New technologies: a challenge to privacy protection? (1989)

Study prepared by the Committee of experts on data protection (CJ-PD) under the authority of the European Committee on Legal Co-operation (CDCJ), Strasbourg 1989

1. Introduction

1.1 The background

In elaborating norms for data protection, the legislator in the course of the 1970s, both at national and international level, took as his point of departure the existing state of computer technology and proceeded to draft legal solutions to the perceived problems created for the individual by the use of such technology. The approach was to freeze technology within a legal framework of definitions and protective principles so as to allow the hazards of the computer to be reduced to a minimum while at the same time allowing computer technology the possibility of providing society with its acknowledged

benefits.

The solutions envisaged in the 1970s were valid insofar as they were brought to bear on the then state of the art, characterised by mainframe/ stand-alone computers with dedicated applications, capable of storing and processing data on "identified or identifiable individuals" on a "file' under the authority of a "file controller" identifiable at will by a "supervisory authority".

Technology, however, does not stand still; it rapidly outstrips existing norms and forces new responses from the draftsmen. While they were giving the final touches to the state-of-the-art legislation of the 1970s, a rapid advancement took place in technology which was characterised by an explosion in the number of computers, an increase in their computing power, a reduction in their cost, and their increased availability in the home, within enterprises and within public administrations. Distributed, decentralised computerised systems with enormous potential for the collection, processing and communication of personal data produced consequences which caused legislators to reflect on the adequacy of the approach they had adopted. All this was made possible by the rapid development in telecommunications whose engineers were able to exploit the ingenuity of the computer experts to render compatible two previously separate technologies. The marriage of data processing and telecommunications not only allowed for greater distribution of dataprocessing systems and for data transmission to challenge existing concepts but also produced a range of telematic services which gradually began to pose their own problems.

1.2. The terms of reference

The Council of Europe, which has sought to give a lead to national legislators in the field of data protection by elaborating and opening to signature the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("he Data Protection Convention") of 28 January 1981, has itself begun to reflect on the impact which information technology has on the norms embodied in the Convention and which are incorporated in the legislation of the Contracting Patties or which are being taken up by states in the process of drafting laws in this field. It is for this reason that the intergovernmental Committee of experts on data protection (CJ-PD) specifically sought authorisation from the Committee of Ministers of the Council of Europe to include an analysis o the implications of certain of the new technologies for data protection in its renewed terms of reference, namely:

"To examine closely the implications for data protection of the following technologies and to prepare any necessary legal instruments:

i. telemetry,
ii. interactive media,
iii. electronic mall systems.'

In embarking on this examination, the committee of experts had already accustomed itself to the type of problems being generated by the introduction and use of the new technologies. In addition to the information acquired through the exchange of views among the experts themselves in the course of various meetings, the committee was able to derive considerable benefit from the scientific reports presented at the 14th Colloquy on European Law which took place in Lisbon from 24 to 26 September 1984 on the theme "Beyond 1984 - The law and information technology in tomorrow's society'. The thinking of the committee was further sharpened by the presentations made by two consultant experts in the field of new technologies, at its 11th meeting (16-19April 1985), Professor Arnbak (Netherlands) and Professor Chamoux (France).

1.3 The working party's approach

The working party, mandated to explore the issue, held its first meeting from 16 to 18 December 1985, during which it was able to gain an overview of the problems posed for data-protection systems by the three types of technologies. To further its work, it decided to seek additional information from the member states in regard to their experiences in the introduction and use of telemetry, interactive media and electronic mail, particularly from the point of view of the problems being posed and the legal responses being provided by member states for such problems. The responses provided by the member states were done so on the basis of the following working definitions of each of the technologies in question elaborated at the first meeting of the working party:

i. Telemetry

The remote collection of personal data by automatic means, where the data subject plays no active part in the actual process of the collection of data;

ii. Interactive media

Automatic data-processing systems which provide the basis for instantaneous dialogue between an individual and such a system with a view to obtaining and transmitting information at the initiative of the individual;

iii. Electronic mail

A telematic system which enables person-to-person storage and forward communication such that. as required, messages can be sent and accessed by a central facility, the sending of messages being under the control of the sender and their receipt under the control of the addressee.

It is important to stress that the working party in its subsequent meetings (1 -3 October 1986; 16-18 March 1987), when drawing up this report. did not regard the above definitions or the concepts themselves as watertight. The replies received in response to the questionnaire confirmed the difficulties which can be experienced in attempting to force new technological phenomena into fixed categories. There is always the danger of

excluding some technology which is not always immediately recognisable in terms of telemetry, interactive media or electronic mail. For example, how should expert systems or teleconferencing be classified? Accordingly, it was thought desirable to proceed on the basis that the terms referred to in the mandate could have a narrower or wider application and to take an illustrative approach to each of the technologies based on the responses to the questionnaire. Moreover, the search for definitional precision could possibly isolate the technologies from consideration of the problems created by the wider context which gives rise to them - the new technological infrastructure formed by telecommunications and data processing. It is this aspect and, in particular, the possibilities offered for multifunctional use of telecommunications networks and increased data flow which provide a common point of reference not just for telemetry, electronic mail and interactive media but for other technologies as well. The analysis, which follows in Chapter 2, of technological trends is therefore valuable not only for placing in context the later discussion of three specific technologies but also for allowing broader problems and issues to be ultimately identified which go to the heart of present concepts of data protection when confronted by technology in general.

1.4. The structure of this report

Bearing in mind the nature of the analysis to be undertaken in Chapter 2, each of the terms used in the mandate will be the subject of a descriptive analysis, the point of departure being the general working definitions used for the purposes of the questionnaire against which tile information received is analysed from the point of view of the service features/technical characteristics and state of existing and proposed regulation In member states of each of the technologies. Following on from an identification of the data-protection issues and problems which each of the technologies poses, an attempt is made to draw the attention of member states to the various ways in which these problems and issues can be addressed.

It is not the intention to draft legal solutions for the various problems which are identified in the report. Rather, it is hoped that states can benefit from their exposure to the approaches pursued in certain countries. In other words, the various options available for resolving the problems posed by the different technologies are highlighted, so allowing states the freedom to develop their own policies in accordance with their own perception of what constitutes the appropriate approach.

Over and above the particular problems, it is considered important to pitch the discussion at a more general level by analysing the challenges which the technologies collectively present for existing data-protection concepts. It is for this reason that Chapter 6 invites governments to consider the continuing resilience of existing data-protection norms for responding to the new technological environment.

2. Present trends in technology

As was underlined during the 14(h Colloquy on European Law. the new technologies are in the process of bringing together all the already known techniques (data processing, telephone, telex, television, etc.) and are improving them considerably both qualitatively and quantitatively.

The marriage of data processing and telecommunications to which the French have given the name *télématique* (telematics) has thus opened up enormous perspectives in every country. It has completely changed the traditional means of circulating information (printing, publishing, etc.) as well as the service sector. As Professor Arnbak noted in his report to the intergovernmental Committee of experts on data protection (CJ-PD), the world market for telecommunications equipment and services is today much more important than the market for computers. In this regard, reference may be made to the French experience where the *kiosques* services of Minitel alone brought the service-providers and publishers receipts of 360 million francs in the first six months of 1986 as opposed to 260 million francs in the whole of 1985. Accordingly, the industrial and economic importance of these new technologies is noteworthy for our societies.

Information, an essential element of our life, has become a marketable commodity and it has now become interesting to capitalise on it hence, the spectacular increase in data banks over the last few years: data banks for general use, often international in character, as well as a host of so-called "localised" banks set up by the press, local collectivities and administrations.

However, information in itself has no value unless it is rapidly accessible and from a distance via networks. The investments necessary for setting up appropriate infrastructures are considerable and this explains, moreover, the need to seek out the most cost-effective use of data-processing equipment. The concern for cost-effectiveness produces the interconnection of networks in such a way as to share out their costs and benefits, and leads also to the integration of several services into the same network. The creation of a single multifunctional network which would integrate the traditionally separate networks used by the telephone, telex and data processing is already envisaged - the Integrated Services Digital Network (ISDN). This is technically possible thanks to the digitalisation of networks and services. When the telephone, telex as well as fixed and moving pictures are represented in the form of "bits", it is possible to process them through a common digital system and in a common network. Furthermore, the separate networks for television broadcasting can also be integrated into this digital network so as to form what is called Integrated Broadband Communications (IBC).

