COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

LEGAL AFFAIRS

PROCEEDINGS OF THE FOURTEENTH COLLOQUY ON EUROPEAN LAW
Lisbon, 26-28 September 1984

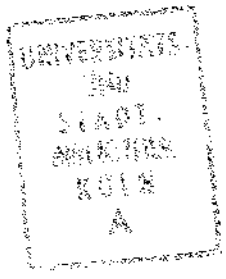
BEYOND 1984 : THE LAW AND INFORMATION TECHNOLOGY IN TOMORROW'S SOCIETY

STRASBOURG
1985

This work has been published in French under the title :

Au-delà de 1984 : le droit et les technologies de l'information dans la société de demain

ISBN 92-871-0754-8



Strasbourg, Council of Europe, Publications Section
ISBN 92-871-0755-6

Printed in France

TABLE OF CONTENTS

FOREWORD

The Council of Europe, whose membership consists of 21 European parliamentary democracies, provides the best framework for legal co-operation in Europe. Accordingly, since 1969 it has organised a Colloquy on European Law each year in a different country.

The object of these meetings is to enable specialists and decision-makers in the field in question to compare their ideas and experiences and, where appropriate, submit practical suggestions.

The subject of the XIVth Colloquy on European Law, which was held in Lisbon on 26-28 September 1984, was:

"Beyond 1984: the law and information technology in tomorrow's society".

It was organised in co-operation with the Portuguese authorities and attended by some 80 lawyers specialising in data protection and new technologies.

Speeches were made at the opening session by His Excellency Professor Rui Chancerelle de Machete, Portuguese Minister of Justice, and by Mrs Marie-Odile Wiederkehr, Head of Division, representing the Secretary General of the Council of Europe.

The discussions were held under the chairmanship of Mr J C de Carvalho Moitinho de Almeida, Director of the Office for European Law.

The discussions were based on four fundamental reports: "Policies and perspectives for data protection" by Professor S Rodota (Rome); "Technological development and its consequences for data protection" by Mr H Corell, senior legal adviser in the Ministry of Justice (Stockholm); "Workers' rights and technological changes" by Mrs M Georges, Research Fellow, in the Commission Nationale de l'Informatique et des Libertés (Paris); "Data protection and social policy" by Professor J Bing, Norwegian Research Centre for Computers and Law (Oslo).

The high quality of the reports enabled the colloquy to develop concepts (on the practical and theoretical level) on the speed of technological change and the positive and negative consequences of the new technologies.

The discussions were of great significance for the work of the Committee of Experts on Data Protection (CJ-PD) of the European Committee on Legal Co-operation (CDCJ). New legal solutions will in fact be necessary in order to meet the challenge of the problems raised by technological change, and Lisbon provided an excellent forum for taking stock of the work so far accomplished and defining future strategies.

After the discussions a general report was submitted by Professor S Simitis, Data Protection Commissioner of the Land of Hesse (Wiesbaden). The colloquy ended in a round table of guest speakers.

The results of the colloquy have been transmitted to the Committee of Ministers of the Council of Europe through the CDCJ.

The present volume contains all the documents presented to the colloquy.

ADDRESS

by

His Excellency, Professor Rui CHANCERELLE DE MACHETE,
Portuguese Minister of Justice

---

1. I should like to start by welcoming the participants to this 14th Colloquy on European Law whose proceedings begin today under the auspices of the Council of Europe. I should like, too, to thank you for coming to Lisbon and for all the work done by the Directorate of Legal Affairs and other bodies and staff members of the Council of Europe who have made this meeting possible.

Your high qualifications and extensive experience offer a sure guarantee of the success of this initiative by the Council of Europe and the Portuguese Ministry of Justice.

2. This year's subject, "Beyond 1984: the law and information technology in tomorrow's society" constitutes a significant intellectual challenge and is tremendously topical, particularly for Portugal.

Speaking of political and social forecasting, Mr Bertrand de Jouvenel has said that, "foreseeing the future would be an absurd undertaking were it not inevitable". Indeed we are forced to bet on the future because we have no other choice.

The construction of alternative scenarios based on carefully clarified assumptions and extrapolations of existing data is after all only a more systematic version of what anyone engaged in politics has to do every day. But apart from models based on certain trends and options we must pose the question of what all this means for humanity, for the values in which we believe, for the society which we wish to create and in which we are going to live.

Thus the fact of knowing where we are going if certain conditions are met or certain choices made can help us discover who we really are here and now. In this context, Orwell's vision of the future, Hayek's "The Road to Serfdom" and Schumpeter's "Capitalism, socialism and democracy" complete each other and help us to understand who we really are and to realise the risks involved in the potential development of certain elements already present in contemporary society.

3. The progress of science and technology and the arrival of more powerful machines and instruments increase man's capacity to intervene in nature and society. His freedom increases and the effects of his actions become greater. But freedom can be used either to give life to the values inherent in the human personality or for its complete destruction.

The defence of what we consider to be the highest good, ie man as a free being, should not and cannot be achieved by fighting against progress and innovation, but rather by the application of the ethical and legal rules which guarantee human dignity.

Modern information technology belongs to this problem area owing to the immense power it puts in the hands of its users. An instrument of choice for the treatment of large and complex systems, it is of great assistance in the public administration in all States. One therefore understands its very particular importance in the relationship between the State and the citizen.

More than 50 years ago , a specialist in German administrative law, Mr Forsthoff, drew attention, in a short monograph, to the fact that in dealing with the administration as a provider of services the average citizen found himself in a state of conditioning and dependency which might reduce him to the position of a subject if sufficient precautions were not taken. Unlike the traditional aggressive government departments of the liberal epoch, government departments as suppliers of services may infringe the legitimate rights or interests of members of the public by their omissions rather than by their actions. The defence techniques, based on the legal annulation of the administrative act (used to protect the traditional freedoms), are ineffective in this case.

The development of States based on social justice and the rule of law and the increased importance of government departments have undermined the fundamental freedoms in this respect so that today this is one of the weak points in the legal protection of the individual.

4. Lawyers were quick to perceive that data processing, while strengthening the possibilities of administrative action, nevertheless constituted a risk for the freedom of the individual. This realisation led to the transfer of the protection of personal data from the category of rights in rem to that of fundamental rights. However it seems to me probable that the essential structure of data protection as a fundamental freedom against unlawful attacks will be more and more completed by conferring on individuals, or organisations by whom they are rightfully represented, increased procedural rights of participation in the making and controlling of decisions. The right to take an active part in the procedure is a form of protection particularly suitable to the contemporary State based on social justice and hence in our time modern constitutions are tending more and more to recognise, in the context of fundamental rights, the importance of procedure and participation in decisions. In this connection, the new information technology raises questions of great theoretical and practical interest as is shown by the prepared reports for this colloquy and which I have had an opportunity of reading. This is one of the richest veins to be explored in this field.

5. The Portuguese Government has quite recently placed before Parliament a private members Bill (sic); this, together with a Bill prepared by ASDI (a political party) was debated last May and given general approval.

At the moment these Bills are being discussed in detail. The "Convention for the protection of individuals with regard to automatic processing of personal data", an instrument essential to complete the legal regulation of this question and prepared in the Council of Europe, has been submitted by the government and approved for ratification by the Assembly of the Republic.

I am sure that the conclusions of this colloquy will provide useful material for the discussions on this question to be held shortly in our Parliament.

6. The Ministry of Justice is very committed to increasing use of data processing as regards data connected with legislation and case law, the working of the courts, the land registry, the civil status registers, police records and the search for wanted criminals. These are sensitive areas and we must therefore act prudently but also with the necessary speed. The subject of the colloquy is very well chosen having regard to the ministry's scheme of activities and we confidently expect useful suggestions from its analysis of this material.

Once again I would like to thank you for your co-operation; I hope your proceedings will be fruitful and that you will have a pleasant stay in our country.

I thank you.

ADDRESS

by

Mrs Marie-Odile WIEDERKEHR
Head of Division
representing the Secretary General of the Council of Europe

---

1. It is an honour for me to have been asked by the Secretary General of the Council of Europe to transmit his personal good wishes for the success of the work of the XIVth Colloquy on European Law, which starts today in Lisbon. The Council of Europe is very grateful to you for having made available to the colloquy the magnificent building of the Gulbenkian Foundation whose excellent installations will greatly contribute to its success; Your Excellency, the Secretary General particularly wishes to express his gratitude to you for honouring with your presence today the inaugural session and has asked me to express his regret at not having been able to come to Lisbon on account of the session of the Consultative Assembly. The Council of Europe's thanks are also due to those of your assistants who for more than a year have been actively engaged in co-operation with the Strasbourg Secretariat in preparing today's event. Allow me to express particular thanks to Mr Moitinho and Mr Seabra Lopes with whom we have established permanent contact by all the various methods, both modern and less modern, available for co-operation at a distance between Lisbon and Strasbourg. Incidentally, the fact that they are both members of important legal committees in the Council of Europe greatly facilitated this co-operation.

2. This Colloquy on European Law is the XIVth of a series which started in 1969. The custom has now been established of holding an annual meeting at which a very free discussion is held on the most varied legal subjects with the participation of specialists and the senior officials engaged in the field in question from the 21 member States. This way of proceeding makes it possible to compare ideas and experiences in a more open and flexible context than our expert committees and has always proved very advantageous for the harmonisation or approximation of the legislation in member States. It makes it possible to examine in detail various aspects of a problem which at a given time is of concern to a certain number of member States: by way of example I would mention the colloquies at Aarhus on mutual assistance in administrative matters, in Madrid on State liability, and in Messina on the legal problems of unmarried couples. In most cases the subjects discussed at these colloquies on European law prepare the way for practical legal steps and often lead to the adoption of legal instruments ie conventions or recommendations, by the member States. The first object of these colloquies is to give an opportunity for a high level scientific debate but the adoption of practical conclusions is an additional benefit which usually accrues.

3. The Lisbon Colloquy follows in the steps of its predecessors. Increasing support was received for the idea of taking advantage of the symbolic year 1984, for a critical examination and a stocktaking of the upheavals in information technology with a view to assessing, in particular, the changes in society likely to result and the desirability of making new legal rules to accompany these changes. A role which the Council of Europe

has successfully played in the past and which corresponds well with its particular aims is to grasp from the beginning a situation which appears likely some time in the near future to become a matter of concern for the law of the member States.

The ideal solution is to organise co-operation and consultation between the responsible officers in the member States even before the legislative procedure is commenced as this is the best starting point for the harmonised development of legislation. This was achieved between 1970 and 1980 for data protection through a committee of experts many of whose members are present here today. At a time when legislation had been passed in very few States the Council of Europe started a forward-looking discussion with a view to defining the basic principles in the field of data protection. This led to the Council of Europe Convention of 28 January 1981 and the co-operation between member States also resulted in the passing of a series of national Acts based on the principles worked out together whilst at the same time taking account of the differing factual situations in the countries concerned. This co-ordinated action is still in progress and several states are in the process of drafting their national legislation and preparing to ratify the Convention. For instance Spain, which after ratifying the Council of Europe Convention is working actively on the preparation of legislation the principal features of which were presented to the Madrid Conference in June 1984. The same applies to Portugal where Your Excellency has given us an account of the progress achieved in giving practical shape to the law on data protection, which, as in Spain, is guaranteed in the Constitution. Switzerland, Belgium, Italy, the Netherlands and Greece are at a more or less advanced stage of the same process. It is interesting to note that a Data Protection Act prepared in 1984 is not fundamentally different to one prepared between 1970 and 1980, which shows, if that were necessary, that the principles governing data protection worked out in the Council of Europe Convention possess a value which is not tied to the particular circumstances of a given period.

4. However, nobody seeks to deny that the state of the art has developed a great deal and very fast and that the changes which have occurred are on such a scale that the problems may now be of a different nature. Does the arrival of techniques completely unknown at the time the Convention and the first generation of Acts were being prepared have the consequence of affecting the validity of these instruments? Does the prospect of a generalised adoption of techniques which are only just beginning to be developed mean that lawyers must throw all their established convictions overboard and draw on their imagination to produce entirely new rules? This is the fascinating question to which the eminent specialists in data protection and more generally in information technology meeting here today must try and find an answer.

They will be greatly assisted in their task by the remarkable analysis of existing concepts presented by the four rapporteurs and their knowledge both of the techniques which are now predominant and of the realities of the social situation in which these techniques are to be applied.

Looking at their first findings one is struck firstly by the fact that all of them seem to be convinced that the main principles of data protection hitherto accepted can continue to apply provided they are

examined from the standpoint of a concept of data protection which permits an unbroken transition with the free circulation of information. The importance of not separating the two aspects of access to information was emphasised already in Madrid and I think constitutes one of the guiding themes of the reports we are to discuss.

A second aspect implicit in the contributions before you is the clear-sighted recognition of the dangers inherent in using the new technologies in a manner which pays too little heed to all types of individual freedom, including not only the individual's right to information relating to himself but also his right to participate effectively in managing public affairs and in the political and administrative decisions by which he is affected. "Knowledge without conscience" wrote Montaigne, "destroys the soul". It appears fairly clearly from the reports that the risks that could rise from the arrival of the new technologies are, at bottom, those which Orwell anticipated, namely, the misuse of information technology either by public authorities or private power groups for individual purposes without concern for the public or private interest which constitutes its sole justification. The rapporteurs appear to be calling for a return to a concept of the general interest which is identical neither with individual interests nor with the interests of the State itself divorced from that of individual citizens; the idea that such an approach may make it possible to hold the balance between conflicting interests and overcome conflicts which might at first sight appear irreconcilable is put forward several times in the reports.

Seen from this standpoint of a balance between conflicting interests which it is our object not to suppress but to respect fully, it would seem possible to find reasonable, and thus acceptable, solutions to the very serious problems raised by the new technologies. So it becomes obvious that the various departments of State must be able to exercise the specific functions conferred on them for a precise purpose using all the information necessary to this end; at the same time, however, the authority conferred on them should not lead to a concentration in their hands of elements of information gathered for all sorts of different purposes, the combination of which would place in the hands of the State a formidable power in the face of which the individual might find himself entirely without defence. In this field and in the field of government the idea of transfer of power to local authorities and the role of intermediate bodies must find their proper place. In the same way, the information required for their activities collected by private undertakings should not be diverted from its original purpose so as to become a source of additional profit in which the individuals who provided the raw material have no share and which may even be directed against them. On the other hand, however, individuals should not consider rights conferred on them as absolute rights but as rights whose exercise constitutes a means of defending the proper working of an ordinary democratic system. Here in Portugal one need not recall that such research is directly connected with the ideals of the member States of the Council of Europe. These ideals of democracy, the rule of law and individual freedom have been applied by these States for more than 30 years. This gives us grounds to hope that the new challenge facing these States by virtue of the arrival of new technologies will be faced and overcome like all the other challenges.

POLICIES AND PERSPECTIVES FOR DATA PROTECTION

by

Professor Stefano RODOTA

University of Rome
Member of Parliament
(Italy)

1. Between utopias and principles

Between the end of the 19th century and the beginning of the 20th century, negative utopias replace positive utopias and in place of utopias of "desire" we find utopias of "anguish". George Orwell's 1984 is situated exactly in this new category. And it has been said over and over again that that is the result of the demise of a blind faith in progress which was typical of the last century. But the anguish of the future does not lead to the refusal of the future: in addition to the perception (even more acute) of the risks of technological progress, one finds the awareness of the impossiblity of stopping this future, even if it does not appear to be entirely positive in outlook. It behoves the writers to highlight the underlying reasons for these widespread fears, to stress the imagined or half-seen risks: "the mimetic fear brought about by literary fantasy discloses the nature of real social fears" (Elias, 1984:11). There is, accordingly, a revelatory effect, an unveiling, in the new literary utopias.

The demise of the idea of progress which is constant and, at any rate, positive focuses attention on the fact that the world can only be better if man wishes it so. From this awareness has been born the image which will henceforth follow the discussions on the social effects of the new technologies: that of the two-faced god, Janus. How many times have we repeated, with scarcely few significant changes, what Herbert Marcuse wrote concerning the experience in Hitler's Germany, underlining that "technology itself can promote liberty as well as authoritarianism, abundance as well as penury, abolition as well as intensification of work" (Marcuse, 1941:414).

Today, conflicts as radical as those may seem schematic or oversimplified. But the new anguish is born out of the awareness of the enormous gulf which exists between the rapidity of techno-scientific progress and the slowness with which the control capacity of the social processes which accompany this progress reach maturity. And it is precisely on this level that we must work, to fill in the gulf by analysing the complexity of present procedures, by launching appropriate policies, by finalising institutional solutions.

Nevertheless, this work often resolves itself into a feverish and vain pursuit of technological innovation. Sometimes, one has the feeling that the distance between the very rapid world of technological innovation and the very slow world of socio-institutional plans is going to increase. One constantly witnesses the rapid obsolescence of legal solutions which have been brought to bear on one single technical matter or on one single problem. In this way, one realises the need to determine principles and to relate them to long-term tendencies. This is precisely the direction which emerges from reflection on the experience of ten years of drafts and of the application of the first laws on electronic data processing.

The difficulties surrounding the quest for these principles are not only attributable to the fact that regulation of a continuously changing reality is in issue. The difficulties arise also out of a necessity to confront a variety of requirements, interests, values, which are often in conflict inter se. We are also concerned with the effect which new technologies have since they penetrate the most widely differing activities and cut across the most varied sectors. Oppositional pairs multiply: authoritarianism/democracy, centralisation/decentralisation, regulation/deregulation, transparency/secrecy, decision/participation ... And one could go on and on, underlining perhaps that in each of these pairs not only are the traditional debates renewed, but that one can discern a "technological" change in what goes to make up these oppositions. It is against this backdrop that we must today launch data protection policies.

2. Technological changes and institutional innovation

One can try to define by way of synthesis the totality of the changes which have upset the scenario taking place before us. Firstly, the diffusion of the possibilities and ways of data processing. Twenty years ago, when the debates on the risks for privacy were in full bloom and at the beginning of legislation on the protection of personal data, the point of reference was a technological reality in which the computers in existence as referred to in the literature, whether doom-laden or not, were equivalent in calculating power to today's personal computers.

