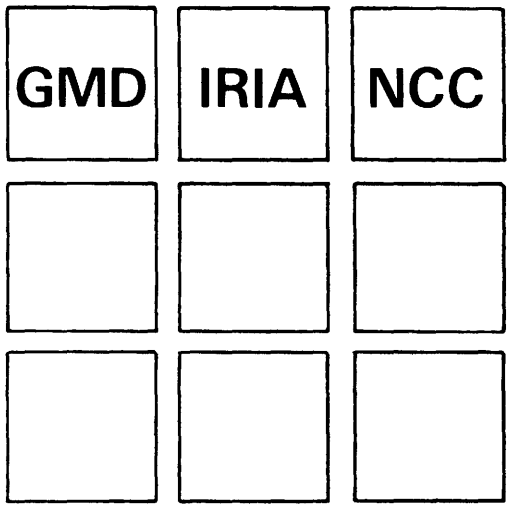


STUDY ON

DATA SECURITY AND CONFIDENTIALITY

FINAL REPORT

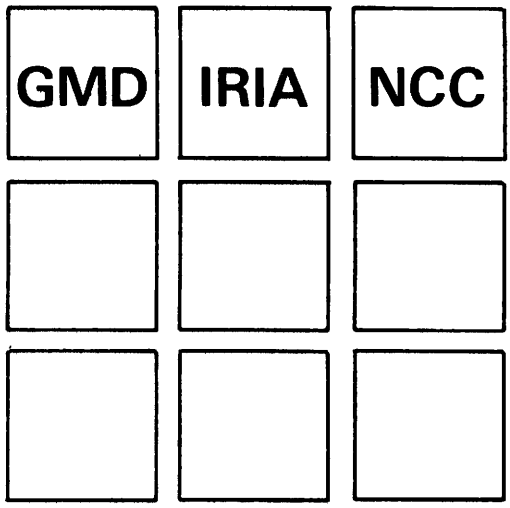
to the Commission for the European Communities

Volume 3 of 6

Section 3: The physical person/non-physical person problem

by F Bancilhon
J–P Chamoux
A Grissonnanche
L Joinet (counsellor)

JANUARY 1980



STUDY ON

DATA SECURITY AND CONFIDENTIALITY

FINAL REPORT

to the Commission for the European Communities

Volume 3 of 6

Section 3: The physical person/non-physical person problem

by F Bancilhon
J—P Chamoux
A Grissonnanche
L Joinet (counsellor)

JANUARY 1980

Contents of all volumes

Contents of section 3

3 The physical person/non-physical person problem

3.1 Introduction

Most European countries are now involved in implementing national policy for data protection, following the path marked out by Sweden since the beginning of the 1970s. In the German of Federal Republic, Austria, Belgium, the United Kingdom, for instance, the preparation of legislative tests to protect the confidentiality of personal data has opened up a wide public debate. When this debate is in progress, as in Belgium or in UK at present, one can state that it should consider two large categories of problems:

- on the one hand, the protection of private life and individual liberty of each citizen; the older laws were devoted to this protection alone, paticularly the Swedish law.
- on the other hand, protection of data connected with the activities and status of non-physical persons, ie associations of people; some such associations, in particular most companies, are recognized as legal entities. This second type of protection has also recently figured in the national laws, as in Luxembourg and Norway.

In fact, public debates on the protection of personal data only concerned the private area of physical personal (individuals) up until now. In the majority of countries where the question of protection of a corporate body's

files arose, this question seemed like a parenthesis to the protection of physical persons, particularly in the case of the technical preparation of draft laws, and the editing of text relating to the field of application of these laws.

Very often, for instance in West Germany and France, the national law-giver's decision has only been necessary at the end of a preliminary debate. In these two caes, the law-giver has declared himself in favour of the protection of physical persons alone, and based his thesis on the protection of the rights of man. The countries which have already had some practical experience in applying a data protection law have only taken into consideration the files of the physical person.

At the time when we are concluding this study, it is therefore not possible to balance the practical difficulties which could arise in the application of national laws like that of Denmark, who have recently introduced the protection of legal persons. Therefore our study should be considered as a departure point for analysis of this question, rather than an empirical fact. We hope to suggest a constructive way of approaching the problems, and analyse the protection issues clearly: on the one hand for physical persons, and on the other for non-physical persons. We hope thus to contribute to a more general awareness of these problems.

Among the laws which have at present been passed and have come into force, only the Austrian, Norwegian and Danish laws protect files containing personal data on physical persons and files containing data on non-physical persons in the same way. The other national laws, those of West Germany, France and Sweden only protect information on individuals.

The Luxembourg texts and the Belgian draft law have deliberately agreed with the first group of countries, treating physical and non-physical persons in the same way. Therefore it is clear that the national law-givers are becoming increasingly in favour of some protection for data on non-physical persons: the Lindop report, for instance, which recently indicated the directions which could be considered by the British law, underlined both: the necessity of separating the need for protection of individuals from that of associations; but also the need for proper protection for each of these two types of person.

Several working groups have considered the problem of this dual protection, either to sudy its economic basis, or even to consider the practical problems which a duel protection would give rise to. After long debates, which are still not finished at the time of writing this repot, the group of experts of OECD has chosen the negative, notably influenced by the American delegation, which stubbornly defended its position. The international instrument which could emerge from several months of work

by OECD, would be therefore a recommendation which would seek to protect only physical persons, for the American delegation is strongly opposed to the idea of including protection of non-physical persons in the same text, as it did not see the necessity for so doing. At the Council of Europe, on the other hand, a draft international convention is being prepared which could find a great following. The protection of physical persons would of course reamin central to the debate, as the Council of Europe is specifically directed towards safeguarding the rights of man. But a facility for extending the rules to the files of non-physical persons could be introduced into the convention, to take account of the decisions made in the national laws of certain countries, which are increasingly numerous in evisaging protection of non-physical persons and to also take account of economic preoccupations in this type of file.

This brief introductory balance sheet shows the topicality of the present study. The question is still largely open, as the countries which have proved protection for non-physical persons have hardly started to set in motion the necessary regulatory arrangements! In addition, professional circles still have varied reactions to this problem. Most of the multinational companies disapprove strongly the idea of any declaration of files, except in the case where these are strictly named files. At the same time, the wide survey conducted in the United Kingdom before the Lindop report revealed a certain agreement by small and medium sited companies

(thereafter abbreviated to SMC) that some protection of the files of businesses in the wide sense should develop. In the same way, the Federation of Swedish Industry, employers organisation, has just declared itself in favour of protection of the files of companies.