In the context of cable communication, mention should be made in particular of fibre optics which considerably increase transmission capacity and open up new possibilities in the field of interactive or bilateral relations.

Satellites constitute another example of multifunctional networks which were at first used for the transmission of telephone conversations but are now used increasingly to exchange television programmes between broadcasting authorities.

This technical evolution towards multifunctional networks and towards the increasing interconnection of systems is reinforced by standardisation measures which are designed to improve the compatibility and linkage of the systems. Indeed, it is only through mass production, and therefore efforts at standardisation, that the cost-effectiveness of communications systems can be promoted.

Technical progress has, moreover, made possible a reduction in the price of computer hardware, allowing it to be more accessible to the public at large. The spectacular development in microcomputers in just a few years is a living example of this. At one time the preserve of specialists, data processing as well as new information technologies are within the reach of a growing number of bodies and individuals. Furthermore, as opposed to other techniques, data processing is more easily assimilated by the population and in particular by young people. Running parallel to this phenomenon, there is also a simplification in the use of data-processing hardware. By way of example, reference may be made to the progress achieved in the software for the electronic telephone directory (Minitel) in France which makes it possible to look up people's names without knowing the correct spelling, or place names without knowing their geographical situation. Although Minitel was primarily conceived in terms of its use as an electronic telephone directory, it has today numerous other applications.

The consequences flowing from the technological evolution just described are of two types.

Firstly, the penetration of data processing in society is such that it becomes "domestic'. Office work within the home can now be envisaged making it possible to manage correspondence and private business under the same conditions as exist within an enterprise. Going further than this, interactive television will, thanks to a keyboard and a simple television screen, offer numerous possibilities - the monitoring of sick people in their own homes, the surveillance of homes against thieves, the organisation of instantaneous opinion polls, remote metering by various bodies (for example energy consumption). the recording of television programmes, the consultation of data banks, the delivery of video programmes, programming the oven or the washing machine, etc.

Accordingly, we are witnessing a gradual "banalisation" of the data-processing phenomenon which in itself presents a danger in that individuals may not be entirely conscious of all the consequences flowing from these technological acts. In fact, there is from now on the possibility of total surveillance of the individual.

In addition, information is today being circulated, disseminated and dispersed in conditions which make it more and more difficult to protect.

The second consequence of the technical evolution described above is that it is practically impossible to isolate data processing from other activities and this makes the work of lawyers much more complicated. What legal rules must be applied to a particular network knowing that it can integrate both information which can circulate freely (television programmes) and at the same time personal data, access to which should be reserved to

certain people? As Professor Arnbak has noted, the legal framework depends today less on the technology applied and the classical rules which are based on a particular technology (press law, television law, etc.) risk being rapidly overtaken. The tendencies towards public integrated networks and interconnection of systems which are accelerated by economic progress and a better exploitation of the systems risk putting fundamental legal principles in conflict if these principles are to be based on criteria or on concepts which are overly technological.

Professor Arnbak proposed, accordingly, to define the categories of telecommunication services to which the same legal rules could be applied. This involves distinguishing the various types of information flows between partners in communication and analysing the related powers and positions of the participants in this context by replying to the following questions:

1. Who controls the transfer of information (in respect of the choice of timing, subject, speed, etc.) - an institution or individual participants?

2. Does the information come from an institution or from an individual?

The combined answers to these two questions make it possible to draw up the following matrix which establishes information flow models. (The models have been constructed by Mr J.L. Bordewijk, Professor of Telecommunications, and journalist, Mr B. van Kaam.)

	Information from individual source	Information from central source
Individual choice of timing, subject, etc;	Conversation	Consultation
Central choice of timing. subject, etc;	Registration	Allocution

Professor Arnbak draws the following conclusions from this diagram:

- copyright issues appear in the right-hand column;
- data-protection issues appear in the left-hand column;
- control procedures and state intervention appear desirable in the lower row;
- on the other hand, as far as the services outlined in the upper row are concerned, it is necessary to guarantee the free flow of information and to keep state intervention to a minimum.

The drafters of this report found such an analysis of particular value in approaching and identifying the various data-protection issues raised by telemetry, interactive media and electronic mail systems. More importantly, it allowed them to enlarge the discussion so as to give consideration to technologies in general. It is for this reason that frequent

reference will be made in the course of the report to the above information flow models.

3. Telemetry

3.1. Service featuresltechnical characteristics

Using as a reference point the information flow models just described, telemetry fails into the category of data registration, the collection and filing by a central body of information from individuals or other sources at times determined centrally. By Way of example, the following may be cited: electronic surveillance systems (sound detectors, video cameras, etc.); remote reading of water, electricity and gas meters; identification of vehicle number plates; assessment of the number of mistakes committed by a typist; monitoring of the television programmes viewed by an individual; surveillance of old people in their homes, etc.

Two factors emerge from this definition: the *remote* collection and storage of data and the non-intervention of the data subject who may not know when the data are being collected and stored or who may not even be aware of the fact that data concerning him are being collected and stored.

The content itself of the definition elaborated (see paragraph 1.3 above) is not particularly problematic, there existing a consensus on the sort of services corresponding to the term telemetry. However, it has been pointed out that the "capture" of nominate data on a computer terminal could fall within the scope of this definition. Accordingly, it has been proposed to stipulate in the working definition that the processing is entirely automated. As regards the term 'telemetry", the opinion is shared by several experts that the word *télémesure* would be a more appropriate term in the French language (remote metering in English).

3.2 The situation in member states and actual and proposed regulation

Although telemetry may appear to be a new phenomenon, remote metering has in fact been in existence for a considerable period of time, notably in regard to the storage of the telephone calls of subscribers. However, apart from the telephone it would seem that there are very few applications of this technique in the member states of the Council of Europe. The following examples may be cited:

Belgium: Remote maintenance of telephone switchboards which may be programmed from the supply company;

Federal Republic of Germany: Remote reading of electricity meters (the Temex system). A similar system is envisaged for water consumption;

France: The installation of call-recording devices in enterprises;

Spain: The sending and receiving of electrocardiograms from ships;

Netherlands: Several municipalities envisage using the local cable television networks to read the consumption of gas, electricity and water in homes;

Norway: A similar system is envisaged for the reading of electricity consumption.

It may thus be seen that the Federal Republic of Germany is practically the only country where a telemetric system is applied on a large scale: the Temex system. This system is subject to special provisions contained in the Telecommunications regulations. According to Article 8, the Temex service providers must inform their clients of the circumstances, the extent and the time of the data transfer. Article 9 states that information obtained through telemetry which contains personal data may be temporarily stored by the *Deutsche Bundespost only* on the request of a public utility and only in order to identify the amount of consumption of their clients. The information used to identity the amount of consumption is only to be stored to the extent necessary for the calculation of the charges made for the goods consumed. The information is to be transmitted to the service provider after four days at the latest and it is subsequently to be erased by the *Deutsche Bundespost.*

The Data Protection Law of the *Land* of Hessen also contains a provision concerning telemetry and remote monitoring. It stipulates that anyone using a telemetric system or any other remote monitoring system located in an individual's household or at his place of work must obtain his prior consent.

In Belgium, remote maintenance of telephone switchboards is regulated by contract.

In France, the introduction and use of telemetric systems are covered by the 1978 law on data processing and freedoms. The law establishes a simple declaration system for the private sector and a system of opinion together with the publication of a regulatory act for the public sector. Article 29 states that any person ordering or carrying out personal data processing is obliged, *vis-à-vis* the data subject, to take all necessary precautions so as to ensure the security of the information and in particular to prevent it being distorted or communicated to unauthorised third parties.

In Norway, the registers set up for the needs of telemetry are covered by the Data Protection Law and the Data Inspectorate is competent to regulate the way in which information can be collected. The Data Inspectorate may also prohibit the use of telemetry or indicate that solutions other than telemetry exist.