From this finding one cannot simply draw the hasty conclusion that the risks denounced at that time have multiplied beyond expectation and even beyond imagination, as if the present use of personal computers corresponded perfectly to those large central computers. It is apparent, at any rate, that certain legislative definitions, conceived with reference to the large computerised systems built around large computers, are increasingly no longer useful. For example, the definition of personal data bank as "archives managed by a system of automated data processing which contain personal data which can relate to a concerned individual", is no longer viable to establish obligations common to all those who own archives which, in principle, fall within the aforementioned definition. Indeed, what would be the costs, both economic and bureaucratic, of a registration obligation imposed on all the owners of personal computers? As a consequence, one can see that exceptions will be made to the laws in force which exonerate from the obligation to register all those individuals who set up an automated archive for strictly personal purposes (see the new Article 1 of the Swedish law).

In following technological developments, one can notice that even the notions of file and "data bank" are in the process of becoming insufficient and outmoded and that the new frontier is not identified solely by personal computers. It is the notion of network which has even more of a central position; the new realities are called local area network, work station; in the diffusion of interactive technologies, account must be taken of the perspectives opened up by telematics.

./.

That is not the only technological scenario which is changing: the institutional framework is also being transformed. Attention is not being exclusively focused on the concept of privacy, although this concept is redefined in the new context. We are moving towards the much more comprehensive notion of "data protection" which goes far beyond the problems of protection of private life and which, in fact, refers henceforth to a basic criterion of the very legality of public action. (Sieghart, 1983 : 16; Simitis, 1983 : 175)

Even the most important product of the first generation of laws on automated data processing - the right of access - has brought about consequences and has opened perspectives which originally were not foreseen and which also go beyond a guarantee exclusively concerning the individual sphere. By offering to individuals a dynamic means of safeguarding their informational patrimony, a way has been opened at the same time to dismantle the secrecy barriers surrounding the data owned by other parties. The laws on data protection have been the forerunners for the laws on access to administrative documents and on administration "in the sunshine". All that has brought about a change in the institutional framework which is by no means negligible because emphasis has been placed more and more not only on the defence of the individual sphere, but rather on the general rules concerning the circulation of information (whether personal or impersonal) which is at the disposal of public bodies.

Throughout this tendency, one can very easily discern the relationship which is going to develop between individuals and information or, to be more precise, between the interests of individuals and the ways in which information circulates. On the one hand, by enlarging the principle of consensus, we arrive at the declaration of a "a right to informational self-determination", at the constitutional level as pronounced by the Constitutional Court of the Federal Republic of Germany (Simitis, 1984). On the other hand, the right to disclosure of certain categories of information (the information right) will enrich itself as Right to Democracy (Yudof, 1983), by identifying, henceforth almost entirely, the democratic character of a system with the quantity and the level of information which circulates within the system.

Transparency also affirms its reasons as the reference point of the real presence of citizens within the social and political organisation. If democracy really wishes to be "government of the people" it is necessary for it to be "government in public" or "government of visible power" (Bobbio, 1980 : 181).

In this way, the personal sphere and the political sphere come together. That does not only mean that the degree of protection for the individual in regard to his private sphere depends on the general way in which the political system functions. It also means that the rules concerning the circulation of information are destined to affect the distribution of power in society.

./.

At this point, another apparent paradox can be discovered. The systems of government "in public" which favour the value of transparency, are those which offer their citizens the possibility of an effective guarantee of their private life, for those very citizens are the holders of an increasing share of the power of control over public (and private) structures. This is exactly the opposite to what happens in those systems which are inspired by totalitarian logic and practices and where secrecy and opaqueness constitute the real rules for the functioning of state structures.

This increase in the opportunities for larger and larger groups of citizens to intervene and control is destined to become more concrete as a result of the spread of information processing systems and the development of interactive technologies. It is precisely this latter technological change which is destined to have repercussions on the concrete arrangements in the relations between citizen and those who collect data. There is an increasing evident coincidence between the data collector and the provider of a service: the new media are also channels (sometimes above all) for the provision of goods and services on the basis of an increasingly rich exchange of information.

We find there an evolution which is producing new relationships. The information provided by concerned parties so as to receive certain services is such, in quantity and quality, that it is at the basis of a series of possible secondary uses which are particularly remunerative for those who manage interactive systems. The latter, by processing the data which have been obtained at the time of the provision of services, can create new information (profiles on individual and family consumption, preference analysis, statistical data, etc.). What we are talking about is the sort of information which is of interest to others and to whom it can be sold.

Accordingly, it is not possible to confine oneself to discussing information simply in terms of a fundamental "resource" for society which can be seen emerging before us. The interactive technologies have the capacity to create a new "commodity" which laws will deal with within the disciplines concerning cable privacy or videotex systems. And it is revealing that it is precisely at this point that one finds more and more norms on opinion polls which today represent the most controversial and sensitive frontier in regard to the expression of citizens preferences. Since these preferences can also concern important choices for the social and political organisation, the regulation of the storage and processing of data can once again not be reduced to one individual denominator. The real theme which is treated by all this is that of the role of the citizen in the computerised society, of the distribution of power connected to the availability of information and, accordingly, how this information is stored and circulates.

3. Privacy: Old ideas and new problems

If an attempt is made to follow legal discipline in this area, it will be noticed at any rate that the problem of privacy still occupies the centre of attention. The permanent nature of this attention must be explained beyond the need to guarantee a protection which is proportionate to the interests which are still found under the rubric of privacy.

./.

The most immediate and most evident explanation can be found in the fact that the underlying reasons (and therefore the fundamental structure) of the first generation of data protection laws expressly refer to the aim of replying to the widespread anxieties concerning violations of privacy brought about by computer technology. It is a question of a priority or privileged approach to the typical legal problems of the new technologies which continues to exert influence even today.

Moreover, this way of raising the problem made it possible (and still makes it possible) to confine the new theme within the framework of traditional private law categories, following a logic which has also influenced interpretations concerning the right of access. Indeed, in the majority of cases this right has been considered as a counterpart offered to the individual in return for personal information "ceded" to public and private bodies and, therefore, according with the typically property concept of exchange. This is not a new scheme of things: individuals have on many occasions succeeded in their attempts to obtain the right to control the activity of certain public bodies for the sole reason that these bodies used resources which have been directly provided by the individual. Suffice it to recall Article 14 of the Declaration of the Rights of Man and of the Citizen which affirms the right of citizens to "follow up the use" made by the State of "public funds".

If the problem is considered only from this point of view, the operational possibilities of the right of access are clearly reduced (this problem will be considered in a more analytical manner later). But it must also be added that it is precisely the place given to the right of access, with its formal link with the individual interest in the defence of privacy, which allows the concept of privacy to continue to play an important role in the legal consideration of the problems concerning the circulation of information.

But the particular attention which has been accorded to privacy questions, and which sometimes does not correspond to the real, actual dimensions of the institutional problems in regard to information, is not solely a consequence of a certain intellectual laziness or inability to glance beyond the logic of property rights. There are other legal policy reasons which push in the direction mentioned.

On the one hand, because the mass media have almost exclusively emphasised this aspect, the association between new technologies and risks to privacy has been the theme to which public opinion has been, and continues to be, most sensitive. On the other hand, a legislative response which is based entirely in terms of individual protection of privacy, and with an atomised control granted solely to individuals, evidently appears to be the one which is least expensive (politically, socially, economically) for those who keep large masses of data.

In a first phase, the convergence of these two types of interest has produced very important innovatory results. Today, on the contrary, that convergence risks putting a brake on an evolution of the legal

./.

control which corresponds to the reality of technological innovation, and also justifying the irony of those who believe that the laws on data protection are purely "decorative" (Enzenberger, 1979 : 30), or the criticism of those who see these laws as simply a means of legitimating large automated archives and the creation of new and useless bureaucracies.

Accordingly, an enlarging of institutional perspectives is necessary for the defence of privacy, going beyond a purely property logic and adding collective controls to individual control, making distinctions between the different aims of data storage, making legal regulation uniform at this level, analysing more thoroughly the interests which are present in the various operations and providing for new criteria for the selection and balance between such interests. By way of synthesis: it is henceforth impossible to relate data protection solely to particular questions, even if these questions are in themselves very important. An integrated strategy is necessary which can regulate the whole of the circulation of information.

4. The circulation of information between free market and regulation

This line of argument is radically contested by those who, for various reasons, do not share the opinion which posits that it is possible or appropriate to enlarge or to articulate regulation in this field. Some have stressed that binding rules on storage, processing and circulation of data are possible in periods which are relatively tranquil even if these periods are not entirely halcyon. If, on the contrary, social instability begins to increase there is also a growing need for information and for collaboration between data banks so as to confront emergencies in the field of public order, the labour market, etc.

To these reflections may be added those which have as their point of reference the economic crisis in different countries and which fall back on the argument of the impossibility of burdening enterprises with extra and unnecessary costs, and among which would be precisely those costs provided for in the procedures set out in the data protection laws.

At a more general level, resistance to legislative intervention is greeted more favourably than in the past thanks to the climate created by the supporters of deregulation. On the one hand, a resurgence of illusory beliefs can be seen in the autonomous and spontaneous regulatory attitude of the new technologies, beliefs which had appeared at the beginning of the discussions in this field (Baran, 1965 : 14). Moreover, it is suggested to leave everything to the logic of the marketplace, either in general or in the specific field of privacy to which should be applied the same negotiatory rules of property rights proposed for other legal institutions by the theoreticians of the economic analysis of law (Posner et al. 1980). Continuing with this logic, it could be observed that the crisis of the welfare state, by compelling a reduction in certain social services, would also compel a reduction in the corresponding data banks and, as a consequence, the legal rules relating to them.

./.

To all these arguments there is added the finding on the very modest working of certain data protection laws or, at least, of certain instruments which are particularly highlighted (among which, in the first place, the right of access). This argument, with its misleading empirical evidence, reinforces the deregulation thesis.

If one wanted to reply meticulously to these arguments, it would be necessary to begin by saying that the first generation laws had refuted Paul Baran's thesis on the impossibility of putting forward a legal control for this domain and, today, the most recent theses on deregulation have been refuted in their turn and by the rich legislative production of the last years, the characteristics of which prevent us from regarding it as a simple continuation of the tendencies towards regulation in the first phase.

Indeed, if one surveys the hierarchical ladder of the various normative sources, one will find rules on the circulation of information in constitutional texts (Spain, Portugal), international conventions, federal laws and state laws, district and provincial ordinances, and in atypical instruments like the Staatsvertrag between the Bund and the Länder of the Federal Republic of Germany. And even the production of codes of ethics or self-regulatory codes shows us that the private sector also does not believe that it is possible to entrust itself completely to the spontaneous functioning of the market place. Finally, there are many cases which are entrusted to the competence of the judicial or administrative bodies which illustrate the necessity of objective rules for the resolution of conflicts.

Beyond the simple observation of this reality, although it is important, concrete reflection on the parties and interests which arise is necessary so as to see if the parties to "information transactions" are in a position of equality or whether there exists a power inequality. In that case, legislative intervention could precisely serve to re-establish certain basic conditions for the functioning of the marketplace. Accordingly, the problems are posed in the same way as those concerning protection of the weak party to a contract, although it is quite clear that the issue is different.

Indeed, one is struck by the very great gulf which exists between the description of the extraordinary consequences of the new technologies (third wave, new industrial revolution, etc.) which would produce a real epoch-making change with the emergence of information as a fundamental resource for the future, and the claim of not following a change on such a scale by appropriate legal institutions. If one wanted to be ironic, one could say that the new Monsieur Jourdain, the fervent supporters of the new technologies, are preaching Marxism without knowing it, for they are confiding to the change in the social formation which has been brought about by these technologies, a gradual extinction of law and of the state. Their position, in fact, has radical characteristics which even go beyond the thesis of the theoreticians of the minimalist state (Nozick, 1974).

./.

In reality the problem is not one of regulation or non-regulation, or of law or no law. The real question concerns the possibility of entrusting a prescriptive value for the future to categories and concepts which - like those of the weak contracting party or of privacy - have been drawn up for situations which still do not recognise the central position of the "information" resource. Accordingly, it is necessary to produce appropriate institutions for the new reality (just as modern law, the child of the industrial revolution took the place of feudal law?); and in this new institutional framework it would also be necessary to reply to the interests and requirements which, through custom or lack of imagination, we still call by their old names.

All this requires careful analysis of the concrete effects of the new media (and old, in a changing technological framework). For example, the increasingly close links between the provision of information and the enjoyment of services, which is typical of the spread of the new media, have resulted in a progressive reduction of the need for privacy rather than its protection according to the laws of the marketplace (Gardner and White, 1983). And the possibility of intervening at the time of social, political or economic emergencies through use of ever-increasing masses of personal information brings about a situation in which the firm principles for the guarantee of individual and collective liberties are endangered.

The real problem is therefore to establish a framework of fundamental principles which can be referred to in a changing situation; not the survival, more or less precarious, of the old institutional framework. In the information age, it is necessary to re-write the table of values so as to guarantee the real expansion of what one means by the words liberty and democracy.

This is not an easy task. The immaterial nature of information makes the slide toward totalitarian practices perhaps less perceptible. Indeed, in the information society an authoritarian régime can arise without those warnings which were typical in the past (mass arrests or deportations, torture, etc.). Accordingly, one must not simply guarantee rights: it is also necessary to safeguard and stimulate social sensibilities, to arouse the capacity for reaction. It is necessary that the institutional apparatus, far from being reduced, be enlarged to a very great extent.

In this situation, the notion of deregulation and of the marketplace is quite inadequate. But, there is the risk that a perspective removed from consensual transactions and linked solely to the reinforcement of "passive" individual defences will also be inadequate, such "passive" defences being composed of prohibitions on data storage and "indispensable" rights. Of course all that remains essential, but it is a point of departure not arrival. After receiving a guarantee for certain fundamental positions, it is necessary that individuals and groups can have at their disposal instruments to make them worthwhile in a direct and dynamic manner.

This path can prevent data protection from being simply a reduction in the flow of information, a brake in social communication. Indeed, by following this path one can bring about increased transparency in decision-making procedures, a greater control over those who hold power,

./.

the birth of new collective identities (henceforth considered as an essential engine for change). And, in a similar framework, there would be a reinforcement of the reasons of individuals, not their mortification.

Following the same line, it will be noticed how very weak are considerations based solely on the increase in costs for public administration and firms. Could one really reject the request for means of protection for the physical integrity of workers in their workplaces by saying that that would be expensive for the firms? In the case of the new technologies, the interests which must be protected and which can appear antagonistic to those of the firm are no less important.

Moreover, there are more than just social costs for which it is necessary to resolve a problem of internalisation or externalisation by means of a calculation based on political advisability or economic advantage. On the contrary, it is necessary to prevent the production of certain effects which are considered to be negative in principle: and the best way of pursuing this aim is by imposing certain charges on those who store data. In principle, according to the conclusions of research on finance carried out by the Commission of the European Economic Community, industrial circles do not consider data protection costs excessive: and among entrepreneurs, there are several who think that the provision of certain rules or standards can facilitate the more rational management of firms.

5. Reflections on the right of access

The problems already covered can be clarified if the right of access theme is examined more analytically. The controversies surrounding this instrument are well known: to the enthusiasm of those who emphasise its great value as a principle there is opposed the scepticism of those who comment on its weakness.

I believe that it is impossible to challenge the innovation introduced by the right of access to the body of principles: firstly, because the principle of the impenetrability of data stored by the public and private sector has been shattered; secondly, because there has been adopted the criterion of widespread control in the community, exercised directly by interested parties and through the criteria of a simple formal attribution of a right, the effective protection of which has since been entrusted to structures, more or less bureaucratic, and, in any case, removed from the interested parties. These two new factors within the framework of principles are at the basis of very interesting developments about which more will be heard later.

However, it has been stated that data subjects have made very restricted use of the new instrument at their disposal. And a more radical criticism has been expressed which emphasises that, at the end of the day, the right of access cannot give great satisfaction because it only concerns "the right to know that one has been recorded". In brief: the right of access does not provide an effective power of control over data which have been stored. On the contrary, it would legitimate their existence.

./.

It is true that in the majority of cases individuals have made limited use of their right of access. But this finding cannot be considered as conclusive. Firstly, the worried reaction of certain organisations (in particular, certain sectors of the public administration in the United States), although cases of the exercise of the right of access are limited, shows very well that the fact that citizens use or do not use this right is by no means without importance. Secondly, apart from concrete cases of the exercise of the right, one can well appreciate that its formal recognition has brought about a spontaneous acceptance on the part of those who store data so as to enable them to confront the possiblity of access by data subjects. In conclusion, in certain countries an increase in recourse to the right of access has been reported. In the United States, in 1983, the access provided for under the Fair Credit Reporting Act was availed of in a million cases (Smith, 1984). In the last report of the National Commission for Data Processing and Freedoms (France), it was stressed that "1982/83 shows a growing number of cases where the Commission has been seized in regard to the right of access (60% increase in consultations by telephone, 26% by mail)" (CNIL, 1984: 113).

Here we are talking about figures which may be considered as modest, whether in the absolute (but more thorough reflection might be necessary concerning the case of the United States), or in comparison to existing data banks and to the quantity of information stored. In any case, the examples cited may be interpreted as indications of a progressive awareness, although a slow one, of the utility of the instruments laid down in the new laws.

But, generally speaking, the principle value of recognition of the right of access must not be confused with its, hitherto limited, use. The real question concerns the development of all the potentialities linked to the principle of the right of access.

There are many reasons which may explain the reduced use of access by individuals: lack of information; the cost of access (in terms of time, money, etc.); illiteracy, the gulf between the power of individuals and the power of the large public and private bureaucracies (Lenk 1982: 287-290); too many prohibitions and limitations regarding access to certain categories of data; the weak value of the data communicated, lack of general information about the system where the data are processed. The future of the right of access depends on the possibility of overcoming these obstacles.