The problem which we must debate is thus topical, and the doctrine is not developed, neither on an international scale, nor even in the different European countries. The current research will add its own stone to the building, and contribute to the widening of the discussion.

3.2 Extension of protection to non-physical persons: view of the people concerned

The reactions of the persons concerned revolve around three factors:

* the legal status of the business,
* the size of the business,
* the public or private nature of the files of non-physical persons.

3.2.1 The legal status of the business

This factor essentially concerns only small businesses. For a variety of reasons, mainly tax reasons, these companies sometimes opt for the status of physical person (individual businesses such as grocers, butchers sometimes for the status of legal person. This difference in title very often arises as a pure legal device, without any direct connection with the type of

business they practice. This is the first cause of discrimination. The physical person business man can exercise his right of access in his position as a citizen profiting from a law which protects his private life. Therefore, he will gain knowledge of information concerning him which is stored in his bank's files. On the other hand, a non-physical person business man, carrying out the same activity, in the same client and business conditions, employing a staff of the same importance, etc ... cannot exercise such a right of access. Since the data about the business is recorded in a file for non-physical persons companies, the law does not apply.

From this point of view, justice itself encourages the exclusion of all discrimination and the extension of the application of the law to the files of non-physical persons. The objection that the right of access could risk unbalancing the rule of fair competition can only be considered with reserve, since, precisely, recognising a right of access only for business men as individuals, in itself produces an imbalance in competition.

3.2.2 The size of the business:

One observes a difference of reaction as one analyses, and this is the second factor:

- relations of large business with each other;
- relations between SMC (small and medium sized business) and large business.

3.2.2.1 Reactions of large companies in their business relations

Large businesses are usually unfavourable to data protection laws being extended to cover files of non-physical persons, at least with regard to their relations with each other. There is a fear that a skilful use of the right of access by rivals might favour certain industrial spying practices.

The general hypothesis put forward is that by a concerted comparison of the information thus obtained, certain parameters could be deduced, which would enable one to deduce the development strategies of the business in question.

The few laws in Europe which apply to the files of companies are too recent application (Austria, Denmark, Norway, Luxembourg) to let one assess the seriousness of such a risk. At present, to the knowledge of the people nationally responsible for data protection no such attempt has occurred.

However, one can consider that, in the near future, this hypothesis will reappear, but in different terms. Let us recall that the recent laws are attempting to make the files public, a developement inspired by the Council of Europe draft convention and taken up again by article 22 of the French law. According to this provision, the National Commission of Computing and Liberty must make the processing list available to the public, which

specifies, for each of them, 'the categories of named information recorded and the recipients or categories of recipients entitled to receive this information'. Even more than a hypothetical collection of information by people exercising the right of access for industrial spying purposes, a detailed analysis of this descriptive classification of a part of the files (information recorded/recipients) could be running the same risk.

Here too, a lack of perspective prevents the checking of the soundness of this hypothesis. Looking at it another way, it is equally true that certain information cannot be, because of its very nature, communicated to the non-physical persons concerned, without running the risk of relationships between businesses, being impaired particularly when management techniques for long term forecasting are used. The idea is this: certain firms, who have very efficient methods of processing information analyse, using the very detailed information on client companies or potential client companies, what will happen to the latter in 5 or 7 years. Some of these companies, will show a downward trend, perhaps disappear because of a merger, absorption into another company, change of business or closure. Thus one can understand the fears of the holders of these files, if one of their clients, having access to this type of information, were to become aware of his own downfall.

3.2.2.2 Reactions of large and small companies in their business relations

If large companies take up the same position in their relationships with the SMC, the converse is not true, clearly, for an obvious reason which the main responsible for a manuafacturing workshop summarizes: 'It is always the big who keep files on the small, and not the other way round!'

When one tries to define the position of those responsible for the SMC one notes:

- that there is certainly a wish (not really a claim) to obtain legal protection against being put on file;
- but this wish is largely motivated by the need to know; it is the right of access which is sought, rather than general protection;
- in addition, this need to know essentially concerns access to banks' files, files of 'payment problems' held in a syndicate by certain professional branches who keep information on the solvency of the SMC, which makes up their clientele.

An example will make this clever:
To raise the 'moral standards' of their clients, 30 wholesalers set up a common file of payment problems of their respective clients. The SMC featuring on this black list are potentially isolated, as competition between large companies only occurs with companies that

are always solvent. The lack of opportunity for these companies put on the file to question the jusice of the information recorded on their account explains the importance for them to have a right of access. An official for the SMC expressed his view as follows: 'Being myself a business man, I do not question the right of a business man to be aware of the solvency of his customers; but there are different types of bad payer! What is there in common between a dishonest director - or simply a bad manager - and a director who finds himself temporarily - perhaps continually - in difficulty - for example in a period of credit restriction, or, more simply, because an important debtor has gone bankrupt, or because a bureaucratic administration has not paid an invoice until it was months overdue? It is bound to discourage the spirit of enterprise if one is kept out of a market for reasons beyond one's control. Or very often, the file holds only the payment incident, without taking into consideration the reasons behind it, which are not necessarily a sign of bad management.'

3.2.3 The public or private nature of non-physical person files

The reactions can be summarised as follows:
since the State becomes the file holder, small, medium or large companies form a united front to claim right of access, and, therefore, profit by a law for protection of non-physical person files.

Three changing factors are the cause of this reaction:

- the intervention of the State in private affairs is felt as a disguised attack on business freedom;
- the management of the State's large data banks is gathering an army of technicians and civil servants, which can jeopardise the security of the data;
- instruments which help in general economic decision, there information systems, because of progress in data processing, risk becoming increasingly used for individual decisions, means of pressure on particular companies. From economic forecasting, one risks turning to individual decision, or, at an intermediate stage to the selection of a target group of companies, which would be subject to unfair pressure by unequal forces to restructure.

In reaction, businesses are more and more inclined to claim:

- an individual right of access to data which concerns them.
- a general right of access to aggregated information (statistics through professional branches, trend studies in a given sector), in order to establish a fair relationship with a State which is powerful because it is better informed.

This last tendency should be improved: it seems to rest on a dual claim which has arisen due to the recent development of information laws.

