evaluation in order to distinguish between one individual and the next in the endless stream of otherwise anonymous individuals they deal with, and most organizations have come to rely on records as that substitute.

It is important to note that organizations increasingly desire information that will facilitate fine-grained decisions about individuals. A credit-card issuer wants to avoid people who do not pay their bills, but it also strives to identify slow payers and well intentioned people who could easily become indepthed beyond their ability to repay. Insurance companies seek to avoid people whose reputation or life style suggests that they may have more than the average number of accidents or other types of losses. Employers look for job applicants who give promise of being healthy, productive members of the work force. Social service agencies must sort individuals according to legally established criteria on eligibility, but also try to see that people in need take advantage of all the

services available to them. Schools try to take "the whole child" into account in making decisions about his progress. And government authorities make increasingly detailed evaluations of individuals' tax liability.

Each individual plays a dual role in this connection—as an object for information gathering and as a consumer of the benefits and services that depend on this information. Public opinion data suggest that most Americans and Europeans treasure their personal privacy, both in the abstract and in their own daily lives, but clearly individuals are also willing to divulge information about themselves, or allow others to do so, when they can see a concrete benefit to be gained by it. Most of us are pleased to have the conveniences that fine-grained, record-based decisions about us make possible. It is the rare individual who will forego having a credit-card because he knows that if he has one, details about his use of it will accumulate in the card issuer's file.

Often one hears people assert that nobody minds organizational record-keeping practices "if you have nothing to hide," and apparently many people like to think of themselves as having nothing to hide, not realizing that whether an individual does or does not can be a matter of opinion. We live, inescapably, in an "information society," and few of us have the option of avoiding relationships with record-keeping organizations. To do so is to forego not only credit, but also insurance, employment, medical care, education, and all forms of government services and demands to individuals or from them. This being so, each individual is, or should be concerned that the records organizations make and keep about him do not lead to unfair decisions about him.

In a larger context, we must also be concerned about the long-term effect record-keeping practices can have not only on relationships between individuals and organizations, but also on the balance of power between the government and the rest of society.

Accumulations of information about individuals tend to enhance authority by making it easier for authority to reach individuals directly. Thus, the growth in society's record-keeping capability is accompanied by a risk that existing power balances will be upset.

The Computer as Information Processing Machine

Automatic data processing possibilities provide a perfect tool for the information needs of modern society. More and more branches of daily life are becoming computerized and this trend will continue. The post-industrialized society will be a computerized society.

The following abilities of the computer are of great importance in this context:

- the possibility of mass storage of data
- multiple choice access to stored data
- low storage costs over an unlimited time periods

- the possibility of linking dislocated input/output stations with a central-unit
- the link between telecommunication and computers
- the future role of computers in the mass media.

Similar lists have often been used by "data protection mafiosi" to show that data protection is a problem related to computers. However, privacy was a legal issue long before the invention of automatic data processing, and practices in recent years show that the real danger to the privacy of individuals started when data were emitted by the computer. It could even be said that computer-based archives are much more secure than manual ones. Here are facing one of the major philosophical problems of data protection: Should data protection be limited to computerized data?

Data Protection as an Option on the Political Scene

The data protection discussion started in the late sixties in the English-speaking countries, mainly for four reasons:

- There has been a growing feeling that computers were giving communities with access to data banks an unfair, unilateral advantage over the individual. This feeling became acute when the use of computers was no longer confined to research and planning tasks.
- The increased use of computers in public administration and the plans of some governments to establish large integrated data banks have been criticized and even blocked by parliaments under the motto "Informations mean power and power should be controlled".
- The rapid development of computer technology and the possibility of linking at with other technologies have raised the question of how to maintain personal freedom in so as to uphold the traditional concept of human rights.
- One of the characteristic features of the new information infrastructure is the introduction and use of personal identification numbers (PIN), which are used not only by public authorities (social security branch), but increasingly also by private parties. Their use permits data derived from different sources to be attributed a single person more easily and its restriction is another goal of data protectionism.