The lines of possible intervention, which are already seen in certain laws, may be indicated synthetically. Firstly, the reinforcement of the position of individuals, either to make access more effective or to fill in, if possible, the gap between their power and the power of the information "barons". In order to bring about this goal, it is absolutely essential to permit access which is "aided" by experts and which has as its aim not only knowledge of personal data but also the criteria used for the automated processing of data (in accordance with

./.

Article 3 of the French law). Even more important would be the recognition of a right of individual access of which the participation of a collective subject would form an integral part (trade union, association for civil liberties, association for the protection of consumers, etc.). In addition, an autonomous base should be provided for direct access by collective subjects, although tempered by the consent of the interested individuals. These collective subjects could begin to recognise that among their institutional functions there is the function of a systematic exercise of the right of access and in this way bring about an effective control over those who store data.

Moreover, in cases where personal data are used by systems for automated decisions, it is not simply sufficient to lay down a prohibition on all automated decisions on individuals which have been taken on the sole basis of personal profiles drawn by automated processing (Article 2 of the French law of 1978 and the Article of the Italian law on the Reform of the Police, 1981). We must place alongside this technique of negative protection a positive technique, affirming "a right to know the programs of the model for the automated decision" (EEC 1983): it is quite evident that we are witnessing an enrichment and a reinforcement of the right of access which is moving towards a recognition for all interested parties of a right to know and to evaluate the context in which the data concerning their private life are processed.

In this way, access goes beyond the framework of personal information and its regulation tends to come together with the much more general right to information as seen in its active and dynamic form: not only a right to be informed but a right to have direct access to the totality of public and private data. It is at this point that the relations between the technological innovations and institutional developments can be seen. Thanks to technological progress, it is today possible to propose a generalisation of the right of access because we are in the process of eliminating "physical" obstacles which, in the past, prevented or made very difficult access from afar, multiple access, access outside office hours and so on.

Accordingly, it can be emphasised that the parallel development of data protection laws, characterised by the new factor of the right of access, and laws on the freedom of information (in the form of laws giving citizens access to administrative documents) is by no means fortuitous. On the contrary, an effective realisation of the right of access to personal data from now on also involves the possibility of having access to an additional series of data (even private data, in systems where control common to both domains is already provided for). These developments in the control produce contradictions and conflicts for which it is not always easy to find solutions. In principle, it could immediately be noted that protection of privacy and very widely conceived access to data are two incompatible goals because the former aims to restrict the circulation of certain categories of data. And the problem exists in reality: the question concerning the relations between data protection laws and laws on access to public documents is becoming more and more central.

In order to reply to this question, conciliation techniques for the different interests which are at the root of the two types of laws are developed. But going beyond specific solutions, it is increasingly evident that the problems must be looked at in the same context. In certain

./.

laws the distinction between the two types of discipline is henceforth purely formal: this can be perceived by analysing the reciprocal reference systems, whether explicit or implicit, and the method tending to approve the two controls together. This is the case in Canada where the Access to Information Act and the Privacy Act constitute Appendices I and II of the same law which was adopted in 1982 and provide striking structural analogies and have procedural rules in common. That proves very clearly that it is now necessary to deal with and resolve the fundamental problems of data protection in a single framework containing rules on the circulation of personal and impersonal information.

One cannot analyse here all the domains where there exist interferences between freedom of information and data protection and the solutions which have recently been canvassed (EEC 1983). We can only stress that we are trying to refer to various principles so as to construct criteria which are capable of selecting and balancing the interests which are in conflict.

In many cases the functional approach will prevail. Thus in the field of scientific research the possibility of access is provided for even in the case of personal data by conferring privileges on the "function" (research) in a framework of procedural guarantees (this model was adopted by the European Science Foundation in its Declaration on the protection of privacy and the use of personal data for research purposes only). In this case, the rules concerning transmission of data draw a distinction between the access stage (allowed even for personal data) and the stage of communication to outside persons of the results of the research (where the anonymity rule prevails).

On the other hand, when the aspect of documentation or historical value is predominant an attempt is made to achieve complete freedom for the transmission of personal data. For example, this model was adopted by the Canadian Protection of Personal Data Act. Section 8 (3) provides "personal data in the public records office which has been placed on deposit or contributed for historical purposes by a federal institution may be communicated in accordance with the regulations in connection with research or statistics". It should be noted that this section is contained in the Data Protection Act and not the Access to Information Act. This expressly confirms the tendency which sees no substantial distinction between the two types of enactment. In other countries the same trend has led to a reform of the legislation relating to public records.

In view of the scale and importance of the interests involved we must also consider the tendency to "liberalise" the transmission of a personal data of an economic nature. This trend is not solely confirmed by an analysis of the rules applying in the various countries. If we restrict our investigation to international documents which establish a distinction between the various categories of personal data (resolution of the European Parliament of 1979; Council of Europe Convention of 1981) it can be seen that the hard core of privacy is identified by reference to categories of information which include no mention of data of an economic nature.

Historically speaking, it is easy to follow the gradual reduction in the hyperprotection given to the personal data of an economic nature (censuses in the United States, DAVIS, 1973: 178). This is a general

movement which is now reaching even the strongholds of banking secrecy (it is enough to look at a certain evolution in the Swiss system). But we must look more directly at two fields where important innovations may be noted: tax legislation and information on the activities of business concerns.

There are now many countries where individuals are entitled to receive tax information not only concerning themselves directly but also concerning other persons. The reasons for this development are obvious: the role of taxation is becoming more and more important in contemporary systems of government. Extended control is therefore necessary to render the actions of government departments as open as possible in this particularly sensitive field and also, by comparing information from various sources, to create conditions conducive to producing equality of treatment between different taxpayers.

It is necessary to emphasise again the importance, both in practice and in principle, of the right of trade unions to receive information on certain aspects of a firm's activities in particular cases (the phases in negotiation of collective agreements) or on a regular basis. But even in this domain, the traditional secrecy barriers are falling down. During the negotiation of collective agreements, information is decisive for the determination of the power of the parties. And given that today the trade union, beyond the factory gates, is participating in the determination of neo-corporatist balancing or is playing the role of protagonist in certain complex operations concerning "political exchange", its position is influenced in a decisive manner by the availability of information on the position of the other protagonist to the negotiation, the entrepreneur.

We are dealing with examples which, taken from fields formerly separated from those which are the object of the intervention of data protection laws, nevertheless find confirmation in the rules which concern the activity of financial information offices. Here the technique of data protection is quite procedural and, essentially, aims to facilitate, not to limit, the circulation of data. We are talking about a regulation which really aims to legitimate operations involving storing, processing and diffusion of financial information. The direct access of data subjects aims to guarantee that information which is diffused is correct and complete, while observing that a continuous flow of correct information on the actors in economic affairs offers a guarantee not only for the interested parties but also for the functioning of the market. It is for this reason that the traditional hostility of the American to intervention in the private sector has not prevented very binding regulation in this field, from the Fair Credit Reporting Act onwards.

It can be concluded, therefore, that there is a tendency in favour of rules which aim to stimulate the circulation of economic information (and therefore access to it). Limitations on the storage and diffusion of data

(and therefore defence of privacy in the more traditional form) are concentrating more on information which is considered "hot" or "sensitive", particularly information which concerns the sphere of opinions, health, sexual life. And above all opinions, because they are the possible point of departure for discriminatory action. But, in any case, each data may be appreciated only in the context where it effectively is situated.

6. Data protection and freedom of information

The analysis of the increasingly close links between data protection laws and laws on access to information makes it possible for us to reveal, on the one hand, the possibilities of enlarging and enriching the right of access; and, on the other hand, the expansion of this right well beyond the field of personal data. If one could consider as personal data information on the activity of a firm set up in the form of a legal person, it is not possible to affirm the same thing for other categories of data which are also important for the effective exercise of the right of access. For example, the case, already emphasised, of information on automated processing programs or on the models for automated decisions.

The effectiveness of the right of access appears therefore to be dependent above all on the possibility of having the largest amount of information possible on the activity of those who store data. But in addition (and from a certain perspective, especially), the right of access confirms its ability to be the instrument for increasing general transparency in the activity of public and private structures, by bringing about the institutional conditions for widespread social control. And it can be seen how the overall framework in which data protection policy has to be considered will be enriched.

That means, on the one hand, that the right to request access to certain anonymous data (or, more generally, impersonal) can also be recognised for parties other than those "directly interested" (by considering as "directly interested" those on whom data have been stored). The other parties can be those who have already been mentioned (trade unions, associations for civil liberties or for the protection of consumers, etc.): but, in this case, the preliminary consent of the interested parties should not be requested as there are no direct risks of violation of the private sphere: It is a matter of impersonal data which have been requested with the aim of social control. And it has already been seen how this type of control can also reinforce the global protection of the position of individuals.

Once having crossed this frontier, it will be found that the path towards a generalised access to impersonal data, which is the real aim of all the laws on freedom of information, levels out (always in principle). And the general finality of knowledge and control justifies the extension of the legitimation of access even to collective parties. For reasons which have already been indicated, those subjects, much more than individuals, have the possibility of guaranteeing a real social control, either direct (on data keepers) or indirect (on the different forms of data processing).

./.

The right of access, therefore, appears as the dynamic side of a right to information which can become concrete on the initiative of groups and individuals. Accordingly, we are witnessing an instrument which can determine or facilitate a distribution of power.

In this perspective, "administrative democracy" is not only being reinforced (Lemasurier, 1980). It is possible to deal with the more general theme of constitutional equality in access to information which immediately concerns organisation at the top of the political system (suffice it to reflect on the problem of access by parliaments to data generated by governments), but which will also spread through the whole of the institutional organisation. And at this moment it is necessary to take account of the theme of secrecy, by revealing the many exceptions to the right of access which are laid down in the different laws.

It is necessary to abandon in this field the very limited guidelines which have prevailed up to now and which are inspired by the criteria of the inaccessibility of citizens to all the data collected by certain structures (for example, the police, security services). Leaving aside rules on indirect access and on control by public bodies (the magistracy, ad hoc commissions, etc.) experience shows us that only a part (sometimes very restricted) of information stored by these parties is incapable of "tolerating" the right of access. In addition, by means of access better guarantees can be given that data stored are correct and that the archives are organised rationally (in regard to the American police, see Laudon 1980).

Consequently, there today appears possible a legislative evolution toward recognition of a right of access even for certain categories of data considered prohibited up to now for reasons based on principle, or simply prejudiced, rather than for real security reasons. The experience of a country like the Federal Republic of Germany shows that even the police adopts a more flexible approach by replying to three-quarters of the requests which are addressed to it (Simitis, 1983: 54).

Finally, if one begins to look at the relationship between enlargement of the right of access and the possibilities offered by the spread of the new technologies in society, the analysis is situated on the level of the determination of the new political dimension which can be created by the fact that these two evolutions are coming together. If individuals and groups have continuously increasing amounts of data and, at the same time, have directly at their disposal small and medium-sized computerised systems, they can, for example, construct models which simulate the effects of a public or private decision which has been taken on the basis of the very data in the hands of the decision makers; or they themselves can produce alternative models for a decision. And, by amplifying these operations, it is possible to go beyond the concept of transparency: one can pass from the traditional polemic of "open government" (symbolised by images such as the "glass house" or administration "in the sunshine") to that of "distributed" government.

It is a development which could allow for a link - neither theoretical nor fantastic - between technology and democracy.

./.

7. Towards a renaissance of consent

The stress laid on the circulation of information must not be considered as an indication of a very favourable attitude to rules which aim to eliminate all obstacles to the storage and diffusion of data. When one speaks of rules, it is very clear that one is also speaking of criteria to distinguish the cases where circulation is permissible and the cases where it is prohibited, with all the nuances between these two extreme hypotheses.

Among these criteria, there is undoubtedly the criterion which is aimed at the protection of privacy: indeed, a functional definition of privacy describes an instrument for limiting the circulation of information. But, in following the debate on the different definitions (Parent, 1983) it is noticed that privacy alone is incapable of providing a solid base for a precise rule on circulation of information: it is above all necessary to consider the social and institutional context in which the problem of privacy arises historically.

Today the reference to privacy is the indication of a value rather than a real legislative definition and this conclusion is confirmed by the fact that data protection laws do not contain any formal definitions of privacy.

It is however important to follow certain developments which have been precisely highlighted by the change in definitions. From the traditional definition as "the right to be left alone", we have passed, thanks to the problems raised by computer technology, to the definition which is the constant point of reference in the debates of the last years: "the right to control the use of my personal data by other parties". In the most recent period we are witnessing the emergence of another type of definition: privacy considered as "the right of an individual to choose what he wants to disclose to others".

It is quite possible that in the emergence of this last definition there is reflected at least a part of the worries and disillusionment which have followed the findings on the limits of a control which is entirely entrusted to the individual right of access (Bull: 1984). In this way, in addition, an attempt is also being made to develop an instrument for the reduction of the quantity of information stored by public and private bureaucracies, following a tendency which has been reinforced by the increase in storage capacity made possible by the new technologies.

We also see that attention is turning once again towards consent of the data subject, in regard to which the recent legislation on cable privacy accords a much more incisive role than the one recognised by the first generation of data protection laws (Westin, 1982; Flaherty, 1983). But also in the field of consent one can find important developments, as the technique of amplified consent is gradually abandoned in favour of informed consent, of which there have been more and more analytical specifications. And even the specific discipline of informed consent appears also as a totality of rules on the circulation of information, and more precisely, of information which must be given to a person if one wants his consent to be valid.

./.

The development of consent is confirmed by the recognition of a "right to informational self-determination"; and it is also confirmed when, in certain draft legislation or theoretical writings, "the presumption of confidentiality" of personal data is discussed. It is a presumption which can have two meanings: considering illegal any storage of information which, leaving aside legislative authorisation, has been carried out without the preliminary and express consent of the data subject; and, in accordance with a line of thought which is closer to the traditional notion of administrative secrecy, a meaning which emphasises the fact that information concerning a person may not circulate outside the competent administration (with a prohibition on its being passed even to other public bodies).

It is necessary to add that this renewed preference for consent can be explained by also considering the difficulties and suspicions concerning the possibility of establishing a complete system of authorisation and prohibition by legislative means. Consent thus appears as a way between regulation and deregulation.

Many of these theses can be criticised by using arguments already invoked at the time of my brief discussion on the problem of the market. One may add that another limitation of this position lies in its one-dimensional nature, in the sense that regulation of the circulation of personal data has as its point of reference merely a property dimension: These data are described as the exclusive property of the data subject who can freely negotiate their transfer. The other dimension has been completely overlooked i.e. the dimension which concerns the social consequences (also for the data subject himself) of an "indiscriminate" circulation of particular data or of data stored for particular purposes. What we are talking about is a problem which must be dealt with by considering values and interests and which cannot be reduced to the property denominator.

Next, all those arguments could be invoked which, historically, have been used by way of criticism of the "freedom" of consent in the context where there were conditions which excluded a real possibility of choice for one of the parties. In the case analysed here, the situation is very clear: the possibility of receiving certain services is not linked solely to the (consensual) transfer of certain information from the user to the provider, but there is also the possibility that these data will be processed so as to create new information which can be passed on to third parties. The providers of services by means of interactive media have a very great economic interest in the production of the new computerised commodity and may exercise pressure on users so as to obtain their consent to the elaboration and diffusion of individual and family profiles on the basis of data obtained at the time when the service was requested. This is an old problem, well analysed (and sometimes well regulated) concerning the mass production of goods and services: but, within the field which is of interest to us, it is not merely a question of taking advantage of that experience. Replies have to be given to very new questions.

./.

Indeed, leaving aside any evaluation of the issue of freedom of choice, one must also ask oneself if the sole technique of consent in the world of the new media does not contribute to the weakening of the social goods which are at the basis of privacy. And, in discussing this problem, it must be added that its solution cannot be sought by having recourse to the two definitions previously cited, one covering control and the other relating to the right of choice.

These definitions are neither of the real type (identifying precisely the object of protection) nor of the stipulative type (putting forward a rule so as to make the language of the legislator rigorous). It is a question of simple procedural definitions, the content of which is bound to change in accordance with the control powers and the possibilities for choice which the laws entrust concretely to data subjects.

8. Interactive media and circulation of information

The problems connected with excess in the collection of data and abuse in their processing can be dealt with by techniques which do not simply place their trust in consent alone. There are general orientations which confirm the necessity of adopting an articulated and integrated strategy.

The lines in legislative evolution are known. They indicate the rules for the circulation of data which are not related simply to the requirements of privacy protection but also to the efficiency and rationality of action by administrative structures. If it is thought that the private sector finds an obstacle in the cost for storing and processing of an excessive amount of data, it can only be thought that the public sector automatically follows the same logic. Ad hoc rules are therefore necessary.

In the first place a direct relationship is provided for between the aims of the parties who want to store information and the data which may be legitimately stored. Subsequently, there is an emergence of the more explicit and detailed force of administrative secrecy which aims to limit radically (or to prohibit) the circulation of data from one public structure to another (that is the technique adopted by the new Swedish Secrecy Act). An almost natural development of this tendency lies in the restrictive regulations on the possibilities of collaboration between public sector data banks.

Accordingly, there is a very clear line towards a functional approach in the definition of rules concerning circulation of data. On the one hand, the unlimited "licence to store", which had accompanied the activity of public and even private parties, will disappear. On the other hand, the monolithic vision of the public organisation will be abandoned: a consequence of a more general reflection which follows the differentiation of state functions after their expansion. It is necessary to recall that "the origin of the society characterised by files goes back to the time when the federal government (of the United States) began to intervene in the fiscal field and in the social security field. From that moment on,

./.

an ever increasing amount of data was required from citizens and stored. Suffice it to reflect quickly on the archives concerning federal intervention in social security and medical assistance, in support of the purchase of accommodation, in urban and public health improvement, so as to clarify this point, as well as the activities of the Census Bureau, the Defence Department, the Office of Economic Opportunities, the Job and Peace Corps and the Department of Housing and Urban Developments" (Miller 1971: 20-21).