3.3. Analysis of the data-protection problems

The services offered by telemetry are many. However, the problems posed for data protection are not the same. The remote monitoring of a house does not pose too many data-protection problems, unlike the automatic reading of a meter or remote collection

and storage of television viewers' preferences for a particular programme.

The data subject's lack of knowledge of when data are collected on him and what sort of data are collected is one of the main characteristics of telemetry. The collection can in fact take place at any time. The telemetric system for electricity consumption proposed in Norway envisages meter readings on individuals every six minutes. Formerly, the reading of meters was carried out once a year by one person. There is therefore a great difference between the former system and the system proposed. In the second case, very detailed information will be collected which is neither justified from the point of view of household electricity consumption nor by reasons of management or statistics. This accumulation of details represents a real danger for privacy, particularly if data are used for purposes which are incompatible with the original aim. One fear which is currently invoked concerns the notion of "the transparent man" who may be monitored continuously, totally and from a distance. It emerges from these considerations that the data subject must be informed that data on him are being collected as well as of the frequency of the registration. The question of the processing finality is equally essential in this context.

Another problem dealt with concerns the possibility of storage by the *carrier* of information which has been collected telemetrically. It has been seen that in the Federal Republic of Germany the *Bundespost* can store, at the request of the service provider, data which have been collected via the Temex service. This case, however, seems fairly unique but there does exist an additional risk of an abuse of the information even if the. storage is limited in time.

The need for certain devices such as those allowing the number of mistakes made by a typist to be estimated also merits consideration. The fact that something is technically possible does not necessarily mean that it should be used. It has been suggested that in such cases it is necessary to determine limits to what is acceptable.

The rights of access, rectification and erasure also appear important in the context of telemetry.

Taking account of the different problems outlined above, any possible regulation of this issue should take account of the following factors:

1. Advance information. even in certain cases obtaining the prior consent of the individual who is to be subjected to remote monitoring or a telemetric system. If this proves impossible, the collection of data should be subordinated to legal authorisation;

2. Information to be given to the data subject in regard to the holder of the data collected, the frequency of data collection. the time of their storage and the use to be made of them;

3. Prohibition on secondary use of data and in particular a prohibition on communication of data to third parties;

4. Right of access to the data and, as the case may be, right of rectification;

5. 'The right to be forgotten': the data stored should be erased after a certain time, bearing in mind the need for time limits for dispute resolution.

4. Interactive media

4.1. Service featuresltechnical characteristics

The term "interactive media" is sufficiently generic to allow a range of technological applications to be covered. Where a user equipped with a terminal and having access to communication lines can oblige a computer to respond to events initiated by him, it is possible to speak of an interactive application. As so stated, interactive media differ from telemetric devices in that the individual takes the initiative to set in motion an automated procedure which leads to a relationship with a third party. The consultation model described in Chapter 2 is an accurate representation of what takes place in electronic information services, one of the most common applications of videotex systems. The information flow is triggered off by the user who seeks to consult a central database with a view to obtaining information from an information provider. Broadcast teletex also conforms to the consultation model although it is not interactive *stricto sensu* in that it permits only the receiving and not the sending of information. Expert systems are also illustrative of the consultative possibilities offered by data-processing systems linked to telecommunications and dependent on the intervention of the individual.

However, it should be stressed that interactive media also permit transactional dialogues between users and service providers which go beyond mere consultation of centrally stored databases. It is increasingly the case that videotex system operators allow their subscribers to interface remote computers so as to make possible teleshopping or telebanking transactions. In this context, the consultation model of data traffic flow remains accurate to the extent that the services become operational at the initiative of the individual user. It will be recalled, however, that any one telematics system may include one or more information flow patterns. In the context of interactive media, regardless of whether a videotex system is limited to user scrutiny of information pages or extends to commercial transactions or beyond that to the conduct of electronic referendums or opinion polling, it will be the case that data registration will also be an issue. As will be illustrated later, it is a feature of interactive media that their use gives rise to the collection and storage of personal data.

At a general level, what may be termed "interactive media' give rise to a triangular relationship: a service user, a service provider and a carrier. However, it must be recognised that there may be additional parties to the relationship, for example the producers of the information which is put at the disposal of the service providers. In addition, it will often be the case that the service provider will also be the carrier as when the PTTs themselves or private cable operators constitute and manage central databases.

Breaking down the relationship into its component parts, the following characteristics may be identified:

i. The service user

An individual or a private or public enterprise may constitute the service user. However, given that the working framework is governed by personal data of natural persons, attention is focused only on the individual. In addition, although of obvious commercial importance, attention will not be accorded to 'anonymous" access to videotex systems where, for example, a data base is interrogated by a third party (a travel operator, a bank) at the request of an individual. In his capacity as user, the individual may avail himself of the following services:

a. public or private data banks which he may consult with a view to obtaining information, for example news, timetables, weather reports, the stock exchange, cinema listings, etc. Over one hundred thousand pages of information may be available centrally in a videotex system with the possibility of interfacing other data bases stored in remote computers;
b. teleshopping: a range of services is possible;
c. telebanking: a range of financial transactions is possible;
d. reservation of trains, theatre seats, holidays, etc.;
e. audience response to broadcasts;
f. electronic polling on certain issues;
g. television programme requests;
h. teleprocessing;
i. electronic games;
j. etc.

As regards the forms of intervention which the individual can use to trigger off the "dialogue" or the "interaction" or, in some cases, "unilateral consultation" where the data bank accessed remains unchanged, regard must be had to the communication framework between the user and the provider.

In the first place, two-way cable television, using public or leased telephone lines or private cable (coaxial, fibre optic) or satellite, allow the individual with a specially equipped television set (that is, with a modem and a decoder) to access a variety of commercial and retail activities and information sources. The attachment of microcomputers to television brings a vastly increased intelligence to the interaction possibilities on two-way systems. Moreover, a home computer, complete with screen using public or private telephone lines, can provide interactive facilities with a service provider without the need for a traditional television set.

ii. The provider

Bearing in mind that the phenomena under discussion do not necessarily require the supply of a service (for example the provision of information or the conclusion of a

contract via teleshopping, etc.) since it is possible for the user himself to directly provide information (for example in response to an electronic opinion poll over a specially adapted television set with a keyboard or other suitable terminal), the provider may be public or private entities furnishing information from public or private data bases, retailers, banks, cable television companies, etc.

iii. The carrier

The carrier is the telecommunications link between the user and the provider (he may even be the provider). He may be public or private, or, as in certain economies, private with a degree of public control. The telecommunications link can be effected in a number of ways, using public or leased telephone lines, by public or private cable or by satellites.

4.2. The situation in member states and actual or proposed regulation

An analysis of the situation in various member states of the Council of Europe allows the following picture of the use of interactive systems as well as the relevant regulatory framework to be drawn.

Austria

There are systems for data traffic between a subscriber and a data bank and in particular videotex (which in Austria is installed as a public videotex service). However, it should be pointed out that the videotex system in Austria is still in its test phase; concrete preparatory work has, however, already been carried out for the elaboration of a law on videotex Which Will create data-protection provisions and which is to form the basis for the organisation of the videotex service.

The Austrian videotex service is partly organised in an anonymous way which avoids the storage of personal data.

In Austria the term "interactive media" also covers private auxiliary devices (terminals and modems) applied to telephone lines, by means of which the subscriber can get access to data banks via the existing *public* data networks making use of the *public* telephone network and private terminals.

Belgium

The RTT interactive videotex service was inaugurated on 27 March 1986. Belgium has chosen to give priority to developing professional videotex. The first phase of the videotex service will be accessible by means of 300 gateways providing services for between 3 000 and C:) 6000 users. An extension to 600 gateways giving a total capacity of between 6000 and 10000 users is planned.

A ministerial circular laying down conditions of use and tariffs is under preparation and should be published shortly. The following principles will no doubt be incorporated in

this circular.

- the supplier is responsible for the content of data;
- the RTT assumes responsibility as carrier;
- the RTT also provides invoicing services and keeps the necessary data on file for approximately six months.