THE EVOLUTION OF DATA PROTECTION

Reports by National Commissions

The data protection discussion started in social science researchers and soon some governments nominated commissions made up of computer specialists, lawyers, businessmen, members of parliament, and trade unionists to explore problems of data protection and to seek guidelines for drafting laws. After having done some in-depth studies the commissions reported to their respective governments. Some of their reports favored the enactment of data protection acts. Some of these are cited in the bibliography.

National Data Protection Acts

The second path in the line of data protection development was the actual drafting and enactment of data protection and privacy acts, which started in 1969 in the Province of Hessen in the Federal Republic of Germany and since then has led to data protection acts in Sweden, the USA, France, Federal Republic of Germany, Norway, Canada, New Zealand, Denmark, Austria, and Luxembourg.

Most of these acts have been rather ambitious. They show a great degree of similarity in principles of data protection. Only the Privacy Act of the USA (1974) was a more or less formalistic one and put its emphasis on future studies of the problem.

International Cooperation

Since computer technology and its use show a truly international structure, international organizations started early to form working groups of government experts to explore the necessities and implications of data protection.

The OECD, the Council of Europe, the European Communities and UNESCO/IBI put data protection on their working programs, mainly for two, somewhat contradictory reasons: 1) to achieve harmony in the structure of legal instruments for data protection in order to avoid problems for international companies and others involved in transborder data transactions and 2) to hinder the circumvention of national data protection acts by parties processing data abroad (in countries with less stringent data protection laws regime).

At the Council of Europe resolutions were adopted by the Committee of Ministers in 1973 and a convention for the protection of individuals with regard to automatic processing of personal data was opened to the signatures of member states and other states invited by the Council of Ministers (Annex 2).

At the OECD, a recommendation concerning guidelines governing the protection of privacy and transborder flow of personal data adopted in September 1980 by the Council of OECD obliged member states to follow its principles.

At UNESCO and the Intergovernmental Bureau of Informatics affiliated thereto, a topic discussed during several intergovernmental conferences was whether to include a "new information world order" into the "new economic world order". In the European Communities the European Parliament adopted a resolution aiming at an international regime governing transnational data transactions.

Data protection schedule

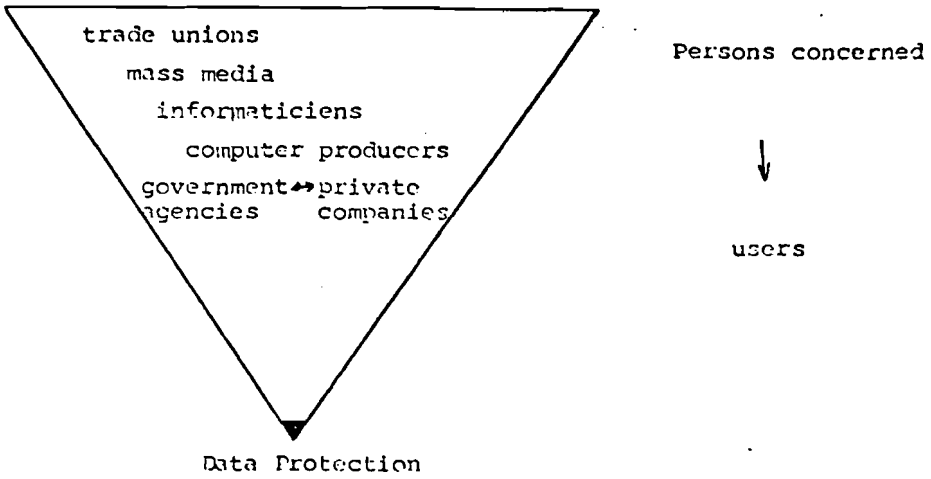
	Reports of committees	Data protection acts	International co-operation
1969		Hessen (FRG)	
1970			
1971			
1972		Sweden	
1973	USA		Council of Europe: Resolution (Private sector)
1974		USA	Council of Europe: Resolution (Public Sector)
1975	UK		
1976	NL		
1977	USA, France	New Zealand, Germany (FRG), Canada	
1978	UK	France, Norway, Denmark, Austria	
1979	Canada	Luxembourg	
1980	Australia		Recommendation: OECD
1981		?	Convention: Council of Europe

The Pressure Groups Involved in Data Protection

DATA PROTECTION PHILOSOPHY

The Concept of Privacy Versus the Concept of Computers

- Is data protection a computer-linked problem?
- What is a computer?
- What is the practicability of legal solutions that deal only with computers?
- Will future development of automatic data processing obscure the strict definition of "data processed automatically supported"?