During the 1970s, in Europe as in America, two sets of laws are overthrowing the well established traditions. Modern democracies tend to devote themselves:

- on the one hand, to privacy laws with their extensions because of technological progress: these are the laws of the data protection type;

- on the other hand, the laws facilitating access to administrative documentation: these are rules of the American 'freedom of information' type.

This development asks in new terms the question about the protection of the files of non-physical persons. The hypothesis is as follows:

- Certain countries, with the aim of controlling certain social malfunctions (eg the struggle against pollution, civil defence, product health and safety control, prevention of the use of dangerous products) are developing policies that are preventative rather than punisitive. Hence the setting up of an a priori control procedure, which requires the collection of increasingly numerous and detailed information. The files are set up on the request of the administration, sometimes having a bearing on previous basic research and experimentation with regard to industrial applications. This information is more and more frequently collected in data banks. It produces a

change of the legal status of this information, which is regarded as information which is processed on the State's account, rather than being private. Should one go on further, and consider that it is 'administrative information', which, as such, should be subjected to these new laws?

Are we not risking, in the near future, seeing these files subjected to the principle of 'open administration' under the pressure of these new laws, to the loss of the protection of confidentiality? It would be beyond the bounds of this study to reply to this question. However, it is appropriate to ask it, for here and now it is being considered in certain business spheres, particularly in the area of industrial research.

3.3 Distinction between the two problems

What is the position at present? The different laws already passed in Europe and the draft laws of which we are aware do not always establish the nature of the problems very clearly. Apart from the basic differences in the definition of the persons whom one should protect, there are also some difficulties in interpreting the very principles on which the laws rest.

The first laws on computer files (from Germany and Sweden) in principle intended to protect the rights of man and of the private citizen. Based on the principles of the rights of man, they define the citizen to be protected as a human being. As a general rule, these

laws only apply to fields which specifically identify physical person, mentioned by name: like an employee in personnel files, or a client of a bank, or a beneficiary of an insurance policy, or the holder of an identity card.

3.3.1 First problem: how far does protection of physical persons extend?

There are numerous examples of files which concern one or several individuals easily identifiable without being mentioned by name in the file, nor even having a named entry key in the file. For instance, one can consider the credit mechanism for small and medium sized businesses. In many countries banks rarely grant credit to a private or family company (eg SARL in France and Grubh in West Germany) without taking a personal guarantee, based on credit or on goods of one or several of the directors of the company in question. Under these conditions, it is clear that the banks' files of financial risks are, in many practical cases, implicitly the files of personal solvency which concern the owners of small businesses, and which tally with the personal credit and the goods of these directors.

Thus it seems that one can ligitimately consider the opportunity to apply the protection of data laws to such files in these countries.

A second example can also reveal this problem of the real effect of laws on files which refer only to physical

persons. In most countries, legal sanctions cannot be imposed on non-physical persons, except for mild penalties like fines. Whenever serious offences, such as tax fraud, industrial injuries, swindling, are attributed to a company the legal penalty is in fact suffered by individuals.

Thus the determination of the boundary beyond which the law protecting individuals ceases to apply is a real problem. With regard to this, European laws are beginning to be interpreted in differnt ways, according to national traditions. For instance in Sweden there is a very strict interpretation of the law: it applies only to the files in which physical persons are mentioned by name, not commercial files like those in the cases we have just mentioned. However one notes that the special law on credit provides the person concerned with efficient means of enquiry. In West Germany, on the other hand, the law on processing can be interpreted more widely: files concerning non-physical persons can come under the law, whenever fundamental liberty can be put in question by recorded information or by the way it is used. In this specific case, the basic principles on which the law is based allow a gradual extension of the law to files where the physical person is not clearly identified.

Thus let us sum up this first problem: each time the law on processing and fields is limited by national legislation to the protection of physical persons, the

problem of how to interpret the law arises. It is a matter particularly of knowing to what extent one can go with regard to non-physical persons files, to provide protection of the privacy of physical persons which the law should aim to protect. Between the narrow Swedish interpretation and an interpretation which treats some files as personal, as seems possible in West Germany, there is a large grey area which needs clarification.

However, one can see that this implies three categories of questions: first national tradition, into which the law on data processing must be integrated to grasp its sociological implication. The Swedish and German cases show clearly the importance of this factor. Next, interaction with legal rights, particularly with those of business, as one should consider it by priority, that legislation on data processing has a direct bearing on trade, and introduces penalties which concern directors of industry and trade. Finally, the relationship with the commercial practice of companies; for at this time one can observe a return to openness on the part of small companies, in which the financial liability of directors for tax and credit is becoming clearer.

The greater or less extent of informatics laws is therefore a very complex problem. But it is a problem which deserves treatment at community level, as it influences economic practice and the balance of competition between companies throughout the EEC.

3.3.2 Second problem: Should non-physical persons actually be protected?

Instead of considering the problem as an extension of the protection given by the law to physical persons to certain non-physical persons files, one can of course consider it in another way: certain countries have gone all the way by introducing into their legal system an equal protection for all files, whether they refer to physical or non-physical persons. This debate has already given rise to much feeling, particularly in certain international business circles. Thus it is urgent to clarify the questions which arise on the Community level.

The first question is one of principle: is there a basic Community rule leading to the restoration of protection t to a filed person through the file holder, a principle which of course grants protection when the filed person is non-physical? The reply to this question is not usually clearly formulated in the laws which exist in Europe. If one refers to the rights of man, as do all the laws at present in force in Europe, and solely to such principles, then it is obviously doubtful whether one can give the same protection and the same right to non-physical persons as to physical persons It is a little too early to set up a first list of practical difficulties in the application of these rules but one can see, for instance, that the right of access granted to physical persons for named information will be difficult to apply to non-physical persons.

We shall go into more detail on this subject in the following section. Let us be aware that there is doubt in many minds about the necessity of potection for company files, and about the fact that this protection is based on the same principles and the same morality as the protection of individuals.

Moreover, it would be particularly useful and instructive to give concrete examples to this debate, which can show that there are serious attacks on the reputation of companies arising from the simple fact that they have been put on file as data. This is why our team tried to find such examples, particularly in the course of the two inquiries that it carried out in 1978 and 1979. Although we have found leads, suggesting that some files, for example the files on industrial risks for insurance - can predetermine the future or the development of companies, these are only indications on which we have not been able to base a serious definitive argument. There has been no open, concrete case which can, to our knowledge, prove the urgency and necessity for a specific protection of companies with regard to computer files.