Today, more so than in the past, because of the criticisms directed at the interventionist state and after the reduction of its presence in certain sectors, it is noticed that archives are a part of particular functions and, as a consequence, their use can be limited to the sector from which they originate. In this way, nothing is prejudged for the accomplishment of the function and, at the same time, one can safeguard the interests of the citizens in the use of the data which is related to the original aim of storage.

This tendency must also be reinforced so as to confront a phenomenon which, in the United States, has already dimensions which must give rise to concern: the purchase by the public administration of large masses of information collected by private organisations. "That means that the fundamental line of demarcation between public action, in regard to which there exists a constitutional protection for the citizens, and commercial activity, where there is no protection, has been irremediably wiped out" (Ellis, 1984).

Reflection is needed on the particular situation of the United States where there do not exist any general laws on privacy protection in regard to the private sector. But reflection is also of basic value by confirming the impossibility of working in this domain as if there were impenetrable barriers between the different data banks. Reality shows us that things are moving in exactly the opposite direction, towards the largest circulation of information between the various sectors and beyond the formal qualifications of such a sector or of such data bank.

It is necessary to place at the centre of our attention this global nature of the computerised universe which technological evolution is enlarging through time and which must constitute the true and essential point of reference of legal discipline. The choice of the path towards the global approach is also necessary so as to avoid undesired effects which can jeopardise the quality of data stored. In the face of the scope of the request for information and the possibility of circulation beyond the domain for which the information was requested, one can see in data subjects (the citizens of the United States in the first place) a reaction of self-defence manifesting itself: they will communicate information, inexact or distorted in part, insofar as this does not produce negative consequences.

There are nevertheless cases and sectors where that reaction of self-defence is not possible because of the technologies set up. That is true, as a rule, for interactive technologies, at least at the time of access to the data by the user and when services are requested. The total dependence of the provision of a service vis-à-vis the accuracy of the data communicated excludes falseness or else limits falseness to very secondary data.

./.

But it is precisely the richness, the precision, the actuality of data collected by the interactive technologies which give rise to the problem already cited of the new possibilities for secondary uses, of the creation of a new commodity, made up especially of individual family and group profiles, which may be transferred to third parties. In this regard there are certain questions which go beyond the traditional problem of privacy.

One may wonder if this production of automated profiles will bring about a weakening in the capacity to seize socio-economic reality in its richness and variety. One can reply that, on the contrary, it is precisely these profiles, always being renewed, which give us the concrete possibility of seizing, day by day, the real individual and collective interests. On this basis, it would be possible to place effectively at the disposal of each person whatever he wants, thus realising the conditions of substantial equality ("to each according to his needs").

At this point one can get a glimpse of the perspective of a system of production capable of giving increasingly rapid and coherent replies to the needs present in society and with an increasing individualisation of such replies. We are talking about a model which can be envisaged for the distribution of goods and services but which, because of the ability of new technologies for diffusion in all domains, could be found even in the political system.

There are no doubt positive implications in these developments which can lead to major efficiency in public and private action, and to an increasing harmony with social demands. But there are also other possible effects which must not be overlooked.

Has the rapid response to immediate needs effects which can be expressed in terms of real equality or will the tendency be more towards "freezing" each person in the position in which he finds himself, with very dangerous discriminatory effects? If for example it has been established that the majority of people in a district only read a certain type of literature there will be economic reasons which compel distribution to this district of only books and newspapers which correspond to the tastes and interests so verified. On the one hand, therefore, it is possible to institute a mechanism which can block the evolution of this community by freezing it around a profile drawn up in a determined situation. But, on the other hand, those persons who do not correspond to the profile of the majority are penalised, so producing a discriminatory effect on minorities.

Again the "categorising" of individuals and groups carries with it risks if no account is taken of "the nuances which come from the spirit of finesse, of feeling, of ethics" (Commission, 1975: 16; Kayser, 1984: 130).

A much more complex alternative than the one between privacy and the diffusion of individual data is seen to emerge. It is necessary to confront the possibility of an increasingly widespread social control which is exercised by public and private centres of power. In regard to

individuals, this control can give rise to serious obstacles to the free development of their personality which is frozen around historically determined profiles. And at the socio-political level, by promoting "conformist" attitudes, there is the risk of making the creation of new "collective identities" more difficult by weakening the innovatory capacity within the system. In both cases the price in terms of democracy would be by no means negligible.

Faced with all these problems, there are no easy solutions. However, if we remain on the specific level of rules on the circulation of information certain general lines can be indicated.

Once again the importance of the global approach must be emphasised. The case of the United States which has already been mentioned proves to us that the clear distinction between the public sector and the private sector - the one regulated the other unregulated - has produced a situation where the latter becomes a "private hunting ground", which is occasionally available for public powers. Can "data havens" arise even within national borders?

It is still the global theme which reappears in regard to processing of personal data as well as anonymous data, in regard to the distinction between individual privacy and group privacy. Faced with the new reality of profiles, these distinctions lose some of their meaning: whether because personal data which are "non-sensitive" in appearance can become very sensitive if they contribute to the construction of a particular profile; or because even the individual sphere may be "violated" in the case where one belongs to a group on which a negative profile has been constructed.

The line of regulation which can be drawn from laws and discussions is moving towards rules which reinforce the functional approach. The relationship between data and the finalities for which data have been collected has been highlighted. The limits and the procedural obligations (often bearing on the consent of the data subject) for the transmission of data and profiles to third parties have been established. Limitation periods for the conservation of certain categories of data are being provided for.

In this regard we will return to the theme of "the right of erasure" which has been discussed again and again in the years gone by. In stating the diffusion of the obligations to erase certain data after a fixed time limit, it is emphasised that there is the risk of restricting the historical memory of society. Another paradox. As the quantity of data which can be stored gradually gets bigger, is there also a decrease in the information which can be kept? As Martin Heidegger said in commenting on a phrase of Friedrich Nietzsche, "the organisation of a uniformly felicitous condition for all men will lead us to an emaciation and such emaciation will consist in 'the elimination of Mnemosyne'" - in the loss of history and memory as a consequence?

Although evocative, that argument is not justified. In the past, the interest in the conservation of information and the technical and physical capacity for keeping it have always been inferior to the mass of information which, at the time, was in reality collected. Today there is an unprecedented increase in interest and in the capacity to conserve; thus, at least from the purely quantitative point of view, the trace of information of our time will be superior to that of previous eras.

./.

After this finalisation of a general nature, we must add that rules on conservation of information must be established as a part (or premise) of the rules on circulation. Undoubtedly, the erasure of files on persons who have borrowed books from a public library or on the purchases made by a family during a certain period by videotex are losses which can afflict an historian involved in the compilation of annals or an enthusiast of microhistory. But, on the one hand, it is quite certain that a quantity of data capable of satisfying even these interests will survive. And, on the other hand, more particular attention for the regulation of archives - by prohibiting all commercial or administrative circulation and by providing for access for research purposes - is capable of leading to a balance of the interests at stake, especially by regulating the question concerning the deposit of historically significant information (documents) in the public archives run by independent bodies.

9. Towards an integrated legal strategy

Within the framework of an integrated data protection strategy, there is a particular place for the theme concerning public control bodies. It is self-evident that the utility of these bodies is contested by those who support an approach which is solely connected with the logic of the market. But, leaving aside the question of principle, suffice it now to underline that almost all the laws are moving in this direction (Burkert, 1982; Council of Europe, 1983; Flaherty, 1984).

It seems to me that general agreement on the position of these bodies in terms of "independent administrative authorities" (Sabourin, 1983) will form. Independence must be guaranteed vis-à-vis the government because among the most important tasks of supervisory bodies is precisely the control of data banks which are very closely connected to executive action eg the data banks of the police or the security services. From a technical point of view, that means that the supervisory bodies must never be nominated by the government (their composition in any case must never guarantee a decisive influence for those members nominated by the executive) so as to prevent ambiguous situations arising with the controllers who are controlled and thus compromising the credibility of supervisory action itself. And the institutional points of reference for these bodies should be parliament so as to guarantee, in addition, the maximum of publicity (and possibly discussion) for positions taken.

In order to guarantee independence, it is necessary to see to it that the supervisory body is placed outside the traditional administrative structures. Once again the reason is clear. It is precisely in the context of large public (and private) bureaucracies that one finds initiatives for data banks: the task of supervision must accordingly be structured in such a way as to divorce it from the very logic of the subjects who must be controlled.

The body accordingly seems like a "fenced off" institution in the system of data protection. One can appreciate this role more clearly if one considers that a task of necessary supervision is in issue in the sense that only this body can accomplish a general and continuous supervisory task. The other subjects who are recognised and authorised - individuals

./.

and groups - can only realise a possibly fragmented supervision. But we cannot draw from this finding that the existence of a formal centre of supervision makes widespread control quite useless for it is precisely the presence of these different types of control which can constitute an antidote for the case where formal supervision becomes schlerotic or is influenced by public and private pressure groups. Furthermore, the supervisory body looks like an institution which is in principle purely functional: in principle, for the multiplicity of possible functions can be reduced in reality by legislative limitations on its competences or by renunciation, whether voluntary or imposed, of the exercise of some of the powers which have been formally attributed to it. Indeed, from reflection on the legislative directions as well as on known experiences, one can draw certain conclusions on the tasks which have been correctly accomplished by the supervisory bodies: "watchdogs" of the legality of action of those who store, process and circulate data (whether in exercise of a power of general or special authorisation or through on the spot supervision); consultative bodies for public (and even private) powers so as also to promote consensus in the determination of rules on the circulation of data; institutions for the resolution and/or for taking the heat out of conflict; bodies with an autonomous normative power or else with regulatory power for the adaptation of principles fixed by law.

In reality, the concrete physiognomy of these bodies results from the way in which its functions (and possibly others) begin to be combined inter se. To this end, it is the legal technique which is used which can play an important role and not just the political and institutional context (a tendency towards regulation or deregulation: rigidity or flexibility in the system of legal sources; constitutional attribution to specific bodies of the competence to deal with conflicts in the field of individual rights, etc.).

Today, because the experience of previous years shows us the rapid obsolescence of regulations which are too rigid and focuses our attention on institutional instruments which are much more flexible, it is therefore possible to schematise the general characteristics of the legal milieu in the field of the circulation of information:

1. a basic legal discipline whose core is essentially made up of "general clauses" and by procedural norms;

2. particular rules, preferably laid down by specific laws, which concern the activity of determined subjects and the status of certain categories of information;

3. an independent administrative authority, competent as the case may be to adapt principles contained in the general clauses to concrete and new situations;

4. a right of appeal to the judicial authority should be provided for, not only in the systems where there exists a constitutional obligaton, but as a matter of principle, so as to give rise even in this domain to principles analogous to those of a Bill of Rights or of Due Process, in accordance with a line which relates many aspects of the field of computerised information to the field of civil liberties;

./.

5. a widespread control should be provided for and entrusted to the initiative of individuals and groups.

This type of integrated strategy, through the combination of its various elements, could promote an institutional flexibility corresponding to the great flexibility produced by technological innovation. Within this framework, even the role of the supervisory bodies can be defined in a clearer manner.

Indeed, this role is bound to increase if legal regulation, beyond the narrow guarantee of privacy, becomes a more general discipline for the circulation of data. Thus we return to the theme of the structures and the means which must be given to the supervisory body if we want it to accomplish the tasks which are entrusted to it.

10. Polls and power

The expansion of the discipline towards a general regulation of the circulation of information must take account of the way in which that circulation is influenced by the various technologies employed. Without making inventories at this point, it can be noted, in principle, that reflection on technological means has compelled the abandonment of the "total" or "monolithic" approach of the first generation of laws and has contributed to the development of an attitude which is more favourable to distinctions. If these two elements are considered together - the more and more general nature of the basic legal discipline, the possibilities offered, and the distinctions imposed by the new technologies - it is possible then to draw indications in two directions. The first direction shows us that the rules on the circulation of information reflect in an increasingly clear manner the protagonists in the different operations, the ways of collecting and processing data, the aims in comparison to the technical method employed. That means, in certain cases, the adoption of a more flexible line: that is the example that it is possible to draw from the experiences of countries who have already laid down an exception to the obligation to register (or be authorised) in cases where data are processed by an individual for strictly personal purposes. On the contrary, there are situations where legislative evolution is aimed at more severe rules as in the case of information collected by interactive means (videotext, cable T.V.), where henceforth the transfer of information by users constitutes an integral part of the use to which these means are put (there is a recording of the simple fact of an interrogation or of the choice of a television channel).

The second direction leads us towards the finding that the new technologies can enlarge the possibilities for action by citizens, users of telematic services, owners of personal systems for data processing. Considered in this perspective, the right of access does not merely involve the possibility of collecting personal or anonymous data but also the possibility of controlling the degree of procedural development, of participating in certain decisions, of intervening in the management of certain systems. In this regard, it is necessary to underline the importance of the recognition by the laws of certain countries of the right to know and the right to challenge the criterion for the request and processing of data (in France, in comparison with data on taxes on large fortunes; CNIL, 1983: 28). This indication will reinforce the thesis on the necessity of allowing data subjects to participate even at the system's planning phase.

./.

One now sees more clearly, although the examples are very schematic, how rules on the circulation of information can concern the distribution of power. Given that we are dealing with a redistribution according to the fundamental resource for the social, political and economic organisation, these consequences can be on a fairly remarkable scale.

It may be that global transparency in public action is on the increase. At least, in principle, there are more parties holding a power of control. The information received from these parties, originally destined solely to promote a control function, will increase the capacity to intervene in the decision and management procedures especially at a local level.

It is still not a question of linear developments. Technical problems, insufficiency of financial resources, and political resistance can check, more or less perceptibly, an evolution of the information discipline towards effective forms for the redistribution of power. And that means that, here as elsewhere, it is not possible to place confidence solely in the technological evolution for once again we are confronting processes the conclusion of which is destined to change in accordance with the way in which they are governed.

Certainly, the passage from the technology of large computers to distributed information processing and thence to the personalisation of information processing makes the opposition between centralisation and decentralisation seem "ideological" and typical of the debates of the 1970's. But, once again, one must be suspicious of simplifications. As in the past when people proclaimed that communism was "electrification plus the Soviets", people today affirm with as much simplicity that socialism will be "telematics plus decentralisation".

Reality does not invite us to be wise but to be attentive. There are forms of decentralisation and of diffusion of the interactive technologies which can be used solely to promote a vertical communication between isolated citizens and the structures at the summit: entrepreneurs, providers of services, political leaders (Rodotà, 1982: 136). The circulation of information discipline and the intervention of citizens in the planning and management of certain systems can, on the contrary, facilitate the birth of forms of horizontal communication which will be increasingly indispensable as the information society gradually erases or radically changes the ways of establishing relations between individuals and the mediators (party, trade union) which are typical of the traditional mass society. This is a difficult evolution because it runs into the resistance of power holders who sometimes, instead of explicit opposition, try to channel the electronic participation of citizens at the local level towards a reinforcement of community action alone rather than towards the enlargement of political participation (Dutton et al., 1984).

An increasingly particular attention for the problems of the socio-political organisation, in comparison with the traditional problems of the protection of privacy, does not only reply to a need, more generic than general, to look at the problem of the circulation of information in its totality. It is the evolution of the most recent laws and draft laws which confirms for us the impossiblity of ignoring this side of the analysis.

./.

Opinion polls already offer us a significant area for reflection for there are at the same time direct consequences for privacy and, more generally, for the relations between individuals and the socio-political organisation. Indeed, laws and codes of practice are already putting forward rules in the field of opinion polls (Westin, 1982; Flaherty, 1983: 71-76); and Article 11 of the Staatsvertrag prohibits any poll conducted by a videotext in areas within public competence.

Confirmation of the link between the private dimension and the public dimension could not be clearer. And once again this compels general reflection so as to clarify the framework where specific rules on the circulation of information may be situated.

Once the appropriate technology has been established, the frontier between polls which are termed "commercial" and polls which are termed "political" could be crossed without any difficulty. The bases for these polls can be simplified and the frequency can be intensified so as to construct hypotheses on generalised polls on all sorts of themes. The first effect produced by such a practice could be a fundamental shift of attention from election time (one off or periodic) towards polls (multiple and repeated again and again at any time). But the replacement of an institutional mechanism (the election) by another non-formal institution (the poll) could also have effects on the institutional system in the proper sense of the term: suffice it to reflect on the neurotic dependence on polls during Carter's presidency or on the possible bearing of polls on votes (which gives polls themselves the value of a discipline and could really be a prelude to their partial institutionalisation). More specifically, the repetition of polls reveals a sort of "permanent social contract" which could have bearing on the role of elected representatives and which could bring about the problem of the gulf between the results of polls and the deliberation of representative bodies.

Criticism of the generalised practice of polls has been very clear and it can be related to the observations which have already been formulated. Basically, such a practice would stimulate the atomisation of society and the cleavage in horizontal communication because it would be the fruit of the formation of a political will outside groups and would reinforce the links between the élite and the individual (there would thus be the reinforcement of a tendency which is already produced in televisual communication). In addition, judicious (or prejudicial) recourse to the technique of polls could be used thanks to successive adjustments which direct public opinion towards the results desired by the promoters of the poll; or, conversely, the poll could be proposed precisely so as to stimulate a refusal reaction on the part of public opinion.

While recognising the undoubted relevance of all these problems, the real question is found beyond (or on this side of) these problems. It can be reduced to the following questions: who proposes the poll? who determines the object of the poll? who formulates the need? who determines the time? what information and what discussion will precede the poll?

./.

Analogous questions can be put forward in relation to another institution which should be concretised by Citizen Democracy - instant referenda. The risks of plebiscite democracy become horribly concrete; but in order to evaluate them seriously, reflection is necessary on the methods and level of electronic referenda without succumbing too much to the temptation to eliminate them en bloc and once and for all.