Have Legal Entities a Right to Privacy?

- The original aim of data protection was to protect the individual. However, certain data pertaining to legal entities are so closely linked with individuals (small and medium-sized enterprises) that they could harm privacy. Thus some countries have included in their legislation the protection of legal entities.
- Small business enterprises should be protected in the same way as individuals.
- For big enterprises transparency should be maintained.

Free Flow of Data Versus Regulation and Limitation of the Processing of Personal Data

- Should there be legal control only in individual cases as they are brought up by the persons affected or should there be "big government" solutions with standing authorities.
- How can the abilities and independence of controlling bodies be ensured?
- Suffice-binding "rules of conduct" by those groups interested in data processing or should regulations be adopted by the state?
- Should data flow be regulated only in the private sector, as some claim, or only in the public sector, as others claim?
- Should licensing or registration systems (with public notice) be implemented for data banks or for information of the individual concerned?
- Should there be "freedom of information" (i.e., public access to government records) or should data about persons filed in such records be protected?

"Omnibus Law" Versus Special Treatment of Individual Sectors

The European solution seems to call for a single, rather general act to deal with all problems of data protection in different branches, while the American approach is to regulate data protection sector by sector (see the Fair Credit Reporting Act 1972). Another often-discussed question is whether it would be useful to crystallize categories of highly sensitive data in order to keep them under special control (see, for instance, the French Act on Data Processing, Data Files and Individual Liberties, Sect. 31, in which computerized storage of personal data that directly or indirectly reflect racial origins or political, philosophical, philosophical or religious opinions or union membership is in principle prohibited).

The Price of Data Protection

- Do data protection requirements result in high costs for the computer users or for service data processing centers? In the private sector data protection seems to conflict with the principle of avoiding government intervention that unduly impedes the growth of productivity.
- However, since data security should be to the computer user's own advantage, the additional costs for data protection seem to be reasonable, as long as the persons filed do not use their rights of access, etc., in an excessive form.
- Charges by the computer user for individual's access to information pertaining to him in a data bank?
- Since in principle data protection tends to hinder data transfer, it might restrict a company's possibilities for using information as a profitable good.

The Conflict of Interests

The right to be let alone sometimes conflicts with the fact that human beings have to live in society. Data protection measures must seek a compromise between the interests of the single individual and those of the community as a whole.

THE PRINCIPLES OF DATA PROTECTION

The Openness Principle

Public administrative agencies and companies must not be secretive about their personal data record keeping policies. No agency or company may conceal the existence of a personal data record keeping system, and every agency or company that maintains such a system must describe publicly both the kinds of information in it and the manner in which it will be used.

Data processing register —special information of the person registered
—and public notice of data banks

Exemptions from this principle may be allowed for public security reasons.

The Individual Access Principle

Individuals should have the right to see and obtain copies of any records an agency or company might maintain about them. Exemptions from this principle may be permitted for reasons of state security or for investigative information compiled for law enforcement purposes. In addition there may be restrictions on patients' access to medical records.

Problems of costs: fees - regular information (each year) without any request

The Individual Participation Principle

An individual shall have the right to challenge the contents of a record containing data about him on the grounds that it is inaccurate, not up-to-date, incomplete, or irrelevant. However, problems may arise with the usage of this right. For instance who must introduce evidence? How could technical follow-up of the request to correct data be carried out?

The Collection Limitation Principle

There shall be limits to the types of information a record-keeping institution may collect about an individual, as well as certain requirements with respect to the manner in which it may be collected. An agency or company is not free to collect whatever information it wishes, nor may it collect information in whatever manner it wishes.

The principle can be implemented by requiring agencies or companies

- to collect only information that is relevant and necessary to accomplish a lawful purpose,
- to collect information directly from the subject individual as far as this is possible,
- to obtain special licenses before collecting and storing certain very sensitive types of information.

Problems may arise with regard to the private sector's right to free enterprise. Also there is some question about how to deal with data for scientific purposes.