France

What was originally introduced as a system to promote the electronic telephone directory, Minitel, now offers a whole range of interactive services (home banking, home shopping, access to data banks, games, etc.) carried through the PTT public monopoly. The Minitel terminal allows the user to access remote databases to obtain services through gateways provided by the Transpac packet switched network. The user may also interface overseas databases via Telenet to which he may be connected via the PTT-controlled international gateway.

The Act of 6 January 1978 on data processing and freedoms and the Act of 29 July 1982 on audiovisual communication provide a regulatory framework for the data-protection problems raised by the interactive media.

The CNIL has played an influential role in focusing the PTTs attention on the need to address the issue of data protection. As a result of the CNIL's decisions, the PTT has had, for example, to introduce data-protection regulations concerning itemised call statements and call-recording devices. In the case of interactive videotex, flat rates have been introduced ("kiosque system'] to ensure confidentiality.

Federal Republic of Germany

A videotex system *(Bildschirmtext)* has been in use since June 1984, the services being carried by the public monopoly, *Deutsche Bundespost,* to users with specially adapted television sets or home terminals. In addition to providing tens of thousands of pages of retrievable information, *Bildschirmtext* also offers a wide array of transactional services by allowing the user access to remote databases through gateways in the network. The present telecommunications regulations in the Federal Republic of Germany impose an obligation on the *Deutsche Bundespost* to protect personal data in the *Bildschirmtext* system. The regulations stress that "the right to be informed of personal data, to have personal data corrected, blocked or erased shall be asserted in relation to the information providers concerned or the subscribers". A more comprehensive scheme of data protection is envisaged. The Federal and state data-protection laws also provide a regulatory framework, as does the Treaty on Interactive Videotex between the *Länder* and the Federal Government.

Ireland

There are systems in use and others are planned especially in the area of videotex in both the private and public sector, for example:

- *Agrilive*, providing information to the farming community;
- *Cognotec*, providing financial information;
- *Patric*, providing library and environmental information.

In addition, nearly all internationally available interactive systems or live databases etc. are accessible by users in Ireland. There are no special data-protection regulations. Ireland enacted data protection legislation in 1988.

Netherlands

There are a great number of projects presently functioning in this field. For some years now the PTT has been offering an interactive videotex service (Viditel) using the PTT telecommunication network with special videotex facilities. This service is intended for the public a well as f or closed user groups. Aside from Viditel, there are dozens of closed videotex services and a few private teleshopping services. Various types of information, reservation and teleshopping services are now available in Limbourg in a large-scale experiment with two-way cable facilities.

The introduction and use of these services did not require special regulations. Legal protection is afforded by statutory and contractual obligations, for example the provisions in the Viditel contract on the confidentiality of information concerning users.

A Data Protection Law was finally adopted in December 1988.

Norway

Interactive media have been introduced in some fields in Norway, for example a legal database covering all the laws, all statutory regulations and summaries of decisions from the Supreme Court. This database is open to the general public but, of course, is mostly used by lawyers and public bodies. Some newspapers and news agencies are now offering their electronic archives to the public. They have to obtain a licence from the Data Inspectorate to do so. The Data Inspectorate has set rules in this connection, for example that certain kinds of information shall not be available after seven years from the year of publication.

Norway also has some videotex systems. The Telecom Authority Service has recently opened its videotex system to the public after a long trial period. It is too early to say how widely used it will be. Another system is planned by a credit information firm in co-operation with a bank. They want to offer credit information, economic information and a news service to subscribers. In addition, some of the largest papers are planning to set up systems and offer news and other information, such as company information, to their subscribers. Some data-processing companies are also interested in accessing this market.

There is, apparently, great activity in this field in Norway at present, but most of the systems are only at the planning stage, and it seems that many of them will not have been finished by the time expected. It is necessary to wait and see how many of them will be operational in the future.

Although no special legislation has so far been passed, to some extent these subjects are covered by the Act relating to Personal Data Registers, etc., of 9 June 1978, administered by the Data Inspectorate. This Act concentrates on personal registers and covers the services in question when personal registers are involved.

Spain

A videotex system (Ibertex) will become fully operational in February 1987 using the telecommunicational infrastructure provided by the Spanish national telephone company *(Telefónica).* Plans are under way to deregulate *Telef6nica,* Apart from setting up the circuits' and maintaining them, *Telefónica's* sole intervention will relate to the invoicing of users for their use of the telephone or the Iberpac network when they avail themselves of a videotex service. The Association of Videotex suppliers has agreed to guarantee, *inter alia,* "the confidential nature of data and privacy of users".

Sweden

The number of users of videotex is increasing in Sweden. The fastest increase is to be found within enterprises but in households also videotex is becoming more and more common. Many banks have now introduced quite complete telebanking via videotex. At certain post offices, there are now also data terminals for ordering theatre tickets, and so on. Otherwise, interactive media are probably not used by individuals to any large extent. On the other hand, there are a number of information agents who, with videotex, are functioning as 'electronic errand boys". Generally, an agent can provide information from different sources according to the receiver's own choice.

No special regulations have as yet been drawn up. The collection, storage, use, etc. of personal data through videotex are covered by the data-protection legislation.

Switzerland

The main interactive system used in Switzerland is videotex, but remote interrogation of a database can also be carried out by telex. In addition, the *Telepac* medium service gives any user of this service the possibility of a dialogue with databases, if he has the right terminals. *Telepac* therefore provides a medium for interactive systems. The PTT provides the necessary technical infrastructure. As a rule, the databases are in private hands. Videotex is the subject of a separate legal instrument which, however, contains no specific data-protection provision. The proposed data-protection legislation will probably contain no specific provision on videotex either.

United Kingdom

British Telecom offers a videotex system called Prestel using specially adapted television sets or computer terminals linked via a telephone to a data base which can provide homebanking services, travel reservations, theatre reservations, teleshopping, access to specialist data banks, etc. There are no special data-protection regulations for videotex other than the general data-protection principles laid down in the Data Protection Act. British Telecom, a private carrier, is subject to regulatory control under the Telecommunications Act which imposes requirements to safeguard the confidentiality of information carried between the user and the provider.

4.3. Specific data-protection problems and possible solutions

From the point of view of data protection, concern has been expressed about the possible secondary uses which can be made of the personal information which the individual releases each time he makes use of an interactive system. It is a feature of interactive systems that they create personal data through their use, for example that X bought a certain item, watched a particular film, transferred a certain amount of money, played a particular electronic game, responded in a certain way to an electronic opinion poll, etc. The information is carried through the telecommunications link to the destinatory so that the requested service can be provided. The data released by the user are stored by the service provider for services and billing purposes. The carrier also will store information on the user for billing purposes (for example time spent on communications link, service number called, etc.). When the carrier is the manager of the data base or the service provider, which is often the case with public videotex systems or cable operators, an information-rich file will be located in the hands of one entity. In other words, the information flow pattern in the network tends towards one of registration and it is at this level that data-protection issues arise. The risk is that the data collected for a particular service purpose will be put at the disposal of third parties to be used for entirely different purposes. In other words, commercialisation and misuse of the personal information created through use of the system are possible and the secondary uses which are made of the information may take place without the user's knowledge.

The issue becomes more complex when secondary use is discussed in terms of individual profiling. A computerised image can be drawn of the user, building on his disclosure to the system of his tastes in literature, consumer products, films; his intelligence may be gauged through his participation in electronic puzzles, etc. The profile is a marketable commodity in itself but the element of surveillance or control of users which such a technique permits is perhaps a more alarming possibility. Bearing in mind what was stated in the discussion on telemetry regarding the possibility of remote sensors being attached to interactive television systems, a more complete control is possible via interactive television since the movements of the user will also be stored in the system (when he leaves his home, when he returns).

Whether the carrier is a state-controlled body or a privately run enterprise adds another dimension to the problem. Although, in either case, data will be collected for billing

purposes, it should be borne in mind that the bill is made up on the basis of an identifiable individual calling up particular identifiable services on particular occasions for certain lengths of time. A close link between the carrier and the administration tends to heighten concerns about the surveillance possibilities of interactive systems.