I believe that the major weakness of the institution is principally to be seen in the orientations which are still indicated by many researchers, as for example the orientations which best characterise the use of the referendum. People generally cite the case of a decision on the death penalty which seems to be precisely one of those questions which must be evaluated with the greatest prudence. Here the interweaving of the various information technologies can bring about decisions which are based on purely emotive reflexes and which are liable to be completely turned upside down by the presence of an opposite stimulus. By way of example, we can think of an electronic referendum carried out just after television has depicted a place ravaged by a terrorist attack, with the bodies of the victims, the despair of the parents; or after witnessing a documentary concerning, thanks to his success as a writer, a person condemned to death and revealing his horrible agony in the electric chair or the reaction of his wife in her home.

It will be said that these risks are linked to the use of referenda and it is true that communication technologies incite them, whether because of the way in which the problem is presented or because of the very brief state which can be produced between the production of the emotion and the expression of the vote. This distortion can be eliminated or limited when the interest of the voter is more directly at stake; a vote on the track of a metro line, its stops, certainly cannot be influenced by emotive factors.

The question then becomes, on the one hand, one concerning the relationship between the electronic referendum and voters' interests and, on the other hand, the degree of critical information at the disposal of voters and the possibility for them to discuss and to evaluate. By just placing the accent forcefully on this second aspect, it is possible to draw a conclusion which would tend to circumscribe the use of the referendum to secondary matters or to sectoral arguments.

At any rate, all these techniques raise the problem of communication and, from that moment on, of the formation of political will in an uniquely vertical form. What allows a perspective of this type to be discerned is the progressive decline in the role of the social mediators (parties, trade union, elected representatives, journalists or vendors). Will the "electronic terminal house for large systems", including the ballot box, not transform mass democracy into a living-room democracy?

BIBLIOGRAPHY

BARAN, Paul (1965) - Communication, Computer and the People. Santa Monica: Rand Corporation.

BOBBIO, Norberto (1980) - "La democrazia e il potere invisibile", 10 Rivista Italiana di scienza politica 181.

BULL, Hans Peter (1984) - Datenschutz oder die Angst vor dem Computer. München: Piper.

BURKERT, Herbert (1982) - "Institutions of Data Protection". 3 Computer Law Journal 167.

COMMISSION DES COMMUNAUTES ECONOMIQUES EUROPEENNES (1983). Data Security and Confidentiality.

COMMISSION INFORMATIQUE ET LIBERTES (1975). Rapport au Président de la République. Paris : La Documentation française.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (1983) 3ème Rapport d'activité. Paris : La Documentation française.

(1984) 4ème Rapport d'activité. Paris : La Documentation française.

CONSEIL DE L'EUROPE-CAMERA DEI DEPUTATI, Législation et protection des donné Roma : Camera dei deputati.

DAVIS, Robert C. (1973) - "Confidentiality and the Census, 1790-1929", in U.S. Department of Health, Education and Welfare, Records, Computers and the Rights of Citizens 178.

DUTTON, William et al. (1984) - "Electronic Participation by Citizens in US Local Government", 6 Information Age 78.

ELIAS, Norbert - "Utopie scientifiche e letterarie per il futuro", 4 Intersezioni 5.

ENZENBERGER, Hans Magnus (1979) - "Unentwegter Versuch einem Ausländischen Publikum die Geheimnisse der deutschen Demokratie zu erklären", Kursbuch n° 56.

FLAHERTY, David H. (1983) - Protecting Privacy: Data Protection in Two-Way Cable Television Services (unpublished draft).

..... (1984) - Limiting Governmental Surveillance and Promoting Bureaucratic Accountability: the Role of the Data Protection Agencies in Western Societies (Paper for the Annual Meeting of the American Political Science Association).

GARDNERS, Sidney L. and WHITE, Robin (1983) - New Technology and the Right to Privacy: State Responses to Federal Inaction. A Report to New York State Consumer Protection Board. New-York: New-York State Consumer Protection Board.

KAYSER, Pierre (1984) - La protection de la vie privée. Paris: Economica.

LAUDON, Kenneth C. (1980) -Management Practices and Data Quality in Criminal Justice Information Systems. Washington D.C.: U.S.Congress, Office of Technology Assessment, National Information System.

LEMASURIER, Jeanne (1980) - "Vers une démocratie administrative. Du refus d'informer au droit d'être informé". Revue du droit public et de la science politique en France et à l'étranger 1239.

LENK, Klaus (1982) - "Information Technology and Society" in Friedrichs, Ganter and Schaff, Adam (ed.) Microelectronics and Society. For Better and Worse. Oxford-New York-Toronto-Sidney-Paris-Frankfurt: The Pergamon Press.

MARCUSE, Herbert (1941) - "Some Social Implications of Modern Technology" 9 Studies in Philosophy and Social Sciences ("Zeitschrift für Sozialforschung) 414.

MILLER, Arthur R. (1971) - The Assault on Privacy. Ann Arbor: The University of Michigan Press.

NOZICK, Robert (1974) - Anarchy, State and Utopia. Oxford: Blackwell.

PARENT, W.A. (1983) - "Recent Work on the Concept of Privacy" 20 American Philosophical Quarterly 341.

POSNER, Richard A. et al. (1980) - "The Law and Economics of Privacy" 9 The Journal of Legal Studies 621.

RODOTÀ, Stefano (1982) - "L'informatique est-elle politiquement neutre?" in Une société informatisée: pour qui? pour quoi? comment?. Namur: Presses universitaires.

SABOURIN, V.P. (1983) - "Les autorités administratives indépendantes, une catégorie nouvelle". Actualité Juridique 275.

SIEGHART, Paul (1983) - "Intervention" in CONSEIL DE L'EUROPE.

SIMITIS, Spiros (1983) - "Intervention" in CONSEIL DE L'EUROPE.

.... "Die Informationnelle Selbstbestimmung-Grundbedingungen einer verfassungskonformen Informationsordnung" 37 Neue Juristische Wochenschrift 398.

SMITH, Robert Ellis (1984) - "Statement" in U.S. Congress, 1984: Civil Liberties and the National Security State (Hearings before House Judiciary Committee. Sub-Committee on Courts, Civil Liberties and the Administration of Justice). Washington D.C.: U.S. Government Printing Office.

YUDOF, Mark (1983) - When Government Speaks: Politics, Law and Government Expression in America; Berkeley: University of California Press.

WESTIN, Alan F., "Home Information Systems: The Privacy Debate" 28 Datamation 104.

TECHNOLOGICAL DEVELOPMENT AND ITS CONSEQUENCES FOR DATA PROTECTION

by

Mr Hans CORELL

Chief Legal Adviser
Ministry of Justice, Stockholm
(Sweden)

INTRODUCTION

1. This report is intended to serve as a basis for a discussion, the theme of which is entitled "Beyond 1984. The law and information technology in tomorrow's society". It is my hope that the report may also serve as a guide for the deliberations which will have to be made in those countries where no positions have yet been taken as to the framework of data legislation. An attempt is also made in this report to demonstrate feasible approaches to the problems created by the swift technological development, also by countries which already have instituted such legislation.

Those who are well informed regarding the issues presented in this report may perhaps not find very much news in it. Still, it may hopefully contribute to a systematic review of the issues involved, issues which sooner or later will call for a solution.

This report has been prepared on behalf of the Council of Europe. It reflects my personal opinions only. However, I have been asked to deal with the situation in the Scandinavian countries in particular.

2. Within the scope of my assignment it is also necessary to draw a distinct line between my subject and the issues which will be discussed by the other rapporteurs to the Colloquy. This task has created certain difficulties, since the issues are often intertwined and dependent upon one another. Thus, the reason why this report does not include analyses and conclusions relating to such factors as the political and economic development, the development on the labour market and of the working environment, issues regarding business secrecy, computer related criminality etc, is that these issues do not fall within the scope of this report. Another limitation is that the report should be approximately 20 pages.

Recognising these premises, we will try to tackle the problems. For those who do not find time to read the entire report, there is a summary, see Appendix I. However, those who only read this summary will miss "The Elephant".

THE BASIS FOR THE PRESENT SYSTEM

3. The history of the present data legislation - extending over a period of 15 years - is by now well-known. There are clear parallels between this legislation and closely related statutes on secrecy for the private as well as the public sectors. But the invasion of computers triggered the development. Even though rules do exist on manual data files in some data laws, all these laws contain rules which give special heed to the dangers to privacy which computers are considered to create.

The latter fact constitutes the starting-point of the international agreements within this field. The first ones coming to mind are the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, prepared under the auspices of the Council of Europe, and the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, which have been adopted by the OECD. (These documents are enclosed as Appendices II and III, respectively. They will henceforth be referred to as the 'Convention' and the 'Guidelines', respectively. I will also use the terminology applied in these documents.)

4. The elements of what may be described as data protection ("protection des données") may roughly be broken down into: the demand for data quality, the demand for data security and the demand for participation by the individual concerned. These elements are easily discernible in the documents mentioned, and in national data legislation.

5. In this context, it may be proper to issue a warning against comparisons between "data legislation" in various countries. At closer range, one will soon find that the elements which together form the data legislation of a country may be dispersed over many areas within the entire system of the national legislation. Comparative studies must consequently not be limited to titles such as "Data Act", which may be found in the national Codes of Law.

6. It should also be stressed that national legislation on freedom of information and access to official documents to a large extent decides what boundaries the protection of privacy may have, when assessed comprehensively. By this, I have no intention of diminishing the importance of data protection also within the private sector. But, by and large, it is the files kept by the public administration which are of the greatest importance when considering the protection of privacy.

7. However, the rules now in force nationally as well as internationally are commonly based on experiences and perceptions of a technological development which is long since surpassed by a wide margin.

COMPUTER TECHNOLOGY - A POSITIVE ELEMENT IN SOCIETY

8. When discussing various problems concerning the protection of privacy, one easily creates an impression of being negative towards EDP-technology as such. Before dealing with the topic of this report, I therefore want to stress - if only for the sake of balance - that one should always pursue the positive results of technological development. Computer technology has already proved itself in practice to entail many advantages. Attaining a good protection of privacy by resistance against this technology is as futile as it once was to fight against the telephone, the car, and the aeroplane or - for that matter - the windmill.

What is important is to create an increased awareness not only of the advantages of this technology, but also of its dangers. It has been said many times before, but it deserves to be underlined again: The interplay between politicians/legislators, lawyers, administrators and technicians must improve. It is not enough that the latter thoroughly inform themselves about existing rules on the protection of privacy; they ought to be the first ones to realize what risks are inherent in the new domains conquered within the technological field.

9. One must also bear in mind, that every new technology creates problems initially. The problems may perhaps not disappear, but they may be made manageable as the set of rules and standards grows. As a reminder, it may be mentioned that the yearly number of casualties from traffic accidents in Sweden in the mid-thirties was 350, while the number of automobile vehicles was 200 000. The corresponding figures for 1983 were 800 and 3.5 millions, respectively. The decrease is thus seven times, which according to the scientists is typical internationally if one takes a comparative analysis.

./.

EDP-TECHNOLOGY-PRESENT SITUATION AND EXPECTED DEVELOPMENT

10. The aim of this section is not to explain new techniques. Nor is it necessary for the purpose of this report to analyse these techniques too deeply. Rather, it is thought by many that the approach so far has been much too obsessed with certain traits of the technique used. This approach has then led to problems as regards the application of the legislation.

A better approach would probably be to concentrate on the achievements made possible by this new technique, to investigate what effects these performances will have, and to use the result as a basis for the discussions ahead. Of course, the trend of the development regarding public and private administration must also be taken into account in this context.

In the following, I will indicate some technological facts which I consider important for the framing of the protection of privacy. For each, I will also point to the qualities which create a potential danger of invasion of privacy.

Smaller, Cheaper, and Easier-to-operate Computers

11. The trend is that computers will go on getting smaller and cheaper. At the same time the possibilities for communication between these small computers themselves, and between small computers and larger data bases are improving. Computers - even fairly powerful ones - are becoming the property of each and everyone.

The problem with this is twofold. Possibilities open up for more and more people to have their computers linked to different central data bases. If these bases are not sufficiently protected, the risks of non-authorised persons acquiring information will increase (cf. para. 23).

The second problem stems from the possibility of transferring large quantities of information in a matter of seconds and to compile new files out of existing ones; the possibility resulting from the large storage and processing capacity of small computers when combined with an advanced communication technology.

Larger Storage and Transmission Capacities

12. The capacity of computers to store and transmit information has grown substantially. With this increase in capacity there is less incentive to transfer information to micro-fiche or other less accessible storage media. It will also probably be easier to have access to older information, also on-line.

Decentralised Systems

13. The trend is pointing towards more and more decentralised systems, which may be linked to central data bases within one's own administration or to external bases (information systems, etc.). These changes will increase the risks of unauthorised acquisition, not only through the staff of one's organisation but also by strangers/third parties. (Cf. what I have just said about the smaller computers.)

./.

Possibilities for Transmission of Graphic Material

14. Digital technology makes it possible also to store and process graphic material to an extent which was earlier inconceivable. The use of video surveillance systems is increasing.

The risks here are that the behaviour of individuals in various circumstances are registered and stored in a way which makes it possible to have quick access to compilations pertaining to those individuals.

Development of Communication and Computer Networks

15. Large investments are being launched in various areas to enhance communication and computer networks. Fibre optics should be mentioned in particular. Through this development the capacity for transmission is increased. New possibilities are opened up for two-way communication.

Cable-TV

16. The development of distribution of TV by cable (especially two-way-systems) has advanced far in certain areas. By this technique there is a risk that the distributors will get information about the customers' viewing habits.

Satellites

17. Communications, etc. are increasingly achieved by satellites. This may possibly create special problems in regard to the rules on transborder data flow. I am, however, assuming that satellites may also be used for intercepting signals from data-communications in general.

Computerised Telephone Conferences. Electronic Mail. Computerised Communication of Written Information

18. In this area a very rapid development is surely to be expected. There is an impending risk that those who operate these communications systems will have access to the information being transmitted. One must assume that the danger of 'tapping' is greater within this field than in ordinary telephone conversations.

Electronic Funds Transfer and Supply Systems. Teledata

19. Also in the area of funds transfer and supplies, a development which will involve most individuals is to be expected.

The inherent dangers from this development are that those who operate the systems in this field will be storing information on their clients' choices of goods and services. Thus, as an example, information about transactions may be stored by the bank and also - possibly - by the retail trade. Out of this an obvious danger will arise that the private lives of the clients may be traced in detail (travels, hotel and restaurant visits, purchases, etc).

./.

Voice Recognition. Fingerprints, etc.

20. The development of what is called "pattern recognition" has perhaps not yet advanced so far as to be generally applicable. But also in this area one should take into account that it may only be a matter of time before this technique will be widespread. Once computers can interpret the spoken word, it will mean a major break-through, at least in the area of office automation. I will at present not denote any special dangers to privacy following from this technique; instead I would like to refer this issue to the coming discussion.

Remote Maintenance. On-line Diagnoses

21. Through this technique, it will be possible to acquire services and maintenance on computer systems by retaining persons who will - by use of a computer which even might be situated in another country - be working on-line on the customer's computer installation. It is obvious that a person retained will also have the possibility of gaining access to the information available. Special problems also occur for the application of the rules on transborder data flow.

Increase of Soft-ware Supply on the Market

22. The foreseeable increase on the market of computer programs constitutes a potential risk that the public will be able to 'break into' other data bases and communication systems. There are already programs available for "code-forcing". The programs will also in general be more sophisticated.

Crackers

23. Experience already shows that many persons find it challenging to try forcing barriers and cracking codes in order to gain access to various data bases. To some people this is an end in itself, but sometimes their goal is also to sabotage the base once the barrier is forced. There is an obvious risk that these so-called 'crackers' will be way ahead of many ordinary computer users on the market.

THE CONCEPT OF DATA PROTECTION

24. The concept of data protection (protection des données) is given in the Convention (art. 2) where it is the comprehensive term for every individual's "right to privacy, with regard to automatic processing of personal data relating to him" (le droit de toute personne physique "à la vie privée, à l'égard du traitement automatisé des données a caractère personnel la concernant").

I will not embark on any discussion of this definition, even though I know that many are critical of the concept of privacy (la vie privée) not having been analysed more throughly in data legislation. I will rest content with calling attention to the fact that this concept caused much discussion during the preparatory work within the expert committees of the Council of Europe and of the OECD, without any universal and lasting result being reached.

Either one has to respond the way the English judge did, who - when seised with exactly this problem - answered that, although he did not know how to define an elephant, he would surely recognise one if he saw one. Or, one could gain a

./.

perception of this concept by analysing the separate parts of each of the two international documents which aim at being guides for national legislative efforts. I will choose the latter alternative, since I imagine that it is the more constructive one; both documents are well-known. I will, however, also return to "The Elephant".

TECHNOLOGICAL DEVELOPMENT AND DATA PROTECTION - SOME GENERAL REMARKS

25. The Convention and the Guidelines contain, as everybody knows, basic principles for data protection. My intention is now to examine these principles one by one to investigate what impacts technological development has brought and - as far as I am now able to survey - will bring to our efforts to meet the demands which are made.

Before making this scrutiny, I would however like to make some observations which are important, at least for the assessment of the development within the Scandinavian countries.

26. Data legislation emerged - especially in Sweden - during times of expansion. When various demands - including the demand for protection of privacy - were put forward by the public, the politicians had no difficulties in meeting them. EDP-systems were relatively few and easily monitored, and the system for protection came to cover them all, even though this perhaps was not necessary. Bearing in mind the development which has taken place since then, one realises that it would now be very expensive to continue down this road.

In the austere economic climate of the past few years, the cost-effects of data protection have come into focus more poignantly. In these costs I am not only including those resulting from monitoring activities which are carried out by special agencies (Data Inspection Authorities) or through other supervisory devices which are established to ensure enforcement of data legislation. Other aspects are coming into the picture as well.

27. One obvious observation is that technological development is demanding more and more control not only because of the multiplying data files, but also because of the need for a more thorough control. But one may also observe indirect effects.