Exemptions for Police and intelligence service records would be exempt from this restriction.

The Use Limitation Principle

There will be restriction on how information collected about individual may be used internally by agencies or companies.

Problem: Borderlines within an institution?

The Disclosure Limitation Principle

There must be limits on external disclosure of information.

Problems: Changes in the pre-defined competence and in the purpose of the data-storage.

Routine use versus exceptional circumstances

Disclosure between affiliated entities

Assistance between administrations

Use and disclosure or personal data for research purposes

Data exports

The Information Management Principle

Someone must be made responsible for the proper management of an information system. The handling of the system and the appropriate measures needed to ensure data security shall be described in a set of norms.

Problems: Competence and abilities of the "controller of the file"

Independence of the "controller of the file"

Technical developments

The Principle of Getting Control Over By-Passers

Personal data processing practices shall be overseen by an independent body that would propose amendments to the law whenever this seems necessary to ensure personal privacy. Circumvention of the law, either by processing abroad or by using new technological innovations not foreseen by lawmakers, must be avoided.

Problems: See under 6.7 and 8.

THE AUSTRIAN DATA PROTECTION ACT 1978

Enactment

1978. Published in Bundesgesetzblatt 1978/565. See Annex 1.

Basic Principles

- Constitutional clause: Right of the citizens to protection of their personal data (Sect. 1).
- "Omnibus law" affecting both the public and private sectors for all "automatically supported" processing of personal data.
- Personal data means information about individuals and legal entities.
- Set of rules for the enforcement of the act by individual rights and before a specialized agency ("Datenschutzkommission or Data Protection Commission), which is courtlike.
- The handling of information is thus included in the legal procedure and must be carried out within the competence of an record-keeping agency or company.
- Restrictions on the collection, storage, and distribution of data according to the legally described competence of an agency or company.
- Separation of roles between a data processing center (responsible for the accuracy of the data security) and of the unit undertaking or ordering the collection, processing or disclosure of data (responsible for the legality of these steps).
- Transborder data transfers only permitted by license issued by the Data Protection Commission.

The Procedure to be Followed for the Creation and Maintenance of an Automatically Supported File containing Personal Data

- The Data Processing Register at the Austrian Central Statistics Office must be notified (before the data bank becomes operational).
- The purpose of the file, the group of persons on whom data is to be filed, the type of data and their use must be circumscribed based on legal instruments (acts, regulations, licenses granted by authorities, statutes).
- Upon registration actual processing may begin. The register is open to the public.
- Disclosed data must contain a registration number ("DVR").
- Persons handling the data must be informed about the confidentiality of data (penal sanctions for breaking confidentiality).

- There are no provisions governing the access archives. Thus for non-computerized archives the question of whether access to documents might not harm the legitimate interests of persons about whom data is filed must be decided case by case in view of the constitutional principle that privacy should have priority (Sect. 1 par. 2 DPA).
- The competences of private companies, at least, are not well defined by the legal system. Thus there is some uncertainity about the legality of their data banks.
- There is no clear definition of "automatically-supported" data transactions.
- The act is inadequate for dealing with the coming reality of "personal computers".
- The lack of special provisions for compensatory damages make to committing an infraction of the DPA a relatively low-risk undertaking.
- The problem of how to strike a balance between freedom of the press and the right to privacy has not yet been solved by the legislators..
- The question of the role of the workcouncil (Betriebsrat)when the employer designs a personnel information system remains open.

OPTIONS FOR INTERNATIONAL DATA PROTECTION

The Possibilities

There are several possibilities for an international understanding to regulate the freedom of international data flow and the protection of privacy:

- International organizations can elaborate principles for fair international information processing in transnational data flow and pass them as a recommendation to its member states. Interest in such an instrument would be a certain moral-political obligation for member states to follow the principles, but there would be no consequences to non-compliance. Only among the European Communities is such a guiding principle or regulation of a binding nature.

Such a recommendation was adopted by the OECD in 1980.

- Principles of fair information processing for international data flows could become the subject of an international legal agreement. The ratifying states would be bound to carry out these principles in their domestic laws. Such a convention would not result directly in rights and duties for individuals. It would be "non-self-executing" and should become part of national legal systems through the inactment of domestic laws. The states would have to oblige themselves not to prevent other member states from data flow by ratifying such a convention.