The lack of concrete examples can be explained by two main factors: on the one hand the current national laws are very recent, and those which concern non-physical persons have scarcely come into operation yet; on the other hand it is well known that the business world tends to be very secretive on matters which are in dispute and on difficulties encountered in the application of the

files, particularly because most of the files involved companies' and banks' finances. Yet, despite the lack of a concrete example, the insistance of many of the circles concerned about the problem of files of non-physical persons shows that it is absolutely necessary to progress to a definition of the problem and to clarify it.

This is why we thought it necessary to make a great effort to specify the concepts of protection more or less implicitly contained in the current laws in European countries. The result of this detailed analysis is that gradual protection of non-physical persons should be considered, not so much with regard to the rights of the individual as with regard to economic rights. In fact it is a question of freedom of action and business for economic agents, who are concerned mainly by the majority of files on non-physical persons. It is only on a secondary level that such files can injure the privacy of physical persons, as we will show now.

3.4 Specificity of the files of non-physical persons

It is interesting to examine the meaning on a practical level of this expression 'file of non-physical persons'. In respect, one must first question what this concept can cover in the different member countries; then one must consider the nature of the data liable to be recorded on a company.

3.4.1 Significance of the concept of non-physical persons

The dichotomy introduced into the legal vocabulary by the adjectives 'physical' and 'non-physical' perhaps oversimplifies the classification which we are seeking with the practical aim of distinguishing the appropriate means of action for each problem.

A first problem appears immediately: a physical person is easily identifiable as a human being in the sense of the Universal Declaration of the Rights of Man, for example. Thus it is unambiguous, largely self-evident to common sense. On the other hand, non-physical personality is not easy to define, and varies in meaning. For instance, this concept will not necessarily receive the same acceptance in tax rights as in civil responsibility; without taking account of the very detailed variations in doctrine which one can analyse at a given time between two European countries - like France and England for instance - or between two different periods in time in the same country. The doctrine fluctuates regarding its definition of non-physical personality, an argument which in itself appears to us to justify great caution in the comparitive interpretation of the laws of European countries.

However, one can distinguish several sets of concepts which form part of the definition of non-physical person for all the EEC countries. In this classification, one is led to distinguish three main categories of non-physical person which cover, in our view, almost the entire problem with regard to computer files.

a) The first category is that of commercial companies, comprising in English law corporations, in German GMBH, in French SARL, in Italian SPA, etc. The legal personality of these companies is not in question, and it is known that a number of the commercial business files contain detailed information on ownership, directorships customers, and the revenue of such companies. In business, one thinks immediately of files of this type when one considers the problem of the protection of non-physical persons.

b) The second category is that of private associations. In Great Britian these are clubs, in Belgium associations but commercial (non-profit societies), in France associations, and generally they are groups of a political, religious, trade union or social nature, which take various forms in law in the countries in Europe. In this admittedly miscellaneous category, it is not always possible to distinguish the person of an individual member from that of the whole association. Particularly because it includes all the groups of men and women who meet together to satisfy a common ideal, the association mut receive special attention from the law-giver. Thus, national traditions express profound differences with regard to the influence of the rules on computer files with regard to the private associations. The problem has not always been very clearly set out before now, but it seems necessary

to match the doctrine of the European countries, since these non-physical persons play an essential social role, which bears witness, in most countries, to the daily exercise of the basic liberty of the individual.

c) The third category of important legal entity concerns the public sector: for example, we can consider the nationally-owned industries in England, the 'Regies publiques' in France, in Italy the 'Ente nazionale' etc. In most member countries there is no problem in treating such bodies, which are becoming ever more numerous, as legal persons. But the special thing about them is that they straddle public service, which is subject to particular rules of operation in the laws on computing, and commercial companies or private societies, from whom they take part of their legal form. It is much more significant that these legal entities often have an essential commercial role, and that they sometimes exploit a monopoly position. Generally, recorded information on non-physical persons cannot be linked to physical persons, but to the state or local authorities. In the spirit of the research undertaken in Sweden, for instance, on the 'vulnerability of computerized societies', one can wonder whether it would be opportune to lay open the files on such non-physical persons, when these files have international power: files which the multinationals keep on their customers and

prospective customers; files of the World Bank; files of UNESCO etc.

This third group should doubtless be dealt with separately, because of its public nature and its political importance. Thus let us leave, in the perspective of our study, the files which record information on commercial companies (files on customers and suppliers, files on credit and solvency, files on mailing, etc.) and files of associations and trades unions.

3.4.2 Nature of the data on non-physical persons

The following attempt at classification takes account of three essential points:

- we have retained the criteria for classification of data which can apply to two main types of non-physical persons mentioned above (companies and societies),
- we have tried to eliminate aspects peculiar to a national law,
- we have tried to introduce obvious criteria so that the classification can support the application of practical recommendations.

The presentation of the five categories of data finally obtained is organised starting with the most public information, or that which is the most easily accessible to the public, and ending with the most confidential

information, or the least accessible to the public. It is obvious that this classification applies to data and not to opinions, it being understood that the declared opinion of M Dupont or M Durant is a fact, and not an opinion!

In the same way, in the meaning of this classification the stated intention to vote or to purchase, when collected by an interviewer, must be considered as an experimental fact with regard to data protection.

3.4.2.1 Public data

This is of course information whose publication followed compulsory regulations, or a voluntary action of the corporate body. This enables the introduction of a complementaty distinction between:

a) all data one is obliged to make public, for example under the terms of the law on commercial businesses, or for publicity in conformity with a law: turnover, constitution, annual accounts, convictions, etc.,

b) all data which one usually declares, communicates or which is spoken or written for the purpose of public relations, advertisement, press enquiries, conferences, etc.

It is obvious that such data on companies whose circulation to the public is covered by specific laws, for example on freedom of the press, can be freely

recorded, and control of the accuracy of the files is relatively simple. This data of course is outside the confidential area of non-physical persons.

3.4.2.2 Revealed data

This is data which has been communicated by the company to a third party, by a voluntary act, without the data being intended for widespread distribution to the public. Depending on the nature of the relations established between the data subject and the file holder, a more detailed distinction is required:

a) a sub-category must include data acquired through more or less obligatory enquiries or questionnaires which are very numerous: trade union, professional and administrative enquiries, export declarations, university research, surveys and statistics;

b) a second sub-category deals with information exchanged between economic agents in a specific contract, the operation of which involves opening its records to the partner: this is the case with industrial groups in a consortium, possibly secret collaborating in large projects; this is also the case with sub-contracts e.g. for commercial accounting skills.