The framework of rules in society is becoming increasingly complex. Through regulations in various areas, notably in the field of taxation, demands for more efficient measures to enforce these rules have increased. In times of economic decline, such demands will stand out in the political debate. The Parliament and the Government are strongly urged to act vigorously against tax and welfare fraud, economic criminality etc. At least this has been the case in Sweden.

Such demands are often at odds with rules on protection of privacy. On balance, today there are surely many who are prepared to give up certain elements in data protection; the interest to trace and punish the "disloyals" tips the balance. They are prepared to give up their own right to privacy to enable society to get at these individuals. "The Elephant" has changed its shape!

./.

The result is that the ongoing debate nowadays is not so much concerned with what rules should be governing the collection, storage and processing of "special categories of information" (cf. the Convention, Article 6). The issues coming into focus are what rules should apply to "ordinary information" collected for a specific purpose, but which - at a cursory assessment anyway - would also be used for other purposes (e.g. control). The result is increasing demands for the matching and multiprocessing of various data files. Such processing immediately creates difficulties to maintain data quality which often will deteriorate, if data are used for purposes other than the ones they were originally collected to serve.

28. Another observation is - and this may be the case in Sweden especially - that, in time, Government authorities have acquired possession of more and more information, all the more accessible, about citizens. This information represents a capital, which could be utilised by these authorities (in the end by the Exchequer) through sales to private enterprises (insurance companies, advertising agencies, car dealers, etc.). This situation, combined with the right - in Sweden, a constitutional one at that - for individuals to request information about and copies of all official documents (i.e. most of all the information on file with the authorities, unless classified under secrecy laws), has resulted in vast amounts of information being made accessible to the general public through the authorities.

29. A contributing element to the opinion that data processing, and file matching in particular, are a very rational form of administration is the civil registration number. Such numbers exist in various forms in several countries, even though the rules for their use may vary. Such numbers are to be found in all the Scandinavian countries. The right to use them is more restricted in Denmark and Norway than in Finland and Sweden, however.

30. To conclude, one could say that the debate on privacy, which during the 1970's led to the data legislation of Sweden and other countries, has stabilised itself during the 1980's, concentrating on the issue of file matching for control or other similar purposes. It therefore seems natural to discuss whether this should also be reflected in the future legislation.

TECHNOLOGICAL DEVELOPMENT AND BASIC PRINCIPLES FOR DATA PROTECTION

31. I will go through the basic principles for data protection which are laid down in the Convention and the Guidelines, in trying to analyse what impact the technological development indicated above will have on the possibilities to meet these standards in reality.

The Principle of Fair and Lawful Data Collection

(Convention 5 a; Guidelines 7)

32. There should be no difficulties in living up to this principles as long as the collection is done directly from or with the participation of the individual.

./.

The development shows, however, that this way of collecting data is both expensive and impractical - especially when the same information is already stored in someone else's computer. Tendencies are that data are being collected to a greater extent without the participation of the individual. Within the Scandinavian countries there are examples of such file matching being effected by linkages of various data bases designed for different purposes. This technique may seem rational. But it creates imminent dangers that the information at times will be found to be useless or perhaps completely incorrect when it is to be used within a new context.

Since it may be assumed that possibilities for data collection will expand in this way, as a result of the increasing volume of information stored on machine readable media, as well as a refined technique for file matching, I find the development worrying. There is an urgent need to try in every way possible to avoid the dangers to privacy inherent in this technique. In my opinion it is doubtful whether the method should be allowed to the extent now practised.

33. One solution discussed in Sweden is to prohibit, by law, all file matching for control purposes which are not sanctioned by law (or ordinance). Such a prohibition could be combined with a requirement of specific security measures for file matching and of information in advance about security measures to be used for the control.

Another possibility is that this activity will be self-corrective: if errors frequently occur, the rationality of this technique will decrease and turn into its counterpart. The problem is that this will probably occur only when the border-line of what is "fairly and lawfully" ("loyalement et licitement") has long since been passed. This, of course, is not acceptable.

34. It should, however, be emphasised that the problems involved should not be exaggerated. It is easy to conjure up terrifying visions. At the same time, it should be noted that the number of actual infringements, in Sweden at least, is very minor indeed in comparison to the volume of data being processed.

The Principle of Purpose Specification

(Convention 5 b; the Guidelines 9)

35. As I have already noted, the technological development will create further obstacles to the fulfilment of this principle. Through the increasing possibility of file matching, demands for efficiency in data processing will grow even stronger. The issue is then how to construe the prohibition on use of data for purposes "incompatible" with the purposes for which these data were originally stored.

It is to be assumed that the legislator may be exposed to hard pressure by administrators as well as others, whose task it is to look to rationality and costs. At the same time one must take into account a change of attitude among the general public, which would - at least for the time being - be prepared to consider several purposes "compatible", if they only aim at correcting certain elements within the society (cf. para. 27). However, it is difficult to assess the durability of such an opinion; changes of attitudes may occur rapidly.

./.

The Principle of Data Quality

(Convention 5 c and d; Guidelines 8)

36. This principle - in the Convention it is used as a headline for the entire Art. 5, by the way - is closely related to the preceding principles and the next two succeeding ones. The criteria used to describe the requirements of the data are: adequate, relevant, accurate, and up to date (adéquates, pertinentes, exactes et mises à jour).

Experience shows that this principle encompasses several problems, especially in cases where data are processed with a view to attaining decisions on the rights and obligations of the persons registered. As has been demonstrated above, the greatest dangers arise when the information has not been collected from the individual, but from another source. It is obvious that violations of justice may occur in such situations.

In reality it is not a rare phenomenon to find that a piece of information stored under a specific heading in one file (fichier) does not correspond at all to another piece of information stored under the same heading in another file. An example may be rendered: "income" has several different meanings in Sweden. The result, if comparisons are made after data file matching, may be errors, misunderstandings and ambiguities, which have to be subsequently corrected.

37. A special risk is involved when one data file is matched and processed with a second one for control purposes. Such matching has been performed in Sweden (by special authorisation) with a view to preventing welfare fraud of various kinds. The result was, however, that some individuals were suspected of offences - suspicions which later were found to be unjustified. Criminal charges have on occasion led to acquittals, because of the imperspicuity and complexity of the system of welfare grants. In these cases it is possible to conclude that the complex welfare system was the cause of the discomfort of the individuals, not the matching as such.

38. Another effect of bringing one data file up to date by using data from another file is that faulty information might be disseminated. Experiences of this have been gained from credit report enterprises, whose files rely on acquiring information from data files operated by the courts or by the enforcement agencies. If the credit report files contain faulty information, it could have devastating consequences for persons who are dependent on having a good credit rating or good business relations in general. Examples exist where errors have been corrected, only to be reinstated again after renewed matching with the file (e.g. containing addresses) from which the errors originated, the errors still remaining in that file.

This is a problem which will multiply proportionally to the increase of complexity in the pattern of data matching. There is a risk that it will not be possible after some lapse of time to trace the origin of an error or the person who is responsible. Such a development violates the principle of accountability (see para. 51 below) and is not acceptable.

./.

The Principle of Use Limitation

(Convention 5 b; Guidelines 9 and 10)

39. As to this principle, please refer to my observations in para. 35 above.

The Principle of Non-excessive Storage of Personal Data

(Convention 5 e)

40. There is so far not much experience gained in this area. The basic opinion is probably - within the public as well as the private administration - that personal data should not be preserved at all if they are not needed for the activities of the administration in question.

Regarding data stored for scientific research and statistics, experiences show that there is an interest in having these data pertaining to individuals. This wish is especially strong where longitudinal studies are concerned. On the other hand, there is here a possibility for protection of the individual by coding and other measures (see below).

It has been said in the Swedish debate that vast collections of identifiable statistical data might entail risks of abuse in times of political upheavals or wars and that such collections should therefore be prohibited by law. In Sweden, however, we have always - at least until now - endeavoured to keep genuine issues of security and vulnerability apart from the legislation on privacy.

41. Specific problems arise concerning access to data through archives. Cost aspects, as well as the difficulty in having a simple way of acquiring programs is in this field another effective, yet unintentional obstacle to making older information all too accessible. Changes are expected to occur, though. It is hardly acceptable to have vast amounts of information which are stored on machine readable media, but which are not accessible for scientific research etc., because of lack of programs for data processing. This, together with the technological development and especially the work in progress on International Standards for Open System Interconnection (OSI), justifies the assumption that the difficulties which I have indicated will soon be overcome.

The Principle of Additional Safeguards for Special Categories of Data

(Convention 6)

42. As was mentioned earlier, this principle has not created any notable complications. Generally, the categories listed in the Convention have been surrounded by specific safeguards even before the adoption of data legislation. Certain problems have occurred though.

One phenomenon causing debate in Sweden is the use by some hospitals of computerised systems, accessible from a great number of terminals, for storage and processing of data on their patients. Since there might be difficulties in protecting these files from unauthorised access through these terminals, comparisons have been made to manual systems where the patients' records were kept in one place and were accessible only to a few of the hospital staff concerned.

./.

One related issue, embracing even more difficult problems, is the pursuit by regional hospital administrations of rationalisation and a better basis for their planning. This pursuit has resulted in demands for data bases holding personal data files common to several hospitals within the region. Thus, data from patients' records can be available also outside the clinic where the patients are being treated.

Both these phenomena to a high degree give cause to ask for efficient methods to prevent unauthorised access to sensitive information. Unfortunately one has reason to assume that development is lagging behind here.

The Principle of Data Security

(Convention 7; Guidelines 11)

43. The obligation to observe this principle is by far the one causing the greatest difficulties, on account of the technological development. One element of risk is that automatic data processing is performed on such a large scale that comparatively greater numbers of persons have access to vast amounts of information. Other risks are that data stored on machine readable media sometimes have to be transported between different computer installations, e.g. in a company and a bank.

The most striking feature, however, is the tendency towards decentralised systems. Difficulties from security points of view arise because of the accessibility to the data base by a large number of terminals and because of the fact that communication terminal-to-computer or computer-to-computer is in general being executed through tele-networks.

The risks arising from this situation not only include a threat to privacy. The possibilities for computer-related criminality and vulnerability issues in general also come into the picture here.

44. Over the years much effort has been made to improve security. Those engaged in this work have often testified that awareness and preparedness in this field are strikingly low.

In Sweden a special commission - the Vulnerability Commission - was assigned to investigate the issues. After its final report in 1979, this work has been continued by the Committee on Vulnerability. This committee has prepared inter alia a method for analysis of the vulnerability of computerised information systems. I will shortly return to this method (para. 58). A committee on vulnerability in Norway is expected to deliver its report during the first half of 1985.

45. Another way of improving security would be extended use of encoded information. So-called electronic seals have been developed. More stringent control measures of authorisation routines have been established. To some extent sensitive material is no longer transmitted through tele-communication networks; instead, information is sent via discettes and the like.

./.

The Principle of Openness and Individual Participation

(Convention 8; Guidelines 12 and 13)

46. The fundamental idea behind this principle is to ensure that a data subject (personne concernée) will be able to establish the existence of a personal data file and its controller, to obtain personal data relating to him and, as the case may be, to have them rectified or erased.

A basic feature of some domestic laws is the establishment of a special authority, issuing a licence to the controller of a specific data file to operate the file. Such an authority would simultaneously get a good general picture of those who are involved in data processing. By turning to this authority, the data subjects would easily come into contact with the controller.

The technological development has shown, however, that it is hardly feasible to maintain a system based on a general requirement for licensing. This would mean, in the long run, that practically every stage in the administration of private and public activities would have to be examined under the licensing procedure. Extended use of computers - especially for commercial applications - combined with the explosive increase in the number of small computers are the reasons why such a system cannot be retained.

47. Nor is it necessary, for the sake of data protection, to interfere in this way, directing private and public activities. Against such a system it could also be argued that the licensing agency would have exceptional powers. In order to carry out a meaningful licensing assignment, such an authority would also need staff. Another problem would be to arrange for adequate control of the observance of decisions on licences.

As we are about to see, it has become necessary, not only in Sweden, to abandon the idea of a general requirement for licences to operate data files.

If this requirement is removed, there is a risk, however, that the authority (the Data Inspection Board) will be deprived of its capacity to give support to data subjects wanting to use their right of access or wanting for other reasons to contact the controller of a file. This risk has been obviated by the requirement of a general licence (see para. 60 below).

48. Many experience difficulties when they want to have errors in automated data files rectified promptly. Especially within the area of public administration there still exists a tendency among various officials to blame errors on the computer and a lack of willingness to expedite such rectifications as are required by the principle. It seems also to be a fact that the objections made by the data subject are often not believed, which means that he has to spend a lot of effort on proving that he is right - not the computer.

This could of course be said to be an educational issue. The staff knows too little about EDP and the systems operated and may therefore have difficulties in handling objections correctly.

./.

49. As I have already stated, the technological development and the tendencies to collect data from external files will probably increase the risks of errors in the processing of personal data. The possibility for the individual to detect errors may simultaneously be diminishing; he is not aware of the existence of the file or he does not realise that a piece of information is incorrect, e.g. because of the complexity of the system of rules administered. This issue must be scrutinised with the utmost care in the future, in my opinion.

50. During the work within the Council of Europe and the OECD, the extent to which data subjects were to use their right of access was much debated. It was assumed that relatively few people would use the right to obtain data about themselves. This assumption may be said to have proved correct. But this is of minor importance. The fundamental idea is that the mere existence of this right has a preventive effect.

The Principle of Accountability

(Convention 10; Guidelines 14)

51. Regarding the application of this principle there is not yet much to observe - at least not with respect to the experiences in the Scandinavian countries. Generally, errors have been corrected in an informal way (i.a. through actions by the Data Inspection Authorities), obviating litigation over compensation for damages, etc.

In Sweden the Chancellor of Justice is assigned to supervise demands for compensation against the Government. Each year he deals with a few matters concerning liability for errors in personal data files. These matters generally concern errors in the car registration and drivers' licences files, and the compensation for damage is relatively moderate.

52. One area, within which the dangers are especially poignant, is the credit report business. As I have already mentioned, an error in a credit file may have devastating consequences for the individual concerned. The system applied in Sweden, however, ensures that a copy of the information is sent to the data subject simultaneously with the report to the requesting party. In Norway, corresponding rules apply when information is disseminated about someone who is not a businessman. In Denmark, as a main rule, the person being registered for the first time with a credit record institute, shall be notified about the registration.

If the data subject is informed about what data are being disseminated, he can have errors rectified before any notable harm has occurred. But it is of course obvious that there is always a risk of damage. Rules on compensation must be provided in such cases according to the Convention.

Transborder Data Flows

(Convention 12; Guidelines 15 - 18)

53. The background to the Convention and the Guidelines containing rules on transborder data flows is well-known. The reasons why domestic laws have

./.

got rules on licensing or other means to limit the right to transmit data abroad, as well as the issue of whether these rules are effective, have been debated intensively. I will not repeat the arguments voiced in this debate.

54. The experience gained by the application of the rules on export of data contained in the data laws of Denmark, Norway and Sweden is as follows.

In Denmark, one licence to process sensitive data abroad has been given.

In Norway, 30 - 50 reports a year are received regarding transmission of personal data abroad.

In Sweden, no exact figure exists on the number of licences. The probable figure is around 50 in all.

55. It may thus be concluded that the number of licences granted is very modest, compared to the extent of domestic data processing. In view of the extensive exchange of information occurring between multinational corporations in particular, the question whether the number of licences reflects reality is appropriate. My answer to this question is no.

It should be kept in mind, though, that personal data constitute a very limited part of the transborder data flow. In Sweden this volume is assessed at 2 to 4 per cent of the total transborder data flow. The volume that warrants licensing is thus not so large. But the question remains if there is any purpose at all in having rules which are not observed - probably because they cannot be supervised in an effective manner.

THE SCANDINAVIAN DEBATE

56. Data legislation was passed in 1973 in Sweden, in 1978 in Denmark and Norway, and in 1981 in Iceland. The principles of these laws are the same, even though there are a few important differences. All these laws contain rules on Data Inspection Boards. Finland is considering legislation with a view to a bill being presented to the Parliament in the autumn of 1984.

Since this subject has attracted intense public interest, the issue of protection of privacy has been discussed all through the 1970's. This debate is still under way.

57. In Denmark, the Ministry of Justice is at present preparing - in cooperation with the Data Inspection Board (Registertillsynet) a report to the Parliament on the experiences of the administration of the data legislation. The report, expected to be published by this autumn, will contain, inter alia, an analysis and an assessment of the technological development and further security measures, if any, which should be established to prevent information from being abused or passed on to unauthorised persons. Furthermore, the Danish Commission on the Penal Code (Straffelovrådet) is at present considering if there is a need for specific punitive rules against those who gain unauthorised access to data files.

58. In Norway, the data legislation has been revised in 1982. The proposal contains a review of the rapid technological development. At the same time it

./.

is noted that this development has entailed that parts of the data legislation are not adequately protecting the right to privacy. This development has also led to drastic increases in the tasks of the Data Inspection. The conclusion drawn in the report (within the given economic limits) is that protection of privacy is best preserved by adding to the data legislation more precise material rules, and that the Data Inspection is turned into an agency with the functions of an Ombudsman, who will have the power to take action, to demand information and to make controls. This agency would also have powers to prohibit activities and to issue terms for those wanting to continue a specific activity. No final decisions regarding this proposal have yet been taken. The administration of the Data Inspection and several other advisory bodies have expressed their wish to maintain the licensing system.

59. Of particular interest in this context is the analysis made by Ragnar Dag Blekeli and Knut Selmer (Data och Personvern, Universitetsforlaget 1977) which forms the basis for the approach in the review of the Norwegian Data Legislation (Complex 1/83, Universitetsforlaget 1983). In this analysis, the protection of privacy ("personvern") is described as a possible interest of individuals in having control over information pertaining to them. Only when the information is actually used, or expected to be used, will the communication of personal data have consequences for the individual. This interest is divided into the interests of

- discretion
- completeness
- being informed
- having a "friendly administration"
- avoiding exaggerated control.

A summary of the Norwegian proposal can be found in Legislation and Data Protection-Proceedings of the Rome Conference on Problems related to the Development and Application of Legislation on Data Protection (pp. 219-226).