The user is what will become the unwitting generator of "the single largest repository of personal data in the history of the world" (Flaherty). As he is not fully appreciative of the informational consequences through use of interactive systems, a problem arises as to the fairness of the datacollection procedures. What does he consent to when he releases data? How can he express consent? How can he follow up the use made of his data? The problems relate to the lack of transparency in the systems in the sense that the activities and responsibilities of the different actors involved are not clearly identified - the provider may also be the carrier, collecting and processing data for services provided and billing. The user's information may generate the creation of several "files" - called data file, accounting data file, a customer request file. Who manages which file and for what purposes? The lack of proper articulation of the rights and duties of the various actors involved prevents the user from effectively controlling the use made of his data.

A comparative analysis of the various approaches hitherto taken for resolution of the data-protection problems caused by interactive media suggests that a national data-protection law may not be a sufficiently effective instrument *Per se* to deal with all the problems. There is nevertheless consensus among lawmakers that, insofar as interactive media give rise to the collection, storage, and processing of personal data, the general norms and supervisory powers of the various control organs contained in domestic data-protection laws will apply. The success of the supervisory body in controlling abuse in the context of the interactive media will depend to a large extent on its capacity to adapt the general principles of data protection to the particularities of interactive media.

There are of course problems linked with this approach, not the least being that many laws, especially those passed in the 1970s, were never designed with interactive media and the accompanying problems in mind. This is of course true of new technologies in general.

It would therefore seem desirable to deal with problems of interactive media by way of a sectoral approach. Videotex, for example, has already been the subject of separate regulation (that is, outside the framework of general data-protection legislation) in the Federal Republic of Germany. Experience shows that it is possible to find particular solutions, based on general data-protection principles, for the specific problems identified above. Drawing on North American and European examples (particularly that of the Federal Republic of Germany) in the field of videotex, it would seem to be the case that new regulatory initiatives should concentrate on the following issues:

i. the consent of the user prior to installation of videotex technology in his residence;
ii. only personal data which are necessary for billing purposes or service purposes should be collected and stored;

iii. the sale or disclosure or further use of the data should only be possible with the informed consent of the user or if authorised by a legal provision;
iv. the security and confidentiality of personal data which have been recorded should be guaranteed, for example by means of encryption techniques, smart cards, password variations, flat rates;
v. strict conservation periods should be laid down;
vi. user rights (access. deletion and rectification) should be provided for the user who should be informed of their existence and shown how to exercise them;
vii. the general data-protection legislation, where such exists, should provide the overall regulatory framework.

As regards the method of implementing these principles in member states, recourse to specific legislation may seem the obvious course of action. However, borrowing on experience in the Federal Republic of Germany, it may also be possible to integrate the principles into the general legal framework for regulating telecommunications.

It has, in addition, been noted that self-regulation has a role to play in the scheme of things. The North American experience, in particular, illustrates the possibilities available to the videotex industry in the private sector to bind its members by codes of conduct/practice. This approach, it is suggested, has much to offer in the deregulated environment of interactive cable television. However, it is felt that self-regulation should be viewed as a possible complement to existing data-protection legislation and such initiatives should take account of this wider framework. In this regard, it may be the case that the supervisory organs, established pursuant to data-protection legislation, can themselves act as the final arbitrators of the efficacy of proposed codes of conduct.

There is possibly an intermediate stage between regulation by law and self-regulation and, once again, the alternative is offered by the practice of certain American states. Although not appropriate for public sector videotex, contractual or licensing control of service providers and carriers in interactive cable television industry could be envisaged at the time of granting public authorisation to operate a cable television franchise in a particular region.

Finally, in addition to the proposals mentioned above, a totally different, more elegant solution to these data-protection problems should be more closely examined: videotex technology allows the user's resort to services, data banks, etc. to be carried out anonymously so that no personal data are stored by the service provider or by the carrier. In this way, many of the known risks are avoided from the start. This system has, for example, already been installed in Austria for access to free-of-charge services via videotex (BTX). In future, the further development of the smart card should make possible the extension of anonymous videotex to access to pages subject to a charge. It would be conceivable for statutory provisions to make the application of this new technology mandatory as soon as technological progress permits.

5. Electronic mail

5.1. Service featuresltechnical characteristics

The term "electronic mail" is relatively clear and does not require a detailed description. It involves Arnbak's conversation model of information flow (exchange of information between individuals) characterised by the equal status of the participants.

Taking a broad approach to the definition, electronic mail systems consist of a terminal and a keyboard capable of transmitting coded messages through the telephone network to which the destinatory/ies is/are connected. Other services may be included: the electronic letter box in which the receiver will find messages which have been sent and stored; the electronic filing of messages which have been sent or received throughout a given period.

Electronic mail systems may also arise from the transmission of telephonic messages (voice mail).

Videotex systems as described in the previous chapter may include a form of electronic mail.

5.2. Situation in the member states and actual or proposed regulation

The majority of member states of the Council of Europe have developed electronic mail systems, both public and private. For the time being, these systems are of more concern to enterprises and administrations as the traditional postal system still presents guarantees of confidentiality as well as incomparable tariff conditions. Two types of electronic mail may be distinguished: internal mail within enterprises which use their own internal networks; and mail between enterprises using the public service facilities (which is the case for the majority of European states) or which use the services of a private carrier.

In Belgium, a public system of electronic printed mail was started in May 1985. This service is exploited by the RTT which enjoys a monopoly in this field. A ministerial decree has fixed tariff arrangements. Moreover, electronic mail systems have been set up in different ministries (Bistel).

In the *Federal Republic of Germany,* experimental services in electronic mail (Telebox) and in the transmission of telephone recordings *(Sprachspeicherdienst)* have been instituted. Regulations concerning these services are now being prepared. In regard to the Telebox service the proposed regulation envisages that each receiver will be protected by an alphalnumeric password (from six to thirty letters). Messages which are particularly confidential may be protected further by a specific password of up to twenty characters. On each occasion when the user accesses the service, the system reproduces automatically the date and time of the last access in order to inform the user about a possible unauthorised access. After three unsuccessful attempts at access to a box, the system automatically informs the user so that he can avoid further attempts (for example by changing the password). In regard to the voice mail service, protection against unauthorised access to the voice mailbox *(Sprachbox)* is assured by the following

measures: station identification of seven characters; individual password of up to eight characters.

In *Ireland,* Telecom Éireann (the national telecommunications board) offers an electronic mail facility in its packet switched network. In addition, the national postal service has been providing an electronic mail service since the end of 1986. If desired. the electronic output can be printed out in hard copy and delivered by the postal service.

In the *Netherlands,* the PTT has launched a public service for electronic mail (Memocom) using the existing telephone and data networks. In addition, several private companies have their own internal systems for electronic mail. The possibility of introducing such a system for central government is being considered. In the Netherlands, communication via telephone or telegraph is protected by the Constitution. Data communication is covered by provisions in the Datanet Order of 1982.

In the *United Kingdom,* there is widespread use of both public and private electronic mail services. The best-known public service is British Telecom's Telecom Gold which, as well as providing the basic facilities for message transfer and storage, also offers telex and gateways to videotex services. Telecom Gold is undergoing a rapid expansion, doubling its customer base every year. Many large organisations in both the public and private sectors also operate private electronic mail systems, some of which have links to international networks.

5.3. Analysis of the data-protection problems

The data-protection problems do not differ fundamentally, depending on whether one is dealing with internal enterprise mail or external mail using the ordinary telephone network (which is the case for the majority of European countries) or necessitating the use of the communication means offered by a carrier.

In both cases, it is necessary to prevent unauthorised access, ascertain the sender's identity, date the dispatch accurately and guarantee the integrity of the content of the mail. The laws of evidence and proof have been discussed in this context. However, it seems that this problem is no different from the problems which are posed by the other information technologies (proving the identity of the user and the receiver, proving the content of the message. the value of any acknowledgement of receipt which has possibly been delivered, etc.).

In regard to security, the question of the management of passwords has also been discussed. Some commentators have stated that it may be dangerous to leave the freedom to choose the password to the user. Experience shows that a user will generally choose something which can be easily put together by third parties. The need for providing information to users as well as educating them in the use of the system therefore seems desirable.