This regulation seems important as it would prevent an imminent danger of protectionism in data flow and, at the same time, maintain the principle of reciprocity. The potential restriction of information flow to non-member states would provide a motive for ratification of such a convention.

— At the Council of Europe an obligatory international convention has been elaborated, which contains principles of fair information processing for national and international data flow and which seeks to ensure that the implementation of the data protection laws is coordinated by means of close cooperation between administrations. The crux of the convention is data protection, both nationally and internationally. The persons concerned should have a uniform legal position towards an information processing company, regardless of in which member state of the convention it is situated.

  The "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" was adopted by the Council of Europe in 1981 and was signed by some member states of the Council. (See Annex 2.) However, to enforce it, the ratification of the convention by the parliaments of five member states of the Council is necessary. In addition to the obligation to respect the basic principles of data protection and to cooperate between national administrations it is stated that data transactions between states subscribing to the convention need not be licensed (except where such transfers would result in circumvention of the data protection act of the exporting state—which could happen in view of the possibility to export further on to a non-contracting state).

— A special legal system that overlaps national law systems can be founded calling for transnational information systems to submit to the provisions of a convention and, consequently, to a single law-system on essential matters. An admissions system would be created for transnational information systems and networks, whereby the admission of a company to one member state of the convention or to an international authority would mean the admission and activity of this company in all member states of the convention.

  Such a model would lead to an international license. While unprecedented, it would probably be the most suitable means of constructing transnational information systems.

  The regime for one such type of such network is described (Annex 3, EURONET), showing the problems of adhering such a system essential for research work without discrimination.

— An intergovernmental conference could be held at which parties would seek to reach informal understandings on the contents of national regulations affecting data flow. Though such non-binding understanding could be very useful and detailed; they would not be able to decrease the existing insecurity surrounding the planning of transnational information systems.

Contents

An examination of such instruments reveals several areas where international regulations could be important, even essential:

- In drawing up common guidelines or conventions among states to facilitate the protection of personal data moving across borders.
- In the creation of new access rules and forms under which data communication services are organized and supplied.
- In the allocation of proprietary rights for computer-based data files the establishment of legal norms, and the formalization of new data rights for individuals, information providers, and users.
- In the establishment of appropriate trading rules, methods of pricing, and contractual procedures in recognition of the economic importance of information as an intangible product marketed by a new services industry.
- In the international harmonization of data communication tariffs in order to ensure the most equitable conditions possible for fair competition by users located in different countries and in reconciling new pricing policies reflecting the opportunities offered by modern technology with legitimate user interests.
- In standards for technical harmonization.

The Need for International Regulations

International regulations on data protection and freedom of information flow seem to be needed assuming that:

- Laws development for data protection continue to be made, leading to data protection provisions in most of western industrialized states.
- Technological development, taken for granted here, indeed makes the transfer of information across large distances cheaper and simpler.
- The necessary communication media are placed at our disposal ("telematics").
- The present world economic situation and the situation with regard to the international relations of companies and the international division of labor remain unchanged.
- Liberalism is also accepted in the field of data processing and information transfers and is guarded against the threat of protectionism in this domain.
- Discussion is limited to transnational data flow by means of automatically supported communication.
- Due to international law or to matters of foreign policy the national legislators cannot sufficiently answer the questions connected with the problem, especially the privacy question.

In affirming the urgent need to regulate transnational data flow

beyond the strict question of data protection, attention should also be paid to the following points of view:

- Transborder data flow it should be free of duties or similar taxes.
- For the time being, the problem of international data flow regulation seems to be restricted to the member states of the OECD. However, every international regulation must be open to accession or acceptance by other states. The development of international information flows will certainly lead to the need to include other states, which must be given the opportunity to accept such international regulations. The UNESCO-IBI Conferences in 1978 (Strategies and Politics for Informatics) and 1980 showed a strong demand by the developing countries to participate in the evolution of informatics and to have access to international networks. These states fear becoming handicapped in their economic progress if they can not bridge the gap in computer equipment and training. An information infra-structure would enable these countries to be partners of our data networks, where our data could be processed.