In all the previous circumstances, the disclosure of data is carried out generally with the reciprocal understanding of the partners at the time of the

contract, that they will keep the data secret. With regard to contractual relations in the private sector, this can be resolved by the English concept 'breach of confidence on trade secrets' or by the French concept 'secret des affaires (business secrecy)'. A different problem arises whenever documentation is collected by an administrative organisaion by means of a public enquiry.

In fact one increasingly finds national legislation which aims to give a citizen free access to administrative documentation: in America, France, Sweden, for instance. When information is disclosed in an administrative enquiry, this information should become a public document, which would automatically make it accessible to citizens if the principle of open admistration were fully adhered to. But such an arrangement is completely incompatible with statistical secrecy, for instance, and the accepted rules for business confidentiality. This contradiction must be clearly expressed, and it should be resolved by specific derogation of the law.

Specifically, the data disclosed by companies and associations today represents a significant part of the field of application of the laws on the protection of files, when these laws apply to legal entities, as in Denmark, Luxembourg and Norway. The confidential nature of these files can be ensured by the conventions subscribed to by interested parties when the data is disclosed. But there is a conflict of interest between this need for confidentiality and the desire for openness

in administration, for the states which have decided to legislate to this effect. So far, however, we have not found a flagrant conflict of law in the member countries.

3.4.2.3 Cleared Information

This third category of information is acquired by chance or by a careful observation of the environment. For instance it concerns data gathered day after day by systematic analysis - by reading a newpaper, photocopying the classified advertisements, etc. In fact the systematic accumulation of a large amount of harmless information provides, after a certain time, a fairly accurate historical picture. For instance, it is well known that one can derive an excellent knowledge of a country's industry by regular reading of the daily papers. This is the nature of information. In the same way, by collecting indirect information on a company, one can get to know very well its strengths and weaknesses, without using irregular or reprehensible methods to find out. It is all a matter of organisation and effort. But currently there are some multinational companies which seem to have both the financial capacity and the technical ability to acquire economic information in this way with no other aim beyond that of improving their knowledge of the environment. All this would be of no import, nor practical interest without the tremendous memory and processing capacity of the computer. As it is, when processed skillfully by the computer, a rather incoherent collection of data acquired over several years can lead to a practical facility.

3.4.2.4 Derived information

By calculation or compared analysis of a large collection of miscellaneous data, one can extract notable facts which would escape the human eye. Multiples repression and correlation analyses, for instance, reveal figures or significant trends of development where none were perceptible before. This type of data, obtained by a sophisticated and expensive method of processing, can be described as 'derived information', and is specifically linked to computers, since without the such data would not exist, as they would be too expensive or would take too long to obtain for what they are worth.

This specifically computer phenomenon is new. It concerns a small number of files, mostly kept by public administrations or the multinational companies. It is a type of documentation which is expensive to collect and make, but the possession of which can give a considerable advantage.

When one says, in current jargon, 'information is power' it is primarily this derived information that is meant. Generally, derived data is classified as CONFIDENTIAL in administrations and as PROPRIETARY DATA in multinational businesses. This is explained by the often increased investment which is necessary to maintain them (daily observation, acquisition, data storage, modelling).

Whatever the original nature of this data, and taking account of its aim which should be permissible, it is

certain that it encourages a bias towards competition in favour of the file holder, which may have repercussions on the economic liberty of the data subject when such data is used to back up industrial decisions. For instance, in France, the ENEIDE file of the Industrial Department can legitimately be put in this category, and it is interesting to consider how it is used to decide to support or to abandon a company in difficulties. Should this be allowed, or should there be a code of conduct for the administrative use of such data on companies? This is the question one must ask about this.

3.4.2.5 Information obtained by spying

We are only mentioning it here for completeness. It is clear that it arises from a different problem from that which we are considering here. From the legislative point of view, the problem is not what type of access or protection one should ensure for this information, because it is clear that the collection of such data should be forbidden, and that, where it has been stored, it should be erased. Thus this problem is more one of applying laws and measures to exert effective control on this type of information.

3.4.3 Protection necessary for non-physical persons

In the very statement of the above classification, it seems clear that data on non-physical persons is either subject to rules of secrecy, or to rules of publicity. According to legal traditions of the State, the law-giver may enact either one or the other of these obligations,

but these two imperatives exist for all European countries. Divided between the rules which tend to anticipate the circulation of data on companies or societies (rules of secrecy) and rules which compel the disclosure of other data on the same companies (rules of publicity), the person in charge of files demands the right to organise his files in peace. But is such freedom compatible with equity in the economic links between the person who files and the data subject? This is the core of the problem of the potential protection of the files of non-physical persons.

3.4.3.1 The requirements of secrecy

Here we are going to specifically consider the question of business secrecy, that is to say the practises which prevent the free circulation of information in commercial circles. First we must recall the reason behind this form of secrecy, and examine the consequences of the right of privacy on the filing of non-physical persons.

The practice of business secrecy is clearly linked to competition, which forces a company to protect itself from indiscretions, whether in the laboratory, where one jealously guards recipes, which let one exploit a technological advance - eg pneumatic tyres - or in commercial services in which customer files are an essential element: every company is obliged to be secretive about its activities and its knowledge. This secrecy is necessary to protect the profitiability of investments in production or marketing. For example one

can consider the customer file of a company, which seems like an element of its ownership, and which is in fact covered by secrecy. The part of the customer file which is located at a concessionary company's office belongs in fact to the original company, which takes it back if the contract is broken. In the same way, commercial results covered by general secrecy, such as discounts, or compensation conditions in case of breach of contract, are a very important factor in competition.

The result of this very wide practice of secrecy in business is clear: as the information on file does not circulate well in commercial circles, most data subjects have difficulty in discovering whether they are on file, by whom, and where the files are. Even with several concurrent clues, one will often find it difficult to prove which file one would like to know the contents of. Further, it seems unfair that a company should demand openness of information from its business associate, without agreeing in return to open its own files.

To summarise, let us assert that the practice of business secrecy is today the corollary of the laws on competition, and these practices tend to make a spontaneous change of practice very difficult. In addition, all these applications are ruled by custom rather than by law, which can make the selective intervention of the law-giver even more difficult, when providing that the files of non-physical persons are

systematically declared open. In this respect, it will be particularly instructive to watch the first applications of the data protection laws in countries like Norway or Luxembourg, to gain practical instruction from them.