Messages circulating in an electronic mail network may contain all sorts of data which may be the subject of a file. The possibility of conflicts between different applicable laws has been emphasised - must messages in electronic mail systems be considered as letters to which the legislation concerning the secrecy of correspondence applies, or must data-protection laws be applied to them, since there is an issue of nominate data being held on a magnetic medium? The issue is important since data-protection laws offer a right of access to personal information.

It may however be possible to regard the message as a letter and, as such, confidential. The person transmitting the message is master of its contents and may include in it personal data concerning other persons if he so wishes. If, for reasons of archiving or whatever, these messages become the subject of a file, the provisions of data-protection legislation with regard to access or rectification cannot be applied to such files without putting at issue the right to respect for the secrecy of correspondence guaranteed by Article 8 of the European Convention on Human Rights. The fact that the message is sent electronically by no means alters the principle of secrecy of correspondence. The problem resides elsewhere - guaranteeing, first and foremost, the security of messages.

The need to define the liability of the controller of the network seems necessary. At the present time, it does not seem to be the case that existing laws make it possible to engage the liability of the controller of the network, with the exception of certain countries, in cases of very serious fault. The controller of the network must guarantee the confidentiality and security of the messages.

Finally, in the majority of countries the traditional mail service benefits from secrecy guarantees laid down by law. In the context of electronic mail, this guarantee is no longer clearly defined. It would seem important for the PTTs to offer electronic mail systems the same guarantees as are accorded to traditional mail services. The improvement of security is a condition for the development of these services and, in particular, their development at the domestic level.

It may be deduced from these considerations that two points seem essential in the field of electronic mail.

1. respect for the confidentiality of messages which must be guaranteed by the law in the same way as for the traditional postal system;
2. the development of technical measures so as to guarantee better security of the messages. Among such techniques, the following may be mentioned: automatic dating, message sequencing, coding and the dispatch of acknowledgement.

6. Common considerations for data protection

Each of the technologies discussed presents a range of possible data-protection issues. Are existing data-protection norms capable of responding to them. or are the concepts on which they are based linked to a previous technological era which prevents them from

effectively dealing with the new problems? Given the influence of the provisions of the Data Protection Convention on the elaboration of data-protection norms (and it itself was influenced by the approach of the legislator in the 1970s), it is interesting to test the continuing relevance and validity of the concepts and terminology used in the Convention against new problems and issues. While the analyses set out in the preceding chapters of this report are aimed at specific issues and the presentation of comparative experience in addressing those issues, the thrust of the present chapter is directed more at assessing the overall impact on the normative framework constructed for regulating automatic processing of personal data.

The conclusions to be drawn from this exercise should not be seen as specific to interactive media, telemetry and electronic mail systems and of no relevance to other technological applications beyond the frontiers of the primary examples. On the contrary, legislators are invited to reflect beyond the concrete examples and examine telematic applications not referred to in this report - for example, teleworking, word-processing systems, smart cards, expert systems, etc. - which create increased possibilities for the processing of personal data which are collected and stored as a necessary consequence of individual use of a system or of control by a system. By way of illustration, although data security and confidentiality are discussed later from the point of view of the problems posed for the implementation of Article 7 of the Data Protection Convention in the context of telemetry, interactive media and electronic mail systems, the issues raised are of relevance to personal data in general which are transiting through or stored in networks regardless of the technology used. Similarly, the challenges outlined to the basic principle of data quality, contained in Article 5, should be seen as having a wider application beyond the specific examples and solutions described.

It is worthwhile recalling at the outset the conclusions reached in Chapter 2 in regard to technological trends: the banalisation of computer technology making it possible for more and more people to be directly concerned by these issues, for example as service users; the trend towards distributed processing systems; the vastly increased possibilities for data transmission, file interconnection', the multifunctionality of networks.

1. Article 2.a of the Convention - The definition of personal data

At the very least it can be said that the amount of personal data in circulation has increased dramatically. In accordance with the findings of Chapter 2, telemetry, interactive media and, to some extent, electronic mail systems have been domesticated, allowing more and more personal data to be collected and stored via data-processing systems. The information stored will in great measure concern the individual as a consumer of services - the amount of energy used by a given householder, the time spent on a telecommunications link, etc. Relating the data to 'an identified or identifiable individual'' is therefore relatively problem-free. An issue does possibly arise at the level of collective use of a telematic service, typically a family household, where the information collected and stored reflects group activity. For example, the shared use of a password for access to electronic mail or videotex among the members of a family or registration of household energy consumption will result in a storage of data which

emphasises group activity at the expense of individual use and makes it difficult for the individual user to "locate" his personal data. At one level, this is a consumer-protection issue, perhaps resolved through the technique of itemised call bills in the case of videotex and electronic mail. At another level, a privacy problem is posed in that the individual is unwittingly linked with the behaviour of the group to which he belongs. There is an added dimension to the problem - the rights of the group itself. The aggregated data on the group may prevent identification of its constituent individuals but, to the extent that data stored on the group may be used to take decisions or make value judgments which ultimately affect both the group as a whole and, necessarily, its members, an issue arises as to the desirability of including, within a scheme of data protection, group privacy recognition. However, it may very well be the case that such an issue does not put in doubt the Convention's definition of personal data. Rather, such problems should be analysed in terms of the means used to collect data, the reasons for collection, the use to which the data are put, etc.

The notion of an identifiable person may also be undergoing change. The Convention did not intend to cover identification of persons by means of very sophisticated methods. However, what constitutes a sophisticated method is relative to the state of technology. In brief, what may not have been technically possible in the 1970s may be possible today. And with the efflux of time it will no doubt be the case that greater possibilities for identifying individuals from the anonymous mass will emerge.

Furthermore, the question may be asked as to the extent to which the Convention's concept of 'personal data" takes account of new possibilities for storing and processing pictures, sounds, voices, etc. When telemetry makes it possible to digitalise and store pictures of car drivers entering a city centre, or of customers in a bank queue, or when electronic mail systems allow the human voice to be stored automatically, it is possible to appreciate the many different forms personal information can take and the corresponding need to regard it in as wide a light as possible. Once again, the flexibility of the Convention definition should be seen as capable of dealing with these types of problems. This said, careful reflection is required before drawing the conclusion that, since automatic processing of personal data is taking place in a given context, the data-protection system is thereby invoked to the exclusion of other considerations. It may occasionally be instructive to consider the limits to what constitutes personal data for the purposes of including certain processing activities within the regulatory framework of data protection. For example, taking up an issue already discussed in Chapter 5, it is possible to analyse electronic mail systems in terms of the automatic processing and storage of personal data concerning identifiable individuals. However, the point of departure for resolving problems arising through use of electronic mail systems may quite possibly be found in traditional notions of secrecy of correspondence, confidentiality of the mail, unauthorised interception, etc. rather than in the concept of data protection.

2. Article 2.b - The definition of an automated data file

The concept of an "automated data file" is seen as being of central importance in the scheme of data protection. It is viewed as contributing to transparency and control of

automatic data processing insofar as its existence can be made known to the data subject, thus enabling him to exercise his rights of access, rectification and erasure. It may be, however, that the notion of a file, as used in the Convention, suggests centralised storage and processing and is not in keeping with the new reality of distributed processing and networks which allow data to be dispersed and yet linked up at will through the possibility of computer-to-computer, or terminal-to-computer, dialogue. If a data file is divided into several sub-sets of data, an unacceptable burden is imposed on the data subject who is obliged to piece together the various pieces of the puzzle, including the unravelling of the network. before it may truly be said that he has had access to his data. Effective exercise of subject access, in reality, breaks down, individual control over data processing is weakened and transparency is diminished.

This result could be typical of any organisation which operates through a local area network with different people in the organisation retrieving and processing personal data at different parts of the network. The public utilities which were referred to in the context of telemetry, electronic mail and interactive media - the PTTs and the various energy authorities, for example - may correspond to such a description of distributed data processing. Accordingly, it may very well be that within a PTT one data file containing call data and billing data will be difficult to locate. Rather, a series of files representing the different uses made by the user of telephone lines would need to be linked up before the sum of personal data stored by a PTT on a particular individual is known.