  So in the not so distant future the range of international data protection measures should become worldwide to avoid "data-havens". This would make data protection no longer a problem restricted to the industrialized western hemisphere.
- It must be considered whether—similar to the national discussion—non-automated data flow and data pertaining to legal entities shall be included in the international discussions.
- Finally, time plays a role that should not be underestimated, in view of the slowness of international organizations and the number ratifications necessary for enacting a convention. Finding compromises according to the principle of unanimity in the organs of some international organizations and the establishment of international networks are also slow processes..

FUTURE PROSPECTS FOR DATA PROTECTION

The Transborder Data Flow Problem Remains Unresolved

If national data banks can be removed from state or citizen access through telecommunication at any time, all national legislation that is not reinforced by international actions becomes superfluous.

The "Vulnerability of Society" Question

Public administrations like private companies, are becoming more and more dependent on computers and their suppliers. The question of how to live with this has not yet been discussed and could lead to the notion of "data protection of the state".

Personal Computers

The basic ideas of data protection date from the early seventies, at which time the acts were designed with a view to large computers. But technological development and marketing strategies have made it possible to offer small personal computers more and more cheaply. These instruments might be used in a way that harms the sensitive interests of persons about whom data are filed. The whole instrumentarium contained up to now in the DPAs seems inappropriate for handling the danger to the privacy of persons about whom data are based in personal computers.

Theory and Practice

DPAs were mainly constructed from the standpoint of theory. Their application must show where the real problems lie and where weighty interests of affected persons were neglected. Until now data protection has focussed on computerized information. However, practical experience over the last years has shown that a lot of the problems related to the privacy of individuals have nothing to do with computers.

Research and Data Protection

The problem of the access of researchers to personal data and of the use of such data has been discussed on several occasions, but thus far no DPA has contained special provisions defining under which circumstances non-statistical data may be transferred to institutions dealing with scientific work. Nor has the question of to what extent data that maintain their identifying functions are really needed by researchers been studied in depth. The answers to these questions might differ from discipline to discipline. Perhaps the problem could be circumvented by finding means to avoid the need for personalized data.

One proposal for principles to deal with the protection of privacy and the use of personal data for research, adopted in 1980 by the European Science Foundation (Annex 4).

Revision of Data Protection Acts

Thus a revision of data protection acts is likely to be undertaken in the near future. This might include a reappraisal of positions in the data protection philosophy mentioned above, taking into account information behavior and handling in all of modern society.

REFERENCES

Westin A. 1968. Privacy and Freedom.

Steinmueller W. 1979. Legal Problems of Computer Networks, Computer Networks 3. Pp. 187-198.

Hondius, F. 1975. Emerging Data Protection in Europe.

Afanasjew, W. 1976. Sociale Leitung und Information der Gesellschaft. (In German).

Nora, S. and A. Minc. 1978. L'informatisation de la society.

Stadler, G. 1981. Vom Datenschutz zur Informationspolitik, Datenschutz und Datensicherung. Pp. 1-9.

UK: Report of the Committee of Data Protection ("Lindop-Report"). 1978.

Comite consultatif des telecommunication et de la souverainete canadienne: Le Canada et la telecommunication. 1979.

Privacy Protection Study Commission (USA): Personal Privacy in an Information Society. 1977.

OECD: Information Computer and Communications Policies for the 80's. 1981. Paris: ECCP Studies.

UNESCO: Les strategies et les politiques en informatique. 1978. SPIN Conference.

Ministry of Defense (Sweden): The Vulnerability of the Computerized Society. 1979. Stockholm.

Annex 1: Austrian Federal Act on the Protection of Personal Data (Data Protection Act), October 18, 1978. Published in Bundesgesetzblatt No. 565/1978. Vienna.

Annex 2: Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. January 1981. Strasbourg.

Annex 3: M.V. Walterskirchen, 1981. Euronet: Growth of a Direct Information Access Network, EFTA-Bulletin. 1/1981, Geneva.

Annex 4: European Science Foundation, 1980. Statement Concering the Protection of Privacy and the Use of Personal Data for Research Adopted by the Assembly of the ESF. 11/1980. Strasbourg.