As for the files of non-commercial non-physical persons, we are not concerned with the reasons for which discretion is required. If one thinks, for instance of reeigious of philosophical groups, it is clear that they imply a recognition of the freedom of creed or thought, and that one finds, on the subject of the filing of such non-physical persons, the same consideration of public freedom and the rights of man, as one does in individuals' files. And also, one should bear in mind, with regard to religious sects for instance, whether the law-giver would not be lead to demand a greater openness of the financial accounts or commercial activities. The events of recent months have proved that the activities of certain sects, dangerous to the human being's integrity, have been made possible by the great secrecy from which they have benefited, particularly using the privileges and statutory protection of churches. But this leads us to an area much nearer to human rights than to economic rights, which are at the core of the problem of the files of non-physical persons.

3.4.3.2 Publicity reputations on non-physical puersons

With regard to non-commercial non-physical persons and churches, we have just considered the corollary of rules of secrecy. In fact, at a time when practices of secrecy are mainly moral, the obligation to make certain data public is, often, fixed by the law. Although the principles monitoring the national law-givers may be the same (to ensure fair competition, information for shareholders, employer-employee relations, etc), there are great variations in the obligations fixed by the different European countries on this subject. Also, for limited liability companies, although publication of the annual reeort is generally demanded, the countries differ in their demands with regard to anual trading accounts: compulsory in Great Britain, for instance; not required in France, etc.

The result is that, depending on the country, the boundary between information which should be made public (3.4.3.1 class a) and information which can be kept private is not the same. But the desirability of competition and internationalisation of business favours following the country which demands the greatest publicity. But commercially, this largely affects the large companies and appeals to the public for investment, whereas the small companies remain subject, primarily to national customs. It would be interesting to study, in this are, harmonization of Community law.

3.4.3.3 Difficulties connected with computer files

It is appropriate without doubt to point out two distinct approaches, depending on whether or not national legislation on data protection has anticipated the protection of files of non-physical persons. For countries which have included this protection in their law, the important question is to know if special arrangements should be made to exercise the acknowledged rights of the data subject with respect to the file holder, particularly in connection with the right of access and the right of correction. As operation of such legislation is hardly even outlined as yet, study of the basic concepts seems necessary to clarify the debate on that point.

Firstly let us consider the right of access. In studying this, one should imagine that the right of access has a bearing on the five categories of information defined above (3.4.2) for the classification we have proposed. For the first category (class 1: public data) the right of access poses no problem because this data is available elsewhere, and the exercise of the right of access does not prove injurious to the user of the file. For the second category of data (class 2: disccosed data), the exercise of thr right of access still poses no problem in principle as this disclosure is made within the scope of a contract, which the data user and the data subject both

accept de facto. One begins to encounter difficulties when establishing the filed company's right of access to gleaned data (class 3). This data represents a certain economic effort on the part of the file-holder who will probably want to protect this data through security measures. The right of access of a competitor to this data may give him an economic advantage. For calculated data (class 4: derived data), one comes up against problems of intellecual property for the models and simulations which have produced this data: and one will also find serious obstacles in recognising that the data subject could get from such information an insight into the industrial strategy of the data user. (Class 5: illegal data) falls into a well-established definition of the current laws, data which is illegal should be erased, that is clear. But, on a practical level, the setting up of control poses certain problems, above all for information relating to economic competition between large international firms.

It seems to us that the above shows that the right of access should without doubt be varied to take account of the specific question of relationships between commercial companies. As a first step, the right of access in the strict sense seems difficult to exercise in the same terms as for physical persons. The same is true of the right of correction. However, one could imagine that the right of access for non-physical persons might be limited

initially to a 'right of awareness', which would enable each economic agent to simply get to know the existence and general structure of the files where he is mentioned. Considering the large conomic files of the public sector, like the ENEDINE French file, the right to acquire knowledge would be great progress compared to the present confusion.

On the other hand, a right to dispute and to correct would seem to be a necessity whenever the company faced a decision based, for instance on a 'commercial profile', or on an analysis of the financial risk in which the dervied data or acquired data has had an overwhelming part. In legal terms, it would not be easy for the data subject to exercise his right, since proof of the existence of the files would be difficult if they had not been disclosed. This is why it seems to us consistent to envisage the dual obligation of the 'right to know' and the 'right to dispute'.

In this proposition, which probably requires a detailed study before being applied, we can see the beginning of a right of the same type as that which is given to the citizen (physical person) by article 3 of the French data protection law. In the extension of community principles on commerce, it seems desirable that the relationships between commercial agents are fair and responsible, and that the computer image of the company attracts the same attention as that of the individual.

3.5 Effective protection for physical person

The previous thoughts can be added to the discussions on whether or not it is necessary to protect non-physical person against the risks introduced by computer files. But they cannot lead to any uniform regulations in the EEC countries, both because of different legal doctrines, and the differences which still exist between the national laws on this subject. On the other hand, the EEC countries are not all involved in research on the protection of human beings, which we have shown can provoke study of the files of non-physical persons, even though the law tends to protect only physical persons.

Thus we shall devote this last section of the report to studying the interfacing problems which arise in the application of computer laws, whenever the data can be connected to a non-physical person, even if this relationship really implies a file on one or several physical persons.

3.5.1 The case of mixed files

The first doubt to be raised is that of files containing mixed and juxtaposed information concerning all types of persons, commercial and non-commercial non-physical persons, and physical persons. Several examples of such files can be given, which show that this problem is topical.

- The case where almost all customer files, or customers of any company - let us say for example the purchasers of refrigerators or cars - are filed in an order regardless of the type of person. The indexing key may be the account number of the customer for instance;
- The case of current bank account files, where one can find following each other and without distinction a business man's account, an individual's account, and the account of a medical partnership:
- The case of insurance policy ffles, fire insurance, and various risks, where one can find next to each other the policy of an individual and the policy of a company.

The daily life, this type of situation is common, which poses rather awkward problems. The first difficulty concerns a declaration of these files: for instance, should one demand that the declaration of files mentions the diversity of the files, in countries like Germany and France, or should one limit the declaration to that part of the file which concerns only physical persons? Whenever the files have a uniform structure (e.g. customer file), it is probable that the declaration will enable companies to know the structure of the files. The important thing at this point will be to know whether the right of access, granted to individual by the law, can be granted in the same way to a non-physical person, when it has the right to demand it, as will be without doubt the case in Luxembourg.

If the records are of the same type, there is no problem. But if a company record is different from that of an individual, the problem becomes complicated.