It would seem necessary to proceed to an examination of the need to be able to establish the existence of what may be termed a "logical file" which allows for ultimate location, through retrieval methods, of all the data dispersed in a network in the context of legitimate storage and processing within any given organisation. Nor is transparency any longer assured simply through knowing of the existence of a file. It would henceforth seem desirable to render transparent the influence of the network on data-processing operations.

Electronic mail systems, as suggested previously, have special characteristics. It is, in particular, inappropriate to regard digitalised messages waiting in the system to be picked up by a recipient as "data files" ' given their unstructured nature. While this conclusion may not be valid for call-data files, accounting-data files, etc. which result from the use of interactive media or telemetry, it does have relevance to technologies other than electronic mail systems - word-processing systems, for example, are distinguished more by their storage of free text than by structured sets of data. The difficulties which such a system poses for access rights are only too apparent.

3. Article 2.d - The definition of the "controller of the file"

This discussion is inevitably linked to the preceding reflections on data files. Distributed data-processing systems entail a decentralisation of control and responsibility and make it difficult to determine "the person or body ultimately responsible for the file". It will be recalled that the Convention premises the data subject's rights on the possibility of establishing the identity and habitual residence or principal place of business of the

controller of the file. Electronic mail systems immediately challenge the validity of this notion of file controller given the impossibility of extending the concept of "data file' to electronic messages. Nevertheless, it still remains essential to adapt the notion of file controller to take account of the new automated context posed by electronic mail systems, so that issues of liability can be resolved when something goes wrong in the system. If 'controller of the file' is found inappropriate, perhaps it would be more fitting to speak of "the controller of the network". Outside the context of electronic mail and other systems characterised by the conversation flow pattern, the notion of controller of the file can still assume validity if account is taken of the factors referred to in the analysis on automated data files. Accordingly, a distributed, decentralised processing system may still give rise to a person or body ultimately responsible for particular "files" if regard is had to the ultimate authorised user of the data - is it a PTT, a cable company operator, a service provider, or an electricity company? Even if the ultimate authorised user so identified - and for this reason it is essential that the roles of the various actors involved in any telematic service should be clearly communicated to the user - operates a distributed data-processing system, it should still be possible to regard him/it as in control of all processing operations in regard to a particular file and, in particular, as being the repository of the sum total of personal data located in a network - the so-called "logical file".

4. Article 5.a - The principle of fair and lawful collection

As the analysis of telemetry and interactive media shows, technology presents novel ways of collecting data. The individual generates data in response to a system rather than furnishing information in response to questions posed by third parties. His movements, his management of household energy, his physical presence, his use of a system, his dialogue with the system, etc. give rise to data - possibly not what was in mind when this principle was drafted. The principle is still relevant and valid, but its value may be diminished if it is seen exclusively in terms of placing a prohibition on deception or misrepresentation. Rather, it should be viewed as part of a wider principle of informational self-determination - the right of the individual to control the amount of data collected on him, to follow up the use made of the data, to remain at all stages aware of the different operations carried out on his data, etc.

Telematic systems, whether of the consultation flow model type (interactive media) or the registration flow model type (telemetry), are both characterised by the collection and storage of personal data irrespective of distinctions based on the activity or the passivity of the role of the data subject *vis-à-vis* a particular system. Although the analysis in Chapter 3 of data collection carried out telemetrically makes out a convincing case for making the passive data subject more aware of what is actually taking place, it is believed that a similar need for transparency exists in regard to user systems. Both telemetry and interactive media raise common problems - increased possibilities for surveillance and control, an unauthorised secondary use of data and varying degrees of individual appreciation of what is taking place.

To make the principle of "fair arid lawful collection" relevant, two ideas should be canvassed: transparency and consent. These notions may be seen as complementary and may perhaps be better translated as "free and informed consent of the data subject". The notion finds concrete expression in the requirement to seek the consent of the individual before the installation of technology in his home, the furnishing of information on what is taking place when the technology is operational, the provision of information on the data collection potential of the technology, etc.

What constitutes a fair and lawful collection procedure will of course depend on the processing context. As illustrated in Chapter 3, telemetry has applications outside the home. Video surveillance of crowds, for example, will make it difficult to apply a notion of "free and informed consent". In such cases, it may be more appropriate to seek a solution based on the need for specific legal provision to exist before data can be so collected. On the other hand, in the employment context, the collection of data on employees through use of telemetry could be made conditional on the free and informed consent of the employees.

5. Article 5.b - The principle of purpose specification

In the field of telemetry, data are essentially collected for billing purposes. It has been seen that telemetric systems currently in existence mainly concern the remote reading of water, electricity or gas meters. The data stored should therefore relate to a particular person (name, address, bank account, etc.) as well as to his energy consumption. In this regard, it has been seen that the frequency of the storage of data on energy consumption could represent a danger for the privacy of the individual. In Norway, for example, it is proposed to read individual meters every six minutes. Such a practice could bring about an almost police-like surveillance of individuals. Does the purpose of processing - the reading of gas, electricity or water consumption - justify such frequent data storage even for the purposes of internal management? Accordingly, it seems essential that, at the time of installation of a telemetric system in an individual's household, the latter should be informed both of the frequency and the time of data storage.

When surveillance systems ate at issue, whether installed in a particular home or at a place of work, it is important that the data stored should be erased within a reasonable time. Such systems are installed for security reasons and the data stored must not be used for other purposes - for example, for the surveillance of individuals at their place of work.

In regard to the remote reading of water electricity or gas consumption, the possibilities for secondary use of the data seem minimal. Internal use of the resultant data could be accepted, for example for the purposes of management of the service or utility. However, if a public service is involved, the data should not be communicated to services other than the service in question.

As regards remote surveillance, the risks of secondary use are greater and it is therefore important that the finalities involved should be clearly specified and respected. No

secondary use of data resulting from such a system should be possible.

Finally, in the field of telemetry in general, a maximum storage period should be envisaged.

It is certainly in the field of interactive media that problems relating to the secondary use of data mostly arise. Two types of data are collected and stored - data allowing bills to be drawn up for services provided and data which have been disclosed to the system and stored at the time of consultation of the service requested by the user. It is the latter type of data which may reveal the preferences and the habits of individuals and which are susceptible to secondary use. Other service providers could very well be interested in having such data for commercial reasons. At this juncture, it may perhaps be appropriate to distinguish between the carrier and the provider of a service. As regards the carrier, appropriate security must be guaranteed by him when data are being stored and transmitted. The only data which the carrier may collect and store should relate exclusively to the drawing up of the bill for the service rendered, namely the relaying of the information. As for the service provider, he should refrain from communicating to unauthorised third parties the information acquired by the user as well as the questions which the user has asked of the system. The sale of such information or lists of names should be regulated. The free and informed consent of the individual should be envisaged, the notion of "informed" implying that the individual must know exactly what he is taking on by accepting that his name may be disclosed to other service providers. If it proves impossible to obtain such consent, the communication of data to third parties should be regulated. However, over and above regulation in this area, the legislator has other possibilities at his disposal and notably technical possibilities. For example, it has been seen that, in France, the *kiosque* system (flat-rate billing) makes it possible for a user to access data anonymously. Only the time spent by the individual oil consulting a service is reckoned. Anonymity is respected in regard to the type of information consulted. A certain number of problems raised above are thus resolved. The only issue left untreated in this context is the security of transmission, and this will be taken up later.

If the principle of finality as defined by the Convention remains as valid as ever in the context of the new technologies, it seems necessary to strengthen it with additional guarantees as far as interactive media are concerned, given the fact that it is impossible to control respect for finality effectively in the light of the amount of data collected and the proliferation of services which they offer.

6. Article 5.d - The principle of accuracy

It is important to ensure that data carried in a videotex system or in electronic mail systems are not distorted. The transmission of inaccurate medical data, for example, could produce serious consequences. Accordingly, measures should be taken to guarantee a good and proper transmission quality. The problem of accuracy is also posed at the collection stage. In all cases, it seems important to allow the individual the possibility of seeing the data which have been collected on him.

In addition, the accuracy of profiles drawn up on the basis of information collected at the time of consultation of a service by an individual may also warrant consideration. To deal with this problem, reference should be made to the issue of the purpose of collection in the context of the interactive media. It has been shown that the service provider could have a legitimate interest in using data for his own purposes (management purposes or sales policy purposes). it could also be envisaged that the service provider will establish profiles for such a purpose. In no case should the establishment of such profiles be allowed to make judgments on individuals. The transmission of such data should also be accompanied by appropriate guarantees - the free and informed consent of the data subject or, if that proves impossible, legal authorisation.

The carrying out of opinion polls by means of videotex should be accompanied by additional guarantees. It is important to ensure that such information is not divulged for political purposes. Once the poll has been carried out, the data should be erased and the choices made by individuals should be kept secret.

Insofar as the principle of purpose specification at the stage of collection and use of data is respected and communication of such data to third parties is carefully regulated, the creation of profiles on individuals cannot really represent a danger for them. Profiles only constitute a fragmented view of individuals for the service provider. The systematic communication of such data to other providers could, on the other hand, represent a danger for the data subject.

7. Article 7 - Data security

Data security constitutes a key problem for all the three technologies studied, regardless of whether or not one is dealing with interactive videotex, electronic mail or remote surveillance of a particular house. Even if the collection, use or communication of personal data are circumscribed with all the necessary safeguards, such safeguards are of little or no use if it is possible for a person to penetrate the network and access the data. This is a crucial problem and users are not always aware of it.

At the present time, different techniques make the physical protection of processing centres possible: protection against electricity failure, protection against fire, control of access or trespass. It is principally this latter type of access which will be examined in regard to the three technologies studied. Access control or prevention of trespass, the object of which is to restrict access to data processing or transactions, can be carried out by means of identification of the correspondent or user. Such identification can be accomplished at four levels: identification of the line linking the terminal to the computer, identification of the terminal, identification of the subscriber or operator (the latter may be authorised by the subscriber to use the terminal). Controls generally consist of the verification of a code, of a password, of a reply to a personal question or of the contents of a magnetic card. Such methods are the ones which today are most frequently used and are carried out by a central system - for example by the service for which access is requested. A study carried out by the Commission of the European Communities on security techniques and data protection shows that such controls are not as reliable as the

controls which are carried out at local level, that is to say by means of the terminal itself and not by the central computer. In the case of centralised control, the individual who requests access is already in communication with the system in the course of the identification procedure. The identification procedure may be imperfect and may make it possible for a user with wrong motives to access the service requested.

Identification may also be necessary for reasons of proof whenever a transaction is carried out. As a result of the imperfections in the identification methods described above, other methods have been developed or are now being developed: verification of signature, voice recognition, fingerprint recognition, as well as other methods involving palm recognition and iris recognition. Smart cards may also be cited. The smart card will undoubtedly be the subject of important developments in the future, constituting as it does a sure and confidential means of identification.

As regards videotex and electronic mail, it is equally necessary to protect the data which are carried along communication lines and which are stored on data-processing media. Among security techniques for such systems, the following may be cited: the coding of the information. cyphering techniques and encryption systems.

For electronic mail systems, it also seems important to have the possibility of keeping track of all transactions carried out in the network - identification of the sender of the message, identification of the recipient, number of the message. date and time of arrival, number of pages, etc.

It may be concluded that, if the problem of computer security is not new, it already having been an issue of concern for the drafters of the Convention, it cannot be denied that it has gradually assumed primary importance with the development of technology and the penetration of data processing into the household.

8. Article 8 - The rights of the data subject and article 10 – Remedies

Data-protection legislation envisages the declaration or authorisation of all personal data processing as well as the exercise of access and rectification rights in regard to processing. However, it has been seen that the exercise of these rights cannot be effected as such as far as electronic mail systems are concerned, a field involving respect for the secrecy of correspondence. But, in the context of electronic mail, a remedy for the individual should nevertheless be envisaged, for example where there is a mistake in the communication of the message. It has been shown that, at the present time and particularly in the public sector, the carrier will only be liable for very serious faults. However, this problem of transmission error may perhaps be resolved at the level of security. There exist technical measures which aim at avoiding this type of error, in particular by means of double transmission or automatic correction of errors.

Thanks to videotex, it is henceforth possible to have access to electronically stored newspapers. It becomes necessary therefore to envisage the possible extension of press laws (libel, the right of reply) to this new type of newspaper, or additional rules or

remedies for individuals should be envisaged. Interestingly, the new French law on the freedom of communication contains a right of reply.

9. Article 12 - Transborder data flows

If, as stated at the beginning of this chapter, the volume of personal data in circulation has dramatically increased, then it is certain that the amount of transborder traffic in such data has also increased and will continue to do so. The technological trends outlined in Chapter 2 make these conclusions inevitable. Accordingly, it may be expected that information flow patterns used in the report to distinguish between different technologies will increasingly be of a transnational character. Videotex, for example, now allows users to access data bases located in different countries. International carriers using satellites and fibre optics have vastly increased facilities for promoting electronic mail use and other technologies conforming to the conversational model. However, as the volume of transborder flow increases, the control possibilities diminish. It becomes much more difficult, for example, to identify the countries through which data will transit before reaching the authorised recipient. Problems of data security and confidentiality are heightened when data are piped through communication lines which traverse countries where little or no attention is accorded to issues of data protection. The transborder flow of sensitive data in particular becomes more acute.

In brief, when advanced communications networks enable businessmen on foreign travels to access their enterprises' data bases via hand-held computers plugged into sockets available in airports and to down-load data instantaneously into their computers across vast distances, the issue of national regulation of transborder data flows becomes problematic indeed.

The transnational character of data processing inevitably poses jurisdictional issues relating to the applicable law. The Convention is silent on the issue of conflict of laws. However, 'collision rules' seem desirable so as to resolve disputes in a transborder context. It may well be that a data file is stored in country A. the controller of the file is resident in country B, the data subject is domiciled in country C. Which law should apply if, through unauthorised access to the file, damage is caused to the data subject's interests in country D?

Access by a user to a foreign-based data-processing system may also pose problems for the extraterritorial application of the data-protection law of the user's country. Does the fact that the terminal allowing access is situated in country X bring the data-processing operations of the file controller, situated in country Y. within the scope of country Xs controls'? Or, alternatively, does the law of the country where the data-processing system is located apply?

7. Conclusion

At the outset, the point should be made that the Convention's principles have the value of generality. As with constitutional and international guarantees of human rights, the principles of data protection are set out in a manner which allows adaptation to evolving situations. It is suggested that the point of departure for the resolution of new problems posed by new technologies should be the broad principle, regardless of whether or not one is dealing with an issue of right of access, data quality, transborder data flow, etc. We recall that data protection is a fundamental human right, intimately linked to the right to privacy. The right to privacy itself, as guaranteed for example by Article 8 of the European Convention on Human Rights, is showing itself to be remarkably resilient in the face of technological threats. The European Court and Commission of Human Rights have both shown their willingness to apply the right to privacy to issues such as wire-tapping, file interconnection. unauthorised access to personal data - issues which were possibly not in the minds of the drafters of the European Convention on Human Rights.

Specific problems can, moreover, be the subject of specific solutions based on the general data-protection principles. This is the value of the sectoral approach to data-protection problems as actively encouraged by the Council of Europe since the opening to signature of the Convention. The recommendations hitherto adopted by the Committee of Ministers, for example in the field of scientific research and statistics (Recommendation No. R (83) 10) or that of social security (Recommendation No. R (86) 1), are attempts to interpret the Convention's principles in particular data-processing contexts. There is no reason why new principle-based initiatives cannot be found for the problems raised by new technologies. The analyses of telemetry, interactive media and electronic mail systems indicate that it is indeed possible to find a specific regulatory framework once the issues are correctly identified. In the absence of specific governmental regulation or self-regulation, it is believed that an enlightened approach to new technology-based data-protection problems, based on general principles, by those responsible for the implementation of data-protection norms can considerably diminish the possible risks to privacy.

As stated previously, constitutional courts at the national and international levels have shown themselves to be capable of interpreting the classic fundamental human rights so as to make them relevant to new changes in society. It may also be the case that the consultative committee, established pursuant to the Data Protection Convention, will also find ways to interpret the Convention's principles so as to ensure their continuing relevance in the technological age.