To explain the type of problems one encounters on this level, let us give an example. When a restaurant owner or a butcher buys a cooker or a refrigerator, he does this as a professional purchaser for use in his profession. He is assumed to poses the necessary competence to discuss prices, guarantees, technical performance of the equipment which he acquires as an essential tool for his work. But if the same refigerator or cooker is bought by a company, to furnish its offices or to equip a kitchen, this purchase become an act of household expenditure, unconnected with the activity of the company which buys it. This example helps us to underline two contradictions:

- the first contradiction: the butcher or the restaurant owner, acting within the normal framework of his business, will profit from the right of access of the seller of the household equipment to the customer file, if he operates under his name as an individual, when he would not have had the right of access if he had operated as a company.
- the second contradiction: the commercial company which acquires a refrigerator for its office equipment, and which is in the situation of a simple

household consumer, cannot use his right of access to the customer files of the supplier, when the law grants this right of access only to physical persons.

Thus one can show, in the light of this example, that the need for protection of data subjects should be defined much more by the nature of the transaction than by the personal status of the purchaser. Thus, in the same way it is natural to grant protection appropriate for the consumer status to a commercial company which buys periodically a car or a fridge, and treat it, perhaps, as a simple individual when it asks for information on the files concerning it.

The problem of mixed files is in any case a very delicate subject, and very common in practice, and it raises many problems when protection of data is granted exclusively to the files of physical persons.

3.5.2 Files containing indirect information about physical persons

Having examined the case of mixed files, we now look at a second case where there is conflict in the interpretation of the laws which do not include any protection for non-physical persons. It concerns the problem of the files of non-physical persons on which information is recorded which indirectly concerns the private life of physical

persons. There are plenty of such cases, as when data is recorded on the sex life, peculiar habits or the inclinations of a company director, e.g. abuse of alcohol, hobbies.

If one refers to the strict interpretations of the law, for instance in Sweden, it is clear that such files should not be declared as personal files, if the individual concerned is not specified by name in the file, even if he can be identified indirectly by his position in the company. On the other hand, it would seem that such information is within the scope of the German law, to the extent to which one can show that the recording of data, e.g. on the sexual habits of an individual who can be identified easily even if he is not named, puts an individual's dignity in question.

In the same context we observe that the European laws which extend to include the protection of non-physical persons do so on the same theoretical basis as the Swedish law: they have extended protection in order to better protect physical persons against an attack on their private life. This is clear, for example, in the introduction to the Austrian law and the Luxemburg law, and also in those of the Belgian draft law and of the Norwegian law.

To sum up, the European law-givers sought to cover non-physical persons not as such, but by extending the cover of physical persons in ways which laws like the Swedish did not provide.

3.6 Conclusions and European outlook

The application of the laws on computing and files in large European countries which were inspired by arrangements made in Sweden in 1973, presents a considerable mass of practical problems, and a major effort to deal with the existing files on physical persons. Due to the very superficial reactions of the general public, which were gauged during the recent conference in Paris on 'Data Processing and Society', it is becoming a generally accepted social objective to ensure that a European citizen has a satisfactory awareness of the places where he is on file, and the information contained in these files.

By a strange accident of history, the idea of giving non-physical persons protection of the same type as that which is offered today to physical persons has asserted itself more and more. Having been rejected by the German and French parliaments, this extension of protection to non-physical persons gradually asserted itself in the most recent laws, in Denmark,, Luxembourg, and Norway. Unfortunately, experience is still too recent to give a practical diagnosis on the true effect of these innovations.

We wanted to show, in this report, that the extension of the computing laws gives rise to two large problems: a conceptual problems, that of defining protection of non-physical persons in terms of principles, and the problems of interpretation in limiting the field of application of protection of physical persons when these persons are not mentioned by name in the files.

The first problem has not been solved in a satisfactory manner by the laws currently passed by the member countries. We have suggested that it should be considered as a commercial right, and not as a human right as in the majority of current laws. If one admits that non-physical persons, and particularly commercial agents, have a legal interest in keeping a strict control on information which they hold, a control which is ruled by the customary right of business secrecy, the concept of privacy in the strict sense can apply only to human beings, and not to companies or societies. Thus it seems desirable to us to specify a purely commercial doctrine on secrecy and disclosure of data which concerns commercial activities, and particularly that of commercial non-physical persons, in order to avoid in future permanent confusion between similar but distinct concepts, which one sometimes wrongly treats as one. If such a doctrine developed, and if it could be operated in Europe, it is probable that one could assimilate it to the principle of the Treaty of Rome regarding fair

competition (Article 85/86). In any case, it is one of the avenues of research which seems today the most promising outcome of this initial study.

The second problem is relatively easier to resolve. Whenever connections between physical and non-physical persons are implicit in the choice of the information recorded on file, it is probable that the laws should apply as if the file referred only to physical persons. Anyway, one should beware of a gradual extension of the field of application of the laws which would eventually take away their purpose. Apart from the fact that an extension without limits wwould mean bureaucratic sluggishness, which is incompatible with the efficiency of file control, this would not fail to raise very strict objections in certain industrial circles. In certain multinational documents, one already notes, for instance, a more or less deliberate confusion between the right of access of everyone to information which concerns him personnally, and the general right of access of the public to all recorded information.

In the commercial world, where secrecy of information is particularly important, the comparison between these two concepts, although very different, can produce rejection. Thus, in our view, it is necessary that future developments of the laws on files are based on a thorough analysis of the need for protection of data, and the form

of this protection for non-physical persons. Particularly, one should distinguish between commercial companies and private societies, and also what protection should be given to companies in the public sector.

Thus we consider that future research should be directed towards a very detailed analysis of the need for protection and the means of applying it, especially as these needs should be based, in our view, on the Common Market's economic principles: balance of competition, and equity in commercial relationships. If this should develop, one could then imagine that the final objective of data protection in Europe would be based on two complementary principles: the protection of man and the citizen on the one hand, particularly with regard to files of physical persons; the protection of 'commercial' man on the other hand, in what concerns the non-physical person! Such are, to conclude, the combination of principles which have the common aim of preserving freedom of personal decision in a computerized world. After all, is it not true that the main treat to each individual is that of being condemned to the determinism of a computer profile? If there is a common right which could be recognised for physical and non-physical persons, it would be the right to dispute in the name of their freedom of future action, the 'decision' of the computer concerning them.

This is without doubt the common objective. But the means of access, of control, and of enquiry will doubtless be different for physical and non-physical persons. Today one is well aware of the means which apply to files of physical persons. Several years more will doubless be needed before the same is true for the files of non-physical persons.

3.7 Bibliography

3.7.1 Legal aspects of transborder data flows

Gotlieb-Kauser-Katz: The transborder transfer of information by communications and computer systems: issues and approaches to guiding principles. The American Journal of International Law (Avril 1974).

Hogrebe: Verwaltungsautomation und Datenschutz in Frankreich. Schiveitzer Verlag. Berlin.

Report to the Privacy and Computers Task Force (Gouvernement Federal Canadien).

F W Houndius: Emerging Data Protection in Europe. North Holland Publishing Company. New York 1975.

La Protection des donnees en Europe. Strasbourg 1975.

Informatique at Libertes. "Rapport Tricot" (2 vol) La Documentation Francaise. Paris 1975.

Report of the Committee on Privacy - Her Majesty's Stationery Office. London 1972.

Colin Tapper: Computer Law. Longman. Londres 1978.

Banque de donnees: Enterprises et Vie privee. Actes du collogue de la Faculte Notre-Dame de la Paix a Manur 25/26 Septembre 1979.

3.7.2 O.E.C.D. documents

M F Hondius. Mesures internationales de protection de donnees Seminaire sur les questions d'order politique soulevees par la protection des donnees. Direction des Affaires Scientifiques. Groupe Informatique (24-26 juin 1974).

Le mouvement transfrontiere et la protection des donnees: Accords et organismes internationaux y afferents. Direction de la Science, de la Technologie et de l'Industrie. Juillett 1977.

Colloque sur les flux transfrontieres et la protection des libertes individuelles (Vienne 20/23 septembre 1977). Document de reference. Direction de la Science, de la Technologie et de l'Industrie.

Colloque sur les flux transfrontieres et la protection des libertes individuelles. Rapport de synthese: Effets et tendance (Vienne 20/23 septembre 1977). Direction de la Science, de la Technologie et de l'Industrie.

Reunion speciale sur les incidences, au plan de l'action gouvernementale, de l'evolution des reseaux de donnees dans la zone de l'OCDE (Paris 13/15 semptembre 1978). Direction de la Science, de la Technologie et de l'Industrie.

Ithiel de sala Pool et Richard Salomon transborder Data Flows: Requirements for international co-operation. Reunion speciale sur les incidences, au plan de l'action gourvernementale, de l'evolution des reseaux de donnees dans la zone de l'OCDE (Paris 13/15 septembre 1978).

Protection des donnees de caractere personnel: 1968 - 1978: Synthese des documents etablis par l'OCDE, le Conseil de l'Europe et la CEE (Janv. 79).

3.7.3 Networks and transborder data flows

L'arbre de vie Rapport d'etude sur la teleinformatique au Canaca. Ministere des Telecommunications. Ottawa (Mai 1972) (2 Vol).

Cap-Sogeti. Rapport sur les reseaux existants ou en project, et les actions de normalisation (Janvier 1976).

Jean Pierre CHAMOUX: Les flux d'information transfrontieres: Typologie et Problematique. Rapport a l'OCDE. Direction de la Science, de la Technologie et de l'Industrie (Paris Oct. 1978).

Droit et Informatique: Diagnostic sur les flux de donnees transfrontieres. Rapport final au Ministere de la Justice. Service de Coordination de la Recherche (Mars 1978).

I.B.I.: Survey on Strategy and Policies for informatics throughout the world (juillet 1978).

Arthur D Little: "Communication scenario for EPCOT. Reeort to "Wed-Enterprises" (Mai 1976).

LOGICA: The usage of international Data Networks in Europe. Special Session on Policy Implications of Data Network Development in the OECD Area (13/15 septembre 1978).

Jean-Claude MONIEZ: SWIFT: un exemple de cooperation interbancaire internationale. Revue Banque no. 355 (Oct 1976).

Simon NORA et Alain MINC: L'informatisation de la societe. La Documentation Francaise. Paris Janv. 1978.

Jean Michel TREILLE: Nouvelles strategies applicables aux informations d'affaires (oct. 1978).

US Department of Commerce. US Service Industries in world markets: Current problems and future policy department. (Decembre 1976).

3.7.4 Data banks, information retrieval networks

Simon NORA et Alain MINC L'informatisation de la societe Annexe no 2. La Documentation Francaise Paris 1978.

John Page: Cooperative information systems: a case study. Report to the commission of the European Communities. Avril 1976 (2 vol).

La revolution documentaire aux Etats Unis. Problemes poliques et sociaux. no. 321 (14 Oct. 1977). La Documentation Francaise. Paris.

J M TREILLE: Les instruments de strategies economiques et industrielles. (Rapport Convention de Recherche 75/47 entre l'IRIA et le CESA). Paris 1977.

3.7.5 Telecommunications satellites

La France et l'Europe face au defi des satellites. Institut International de Communications - Telequal - Actes du colloque du decembre 1978.

Telesat, Symphonie et la Cooperation spatiale regionale: Institut et Centre de droit aerien et spatial (Mac Gill University). Centre de Droit maritime et aerien (Universite de Nantes) Editions A. Pedone. Paris 1978.

Philip N Whittaker: SBS: A concept for the 80's. Special session on Policy Implications of Data Network Developments on the OECD Area (13/15 septembre 1978).

3.7.6 LINESCO documents

L'information a l'ere spatiale: le role des satellites de communication. UNESCO 1968.

Etudes et documents d'information.
no. 41: Les communications spatiales et les moyens de grande information (1963).
no. 53: Satellites de telecommunications pour l'education, la science et la culture (1968).
no. 60: La radiodiffusion par satellites (1971).
no. 66: Guide des communications par satellite (1972).

Meeting of Experts on the Draft Declaration of Guiding Principles on the use of Satellite Broadcasting for the free flow of information, the spread of Education and greater cultural exchanges. Final Reeort (Paris Mai 1972).

Declaration des principes directeurs de l'itilisation de la radiodiffusion par satellite

Data regulation: European and third world realities On Line conference proceedings - (Nov. 1978).

Multinational Telecommunications: Opportunities, costs and constraints - On Line Conference proceedings (June 1979).

3.7.7 Other interesting sources

Trans-National Data Reports (bi-monthly)

Le Journal de la Telematique (bi-mensuel)

Computer Law & Tax Report (Janv. 1979)