60. In Sweden, already in 1976, a commission was assigned to review the Data Act. Based on proposals by this commission, consecutive amendments have been passed. The latest of importance became effective on 1 July 1982. The reform aimed at rationalisation of the Data Inspection's activities so as to ensure concentration of its resources on such personal data files as are particularly sensitive with regard to privacy.

This reform meant, inter alia, that the existing prerequisite of a licence to operate a personal data file was limited to files containing sensitive information on, for example, diseases, crimes, political opinions, religious beliefs, or data containing assessments of the data subjects. A licence is also required if no particular connection exists between the controller and the data subject (employer, customer, member, etc.) and if the file is to be established by data file matching.

Instead, a system was created, by which everybody who wants to operate personal data files (the controller) has to notify the Data Inspection Board which on the basis of this notification will issue a general licence. Those who want to operate files exclusively for private purposes do not need any licence or permission even though this would have been mandatory had the file been

./.

operated by a businessman or an authority. (It may be noted that licensing was discarded as being too cumbersome by the Norwegian revision). Furthermore, all controllers requiring a licence are obliged to keep a ledger of all their personal data files.

61. The Commission on Data Legislation continued working, its terms of reference being to deliberate whether a universal data act, including manual files as well, should be introduced. The Commission soon arrived at the conclusion that there were no grounds for such a proposal. One reason for this opinion is that data subjects within the public sector already have insight into the activities carried out by public authorities through the principle of open government. Another reason is that manual records almost never may be said to entail the same risks to privacy as automated files.

The Commission then continued to work with a view to bringing about further amendments to the existing legislation. First of all attempts were made to ease regulations in areas where experience had shown that the law was more stringent than needed, and to strengthen regulations where a need was found, for example, concerning data file matching and processing for control purposes. During this work differences of opinion emerged within the Commission. These differences were so strong that the Government dismissed the Commission in spring 1984 at its own request.

62. One issue causing a vivid debate in Norway and Sweden is the use of civil registration numbers. As I have pointed out earlier, these numbers allow for an efficient identification concept, simplifying to a great extent data file matching and processing of different files.

This issue was firstly deliberated by the Swedish Commission on Data Legislation. In 1978 the Commission concluded that there was no reason to prohibit or limit the use of civil registration numbers from privacy points of view. The want of such numbers would, according to the Commission, not create a guarantee against data file matchings as long as other means of identification remained, e.g. names and addresses. On the contrary, the Commission found that civil registration numbers contributed to the enhancement of privacy, by being a guarantee against errors and identity confusion. This conclusion was shared practically unanimously by a wide range of observers and by the then existing Parliament and Government.

In Norway, this issue has been deliberated by a Commission which presented its report in August 1983. The conclusions drawn by this Commission are largely identical to those put forth in 1978 in Sweden. It should be noted, however, that Norway only allows more limited use of civil registration numbers than Sweden.

In Sweden, the debate has risen again during the last months, which has caused the Government to appoint a new Commission to reconsider this issue.

63. It should in this context also be mentioned that the battle against economic criminality has come into focus to a high degree in Scandinavia, particularly in Sweden. In the autumn of 1982, the Swedish Government appointed a Commission whose terms of reference were to present proposals for combating this type of criminality. The Commission, which by now has presented its final

./.

report, has during a little more than a year presented some 30 different proposals for amendments to the Swedish legislation. These amendments entail in various ways increased control of the observance of rules and regulations in society. The ensuing debate over these proposals has been vivid, and final decisions have not yet been taken by the Government. This issue is, however, of importance with regard to data protection. Several of the proposals will entail increased control, should they be accepted by Parliament. This control is intended to be performed, inter alia, with the use of information from automated personal data files.

64. As I have already touched upon (para. 44), the issues on vulnerability have also attracted growing attention in Scandinavia.

In Norway, a commission was appointed in February 1983 to investigate the vulnerability of an EDP-dependent society.

In Sweden, the Committee on Vulnerability has prepared - in co-operation with the local communities and the industrial sector - a method of analysis of the vulnerability of EDP information systems. The idea is that this new method, "the SBA method", will enable an enterprise or an authority to analyse in a few hours time whether there are any risks of vulnerability in their EDP system. The scope of the present report unfortunately leaves no room for elaboration on this method.

In Finland, discussions have barely started yet. The Delegation for EDP-trade, answering to the Ministry of Finance, heads a few working parties appointed to investigate security matters, etc.

DATA PROTECTION FOR THE FUTURE

65. I have now arrived at the point where the rapporteur is supposed to present his pioneering thoughts and, with a few bold strokes, paint the picture of how data protection is best organised in the future. The reader will be all the more disappointed. I can bring no revolutionary proposals. But some ideas may contribute to the discussion.

66. As a point of departure for this discussion, I want to state two things firmly.

Firstly: Computers are now so widely dispersed - in various sizes and powers - that they are to be found everywhere in society. It will therefore become increasingly difficult to isolate the use of computers from other activities; this use will become an integrated part of activities in various areas.

Secondly: The development just described must necessarily be reflected in the legislation. It will certainly be impossible to encompass in one comprehensive legislation what may be described as the data legislation of one country (cf. para 5). But this must not prevent the principles, which form the foundation of the data laws (the concept taken in a limited sense), from being expressed universally throughout the legislation. The Convention and the Guidelines are very apt for serving as lodestars here.

./.

67. What then, are the conditions for the protection of privacy with regard to the technological development? My immediate answer is: One really cannot discuss data protection with regard to technological development alone. Several other aspects must be accounted for. As I observed initially, these other issues would generally fall within the scope of my co-rapporteurs' assignments. One problem which must not be overlooked in this context is, however, the attitude of the general public to personal data recording. The question is: Has this attitude changed in recent years?

68. As I have already stated (para. 9), all new technology has caused problems, and has even been met by doubts and scepticism, initially. This is the case also with computers. As the public becomes more familiar with computers - in their work, in their leisure time, as consumers, etc. - their knowledge about them and about their capabilities will also increase. Already now, it seems that people are no longer paying much attention to the fact that data about them are stored in computers with authorities, employers, trade unions, and the like. The data subjects themselves have often given their consent to the recording of this information, which in this context is considered quite harmless.

69. But problems arise as soon as there is talk of using this information as a basis for decisions bearing on or involving the individual or for random selections or compilations of various kinds.

Thus, it is not correct to claim that the general public is not nowadays concerned with the potential threat to privacy inherent in computers. The ever reiterated debate on various phenomena in the computerised society is a proof of this concern. In my opinion, a critical and alert approach is justified. It is important that we do not let our vigilance slacken.

70. At the same time, the subject is still hard to master. Today, as 10 years ago, the changing debate still concentrates almost solely on fears of what could happen and very little on what has in fact happened. General fears must be substantiated to such a degree that the legislator will be able to deal with them and really concentrate his efforts on important issues.

71. Experience shows that data legislation in some places has been structured in a way not quite in time with development. Some obvious inadequacies have of course been corrected. But the question remains whether these remedies will be enough in the long run. In other words: are we concentrating on the right issues today? The question has been put whether it is time to redefine the concept of protection of privacy (protection de la vie privée).

As I see it, there is not much sense in redefinitions of this concept. Our friend "The Elephant" enters the picture again. The meaning of the concept of protection of privacy varies from time to time. Compared to the situation of earlier periods, today's protection of privacy will surely stand out as a sheer luxury.

./.

72. It could be said that the concept of protection of privacy is the sum of the protections given by the judicial system to the individual, in competition with other, opposite interests. Analysing these conflicts of interests and taking a position on various practical problems, would probably be the most effective approach to the issues. The basis of the Norwegian investigation would be a good guide here.

73. Among the phenomena which I have regarded as important (paras. 11-23) for future data protection, there are a few which in my opinion play a particularly important part, namely:

- The increased use of terminals capable of communicating with one another, as with central data bases

- The tendencies towards information being collected through automatic processing of data already stored on machine readable media

- The possibility of using data on one file with a view to controlling data on a completely different file

- Systems based on two-way communication (electronic funds transfer systems, text communication, cable-TV, Tele-Data, remote maintenance)

- The dangers of unauthorised access to computer systems (crackers).

74. When comparing these observations with the interests listed in the Norwegian investigation one will find that they are more or less in complete conflict with one another. In what way can this be remedied?

In my opinion, the principles laid down in the Convention and the Guidelines still provide good guidance. The partition in the Convention of data quality (Art. 5) and data security (Art. 6) points to the two main areas where problems occur.

75. As far as data quality is concerned, the conclusion must be that the development towards an increased use of personal data from other automated files is difficult to prevent.The decision is of a political nature, and in the discussions it is always more difficult to attract an interest for the elusive concept of protection of privacy against the declarations by administrators and technicians that large gains in rationality will be made, if this method is used. This is especially true against the background of the increasing demands, politically, for economy and efficiency.

Undoubtedly, a considerable rationalisation may be achieved without endangering privacy. But errors do occur. One of the most important features of future data protection, then, must be the availability of rapid and safe routines for corrections, in order to avoid damage and unnecessary trouble for the individual.

76. The premises for monitoring data file matching and processing are markedly different, depending on whether a special licence is required for the matching or not. The safest method is of course a system of permission of some kind (by law, by an authority or by the data subjects themselves) to each and every matching procedure. Especially when the licensing is handled by an authority, a fruitful dialogue may take place between this authority and the controller. The

./.

outcome is often good, particularly when the controller's attention is drawn to issues that he might otherwise have overlooked. On the other hand, it must be kept in mind that this authority may be entrusted with issues of discretion that really should be solved politically.

77. Should data file matching be allowed without specific approval, other security measures must be taken. The fact that data subjects have the right to obtain information (Convention 8 b; Guidelines 13 a and b) is hardly sufficient here. Above all, in cases where the information is material to decisions pertaining to these data subjects, there must be a mandatory requirement that they be automatically granted the right to submit observations before any decision is taken. To some extent, regulations by which parties to administrative proceedings are granted access to material information should offer protection in this area.

78. But the issue demands attention not only when collecting data which is material to a decision directly affecting the individual. In Sweden, the Government recently rejected a proposal, that data for a census on citizens and housing be collected - not from the citizens themselves - but from various automated data files. One decisive reason was that data quality would be inadequate. It should be noted, that these data were to be used exclusively for statistical purposes in a non-identifable form, and not for any decisions concerning individuals.

In this context, I would also like to refer to the interesting judgment by the Federal Constitutional Court (Bundesverfassungsgericht) of the Federal Republic of Germany, on the 1983 Act on Census. The court found in its judgment of 15 December 1983 that this Act, which had been passed unanimously by the Bundestag, to a large extent violated the German Constitution (NJW 1984 pp. 398-405 and 419-428).

79. For the future, particular heed should also be given the development within the field of two-way communication between the data subject (whether directly or, for example, through his participation in an electronic funds transfer system) and the controller. There can be no doubt that such a system creates a potential danger that the controller will be able to get a very detailed picture of the private life of an individual (purchases, including kinds of goods, hotel and restaurant visits, and the like).

Along with the introduction of two-way cable-TV systems possibilities for storage of program choices will arise. This problem has attracted more attention in the United States and Canada than in Europe (cf. the Transnational Data Report, Vol VI No 8 p. 426 and the references made there). On the other hand, it may be said that the individual, at least so far, has a free choice to participate or not, and that therefore he is in a position to assess for himself the dangers to his privacy.

Information of the kind now being referred to is undoubtedly regulated by the Convention as well as the Guidelines, but since it has been left by both of them to the domestic legislator to solve the problems of satisfying their requirements, they cannot serve as exact guides. This issue calls, however, for further attention on the international level.

80. Passing on to <u>data security</u> one may state that this issue has not been sufficiently considered, at least not until recently. The difficulties are many. Contributing facts are, of course, the increased use of on-line systems and the

./.

potential danger of unauthorised access inherent in this increase, through legitimate terminals, as well as through the vast amount of terminals in general.

At this point, I believe it necessary to have a clearer picture of what the risks actually are. One may very well come to the conclusion that certain information, which is today found in machine readable form, should be completely excluded from automatic data processing.

The next step is to allow data storage and processing, while prohibiting on-line linkage outside an "inner shell" at the processing departement. Physical transportation of discs, tapes and other media may be another way of protection, if necessary precautions are taken against the risks of the transportation.

81. Also, I ask myself what possible means of unauthorised, or at least uncontrollable, access is created by remote maintenance. Doesn't this method mean that the controller would loss control over his file? Do possibilities exist which would enable the controller, through logging or similar measures which cannot be manipulated from outside, to find out afterwards exactly what the maintenance personnel has been doing? And when maintenance is carried out across the borders, is this method not in fact an opening to completely unlimited data export?

82. Several other issues of data security ought to have been brought to attention here, but they are of a more general nature and fall within the vulnerability issues. Therefore, I do not intend to enter upon these issues now.

83. When comparing the problems of data quality and data security, I have the impression that the efforts made have been concentrating on general measures regarding data quality. At the same time, security issues have not been considered to the extent needed. The reasons are partly the costs. If increased use of electronic fund transfer is being planned for the future, security demands will probably assert themselves more strongly. Hopefully, the demands urged in that area will also benefit others.

84. Thus, my suggestion, as far as security issues are concerned, is that they should be given closer attention generally. If security measures against unauthorised access, alteration or dissemination fail, the controller is not helped by the fact that he has put much effort into maintaining a high level of data quality. Regarding data quality, however, I believe that a wider differentiation of the ambitions could be attained. As I have shown earlier, there should be different ways of controlling the observance of rules. Such control could be adjusted according to who is the individual controller, what use the data will have, and what the possibilities are for the data subjects to exert control themselves.

85. One important issue is of course whether protection of privacy should be supervised by a specific authority. Neither the Convention, nor the Guidelines, take a stand on this question. Since conditions vary in different countries, there is no universal answer to this question. I can only remark that the rights, which the Convention and the Guidelines aim at protecting, are closely related to the guarantees laid down in the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the United Nations Convention regarding the same subject. These guarantees demand efficient supervision.

./.

86. Thus, the issues involved are important. The technological development must be followed closely. Its impacts on the individual must be carefully scrutinised, and if need arise, measures must be taken. A body with specific responsibility for these issues is of great value.

87. One phenomenon to be noted in this context is that the weighing of pros and cons often reveals political differences of opinion. In such cases, tensions may emerge between the Data Inspection Agency, on one hand, and other authorities - ultimately the Government - on the other. This is part of the system, though; the most important task for a Data Inspection Agency is the protection of privacy, whereas other authorities and the Government must take other factors into consideration as well.

This problem, which is of a constitutional nature, is to my mind quite bearable. This is so because I am of the opinion that the domestic data inspection authorities - provided that their tasks are executed properly - are playing an important part in the system of protective measures, constituting a balancing element in a debate which would otherwise perhaps deal too much with efficiency and rationality only.

88. Finally: as I see it, the greatest threat to privacy lies not in the technological development as such. We are in a position to decide for ourselves to what uses this technique should be put. The danger is rather that, in taking these decisions, we loose the general picture and get closer, step by step, to a "control society" of the kind symbolised by this year, "1984".

We must be on the alert. We do not want the "The Elephant" to suffer the same fate as the mammoth. Do we?

./.

APPENDIX I

TECHNOLOGICAL DEVELOPMENT AND ITS CONSEQUENCES FOR DATA PROTECTION

SUMMARY

After the introduction (paras. 1 and 2) a short background to the issues is given (paras. 3-9).

A review (paras. 10-23) then follows, covering the significant parts of the technological development. This review does not aim at describing techniques, but at those features of the techniques which are creating problems regarding data protection.

Next, the impact of the technological development on the possibility of observing the obligations expressed in the European Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, and the Guidelines on the same subject, adopted by the OECD, is analysed (paras. 24-55). The present debate in Scandinavia is then described (paras. 56-64).

The author next declares his views on data protection for the future (paras. 65-88). Among the elements important to the way in which this data protection should be organised, the following are mentioned:

- The increasing number of terminals, which are interactive with one another and with central data bases

- Tendencies towards information being collected through automatic processing of data already stored on machine readable media

- The possibility to use data for control purposes

- Systems for two-way communications

- The dangers of unauthorised access to computer systems.

Regarding data quality, the author stresses the importance of concentration on the following areas:

- Rapid and safe routines for correction of erroneous data

- Requirements for specific licences for data file matching, and - at least - a right for the data subject to see the information before its being used as a basis for any decision concerning him

- Closer attention to two-way communications systems to prevent mapping of the private lives of individuals.

Regarding data security, a closer attention is urged. The author points to the need to observe the following:

- It should be questioned whether certain kinds of data should at all be processed by computers

- A cautious approach to on-line systems is recommended, and when necessary on-line processing should be limited to an area inside an "inner shell" at the processing departement

./.

- On-line communication may have to be replaced by physical transportation of storage media

- Special precautions should be taken regarding remote maintenance.

Compared to what surely has hitherto been the case, a closer attention to security issues is recommended. Regarding data quality a wider differentiation of ambitions could be appropriate (depending on who is the controller, what use the data will serve and what possibilities data subjects have to exert control themselves).

Finally, the author expresses the opinion that it is of great value, if the supervision of data protection issues at the national level is carried out by an authority with specific responsibility for these issues.

./.

APPENDIX II

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

PREAMBLE

The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms ;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing ;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers ;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows :

CHAPTER I — GENERAL PROVISIONS

Article 1

Object and purpose

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Article 2

Definitions

For the purposes of this convention :

a. "personal data" means any information relating to an identified or identifiable individual ("data subject") ;

b. "automated data file" means any set of data undergoing automatic processing ;

c. "automatic processing" includes the following operations if carried out in whole or in part by automated means : storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination ;

d. "controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.

./.

Article 3

Scope

1. The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.

2. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe :

a. that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law ;

b. that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality ;

c. that it will also apply this convention to personal data files which are not processed automatically.

3. Any State which has extended the scope of this convention by any of the declarations provided for in sub-paragraph 2.*b* or *c* above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.

4. Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2.*a* above may not claim the application of this convention to such categories by a Party which has not excluded them.

5. Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraphs 2.*b* and *c* above may not claim the application of this convention on these points with respect to a Party which has made such extensions.

6. The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

CHAPTER II — BASIC PRINCIPLES FOR DATA PROTECTION

Article 4

Duties of the Parties

1. Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

2. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

./.

Article 5

Quality of data

Personal data undergoing automatic processing shall be :

a. obtained and processed fairly and lawfully ;

b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes ;

c. adequate, relevant and not excessive in relation to the purposes for which they are stored ;

d. accurate and, where necessary, kept up to date ;

e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6

Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7

Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Article 8

Additional safeguards for the data subject

Any person shall be enabled :

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file ;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form ;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention ;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs *b* and *c* of this article is not complied with.

Article 9

Exceptions and restrictions

1. No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

./.

2. Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of :

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences ;

b. protecting the data subject or the rights and freedoms of others.

3. Restrictions on the exercise of the rights specified in Article 8, paragraphs *b*, *c* and *d*, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10

Sanctions and remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

Article 11

Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this convention.

CHAPTER III — TRANSBORDER DATA FLOWS

Article 12

Transborder flows of personal data and domestic law

1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2 :

a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection ;

b. when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

(Articles 13 - 27 excluded here.)

./.

APPENDIX III

Annex to the Recommendation of the Council of 23rd September 1980

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:

   a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;

   b) "personal data" means any information relating to an identified or identifiable individual (data subject);

   c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

   a) the application, to different catagories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;

   b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or

   c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

   a) as few as possible, and

   b) made known to the public.

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

./.

PART TWO
BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identify and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

i) within a reasonable time;

ii) at a charge, if any, that is not excessive;

iii) in a reasonable manner; and

iv) in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs *(a)* and *(b)* is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE
BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR
NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

a) adopt appropriate domestic legislation;

b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;

c) provide for reasonable means for individuals to exercise their rights;

d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and

e) ensure that there is no unfair discrimination against data subjects.

./.

PART FIVE
INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:

i) information exchange related to these Guidelines, and

ii) mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

WORKERS' RIGHTS AND TECHNOLOGICAL CHANGES

by

Mrs M Georges

Chargée de mission
National Commission for Data Processing and Freedoms
(France)

Let me start by stressing the importance of the Council of Europe's decision to include among the themes for this colloquy the subject of workers' rights and technological changes, one which has so far rarely been examined in detail.

For one thing, the problems of individual rights and information technologies, whether in relation to data protection or audio-visual media, have seldom been studied in the context of business and industry. Much more attention has been paid to systems affecting consumers, users or citizens in their dealings with the various public authorities, rather than employees.

For another, the logic of social aspirations in industry has resulted in priority being given today to obtaining increased productivity through the adoption of new technologies and the monitoring of their effects on employment, pay, status or working conditions.

And yet current technological changes have very direct implications for every employee, affect their attitude to work, modify working relations and organisation, while necessitating the creative genius of extensive networks of producers to evolve them and operate them efficiently.

What new modes of production can be devised, and at what economic and social cost? What future is there for employment? These questions lie at the heart of the discussions being held inside industry, usually on a practical and experimental basis without reference to theoretical considerations.

The real question then, is how people use individual and collective rights to create a different working environment and conquer fresh areas of freedom by exploiting new technologies.

This question is all the more urgent as it refers to the use of technologies that are ambivalent from the point of view of rights and liberties: while information technologies may encourage the redeployment of economic activities, call in question Taylorist principles of work organisation and lead to greater knowledge, they also threaten to ensnare human values in an immutable system of rationalistic and economic constraints.

The list of data-processing techniques currently employed in industry and posing a potential threat to liberty is already very long: staff selection aids, recruitment on the basis of detailed questionnaires, monitoring of working hours and output, career management, assessment, disciplinary sanctions, training, medical tests, electronic delivery systems etc.

Since they concern personal data, these processes are amenable to the legislation on data protection (1). In France, many cases involving such data banks have been dealt with, after having been submitted to the National Commission for Data Processing and Freedoms (CNIL) (2).

Nevertheless, it is difficult to gauge the scope of these problems and all the practical implications from these sources alone and the case-law to which they have given rise. The positive law concerning "workers' rights and technological changes" is still meagre and an examination of these applications of the law leaves one feeling rather ill at ease.

This uneasiness derives first and foremost from the weak mobilisation on the part of the individuals and groups concerned. Whereas tens of thousands of processed data have been reported, only a tiny number of cases have given rise to claims, complaints or action by the workers affected. In addition, most cases of "data protection" rights are off-shoots of a wider conflict: blacklisting of trade union activists after a factory sit-in; criticism of a method of recording work rhythms as part of a time and motion study; critical report on electronic switching systems by trade union members employed by a major computer manufacturer etc.

Further, whereas the examples given may appear to be special cases, the feeling of uneasiness also derives from the fact that the supervisory bodies do not succeed in arousing interest or arriving at a consensus on a more general approach. In France, the CNIL endeavoured to approach these questions by using simplified standard procedures. But one trade union organisation, the "Confédération Générale du Travail" (CGT) insisted on taking a stand against the simplified standard relating to staff management, and succeeded moreover in having it rejected.

Indeed the whole matter leaves one with a sense of unease owing to the great, and perhaps growing, discrepancy between the interests of the "data protectors" and those of the labour organisations.

Rather than using this report to analyse the problem of "workers' rights and technological changes" based on a study of the case-law, therefore, I should like to turn to the root cause of our sense of dissatisfaction and ask three questions: Are the data-protection laws fundamentally inadequate for solving the problems of labour and industry? Is the very concept of rights pertinent in the industrial context, given the other issues raised by technology? How can progress be achieved in bringing together the world of technology and the world of labour?

---

(1) The French expression corresponding to the international term "data protection" is "informatique et libertés".

(2) CNIL: Commission Nationale de l'Informatique et des Libertés.

By defining my subject in these terms, I feel that I am contributing to the wider debate on the necessity of rethinking the concept of "data protection", while taking account of technological, economic, social, cultural and political developments.

DATA PROTECTION AND WORKERS' RIGHTS

If data protection seems difficult to reconcile with the behaviour of the various social agents in industry, this is essentially because of the assumptions underlying the approach.

In the early '70s, there was essentially a new awareness in political circles of the importance of technology, no longer merely at the industrial level (witness the previous discussions on national independence), but in terms of its applications. Thus, consideration was taken of the increased power conferred on those organisations possessing these new high-speed mass processing media in the form of computers, above all the State and the major multinational corporations.

Attention was not paid at this time to the changes inside organisations which permit and accompany the adoption of these techniques in working processes.

Reflection on data protection traditionally belongs to the history of human rights and civil liberties: data processing is used principally for managing citizens (by State administrative departments), or managing clients and users (by banks, insurance companies etc). Its subject matter which consists essentially of personal data and computerisation projects were regarded as confidential, or indeed secret.

In this context, discussions are centred on two major themes.

In view of the storage and supply potentialities of information techniques, it became urgent to protect individual privacy as an extension of the natural rights of individuals, hence consolidating the concept of private life gradually gaining ground in the catalogue of fundamental freedoms.

Certain national and international approaches have concentrated on this theme: the universality of information technology was reflected in the universality of human rights principles.

In certain countries, where memories of the ordeals suffered under Fascist rule were still fresh, public discussion also took account of the threat of totaliterianism. Prominence was given to the risk that the State might reduce the population to mere ciphers, programming all the decisions affecting them by interconnecting various data banks on the pretext of rationalisation and efficiency.

This led, for example, to discussions on the legitimacy of single identification numbers, the preparation of behavioural profiles or, again, the independent status of the data protection commissioners.

This approach, rooted in the tradition of human rights, has several implications regarding methods of grappling with the problems of business and industry:

- The individual firm does not appear to be a place especially prone to new problems of liberty, except that, as a legal entity, the undertaking itself might be threatened by the circulation of information concerning it but over which it had no control.

- The approach is essentially geared to safeguarding liberties. Since questions of principle relating to ethics are at stake, those controlling and operating the information system should be made fully aware of their responsibilities, and further developments should be systematically monitored by a supervisory body: this is essentially the task of members of data protection bodies. Although this protective, educational function, exercised from above, may foster awareness when applied to major State systems, it is inappropriate for the issues at stake in industry: here, it is not only necessary to protect threatened liberties, but to conquer new ones (not least by exploiting the potentially liberating aspects of the new technologies themselves, as illustrated in numerous industrial conflicts), as well as inspiring new creative ambitions, overcoming archaic organisational arrangements by stimulating perception, initiative and constructive criticism.

- The approach to data protection is concerned with individual liberties which transcend organisations and their operation. This approach is such as to make the various protagonists in industry realise that these technologies do affect individuals, but it may nevertheless fail to take account of how, through the use of these same technologies, new rules governing the life of the working community are fashioned and emerge through the interplay of the rights and freedoms engendered. In this respect, the new personal rights instituted by the data-protection laws (right of access, of rectification) only partially meet the problems raised.

- When reflecting on the subject of data protection, more stress is laid on the data-processing aspect than on rethinking the concepts of rights and freedoms. Whereas the protection of human rights has its history, its definitions and its legal machinery, computerisation on the other hand, understood as a potential means of violating these rights, has no place in law. This being so, a major effort has been made by lawyers to furnish the concepts and principles necessary to enable this new technique to be apprehended and made amenable to the law. For one thing, descriptive categories were devised such as: directly or indirectly personalised data, manual or automated data, data collection, transborder flows etc; principles were also worked out to which the technique could be subjected: liability of the computer operator, limitation on the collection and preservation of data, data quality (relevance, accuracy etc), conformity of processing with the specified purpose, the safeguarding of data etc.

With regard to the question of workers' rights, this approach nevertheless has several consequences:

- It restricts observation to the processing of personal data. But when one looks at what really happens in various industrial sectors, one realises that the computers whose use may create new constraints for workers owing to the exigencies of time or space are not primarily used to communicate personal data.

- It focuses attention on what happens inside the machine rather than on the way the latter fits into the working environment; yet one and the same technology may correspond to very different methods of work organisation with regard, for example, to individual worker autonomy. In this respect, technology and organisation form a whole for those affected, without their exact combination being absolutely predetermined.

- It perceives the technology only in terms of its "controller", ie the company management, whereas technological changes often affect whole sectors of economic activity and may induce new forms of dependence.

THE LOGIC OF SOCIAL HISTORY

The evolution of the concept of workers' rights in social history as a whole, is distinct from that of the concept of individual freedoms.

It is different in form and in content: rather than proclaiming the natural rights inherent in human personality, it is a case of combating the excesses of liberal individualism and the ravages of uncontrolled industrialisation by demanding the recognition of collective freedoms: freedom to organise and form associations and the right to strike.

It is also different in its pace of development: the history stretching from the recognition of freedom of association to the acceptance of trade union branches in firms is recent and its progression slow.

There is further difference in aims and means of action: rather than organising human rights to guarantee individual liberties, the aim is to conquer and defend social rights through freedom of association: social security, a guaranteed minimum wage, employment, health, training etc. These rights are seen as debts owed by society or the employer rather than freedoms.

The Marxist tradition illustrates the idea that altering the mode of production is the only way, in the long run, to confer any significance on the promotion of individual liberties, let alone the defence of common interests.

The radical nature of technological changes over the last 20 years has dealt a severe blow to this logic:

- The concern of the agents of social change had to be extended from the industrial sector to the tertiary sector, where trade unionism was less well established and the working population contained more women and young people.

- Certain conflicts revealed the ambivalence of technological progress and the multidimensional aspects of the employment problem (job insecurity, shift in qualifications, contradictory liberating effects, individualisation of tasks, increased monitoring etc).

All these many conflicting facts make comprehensive analyses difficult, especially as the economic crisis has brought greater fears of the negative effects of the current unsettling trends.

This situation has led trade union organisations to pay more attention to all demands and aspirations that do not emanate from the entire working class, a whole sector or even an entire firm. The new interest in workshop councils and independent production units, which began in Italy before making its appearance in France, seems to indicate the growing concern about all "local" issues and a desire to adapt to the technological changes which have split employment into smaller and smaller fractions, dissolving former communities and indeed encouraging the individualisation of work.

This general movement is composed of many strands, frequently connected with technology: working conditions, flexible working hours, personal working time, job mobility. The ultimate aim of the trade union movement in pursuing these various subjects is to try to adapt its language and structures to changing aspirations and outlooks. It endeavours to achieve this by more open discussion and greater democracy in industry. Hence the renewed interest now perceptible in France for experiments in participation and joint management as evolved in the German and Scandinavian social democracies.

French trade unionism today is considerably influenced by the advocates of self-management, which combines speculation about decentralising employees' activities and about their participation in managing their firm. This current bears witness to renewed interest in the problems of rights and freedoms. These are seen as having a twofold connection with the discussion on technologies. For one thing, technological progress was largely responsible for sparking off the preoccupation with the whole subject of freedom. In addition, it seems to offer some of the possible answers to the problem of injecting more democracy into industry. As a follow-up to the enquiries on the role of cybernetics, which were a feature of the re-emergence idea of self-management in the early '60s (cf Radovar Richta's work on "Civilisation at the crossroads"), the trade union movement now has to ask itself about the possible uses of information and communication techniques: audio-visual media, company networks, data banks and, imminently, expert systems.

A profound interest in questions of democracy, freedom, individual and collective creativeness is thus permeating the industrial world. This trend has been set in motion and brought to light by technological change and its effects in superseding the Taylorist model of manpower organisation.

Questions on "technologies and workers' rights" are thus beginning to surface. In legal terms, they have already given rise, however, to specific texts and concepts. In France these include: the "Auroux laws" on the right of expression, on the rights of employees and on the new role of representative bodies; or, again, the Act on the democratisation of the public sector.

We still seem to be a long way off from the themes of data-protection legislation. What means could be found to make progress in closing the gap?

THE NEED TO UNDERTAKE RESEARCH

In concluding this brief analysis, we feel that overcoming the difficulties surrounding the question of workers' rights and technological changes assumes that a serious effort be made to undertake research.

Such a choice represents something new in the field of data processing and rights and freedoms. Hitherto, it was thought sufficient to rely on the inherent dynamics of the new awareness and the persuasive effects that could be expected of the new ad hoc structures, providing checks and balances and an element of "moral conscience".

But to resolve the issues facing us today, recourse must be had to more extensive legal, technological and historical expertise.

It is no longer enough to address oneself to the problems of safeguarding privacy or the threat of totalitarianism alone; there are other, complex subjects, such as relations of authority or systems of interdependence within society that need to be investigated.

Where these are concerned, the ambivalent nature of technological changes cannot be ignored: whereas, for example, the individualisation of jobs that accompanies computerisation opens the door to closer monitoring, such individualisation may also be seen as a factor of progress.

There can be no one-dimensional approach to these questions; whether social or legal, numerous aspects must be compared and contrasted, all of which have their particular pace of development: working conditions, safety etc. For example, concern for the safety of isolated workers (lorry drivers, caretakers in hydro-electric plant, control room operators etc) calls for a system to monitor their movements from a distance, which in turn brings us back to questions of freedom.

To analyse technologies in terms of their "effects" gets us nowhere: by dissociating information technologies from their social impact, we overlook their potentialities for greater freedom: better knowledge, greater autonomy etc. Observing the evolution of technologies leads us to question their capacity to adapt to the cultural aspirations of society. It would be instructive to understand more clearly how workers' demands for self-management, the decentralisation of decision making, autonomy etc, are taken into account (disregarding the advertising slogans of the manufacturers) in the redesigning of information networks or personal computers.

Conceiving the relations between technology and society in terms of determinism no longer works. There is room for investigating new concepts such as, for example, the "flexibility" of organisations. To construct these, it is necessary to abandon for a time the sphere of ethics and the defence of acquired rights, in order to observe the

facts, more particularly as regards labour, in order to draw comparisons with other currents of thought, and benefit from the experience of other, more decompartmentalised experts such as biotechnologists, computer engineers, heads of quality circles, lawyers or individual workers themselves.

It is by dint of such efforts that we believe that we can actively contribute to giving some substance to the emergent notion of workers' rights.

We have endeavoured to do this in France by launching a research campaign on "technology and workers' rights". Forming part of the "mobilising" research programme on "Technology, Employment, Labour", in collaboration with the CNIL, this campaign currently focuses the efforts of six research teams.

The initial findings will be available by the end of this year. We hope to be able to compare them with similar projects conducted abroad.

It is therefore with an appeal for the use of the tool of organised research that we wish to conclude this preliminary consideration of workers' rights and freedoms. After stressing the need to rethink the issues involved and place them in a wider context, it offers a means of achieving joint progress.

DATA PROTECTION AND SOCIAL POLICY

by

Mr Jon BING
Norwegian Research Centre for Computers and Law,
University of Oslo (Norway)

1. Introduction

In the year of 1984 the dystopian novel of George Orwell has been some sort of leit-motif in reflections on the development of society. this novel is - among other things - a novel discussing the relationship between language and technology, a relationship interpreted by Orwell as power - power to create and control social change.

Those in power used paradoxical slogans to indoctrinate the population and induce a feeling of political paralysis:

WAR IS PEACE
FREEDOM IS SLAVERY
IGNORANCE IS STRENGTH

These are all slogans with associations. Orwell wrote his book in 1948 (which explains the title). He wrote a novel to make his own contemporary society aware of the coldness which followed in the wake of the Second World War and the prevailing presence of tyranny. And he used his paradoxical slogans deliberately to evoke echoes from the past. The slogan FREEDOM IS SLAVERY invokes a macabre echo - above the entrance to the Nazi concentration camps it was written: ARBEIT MACHT FREI. IGNORANCE IS STRENGTH invokes another echo. The maxim KNOWLEDGE IS POWER is attributed to the Franciscan brother Roger Bacon. In the 13th century he was a controversial philosopher, although the respect for his great knowledge had gained him the name "Doctor Mirabilis".

The maxim "Nam et ipsa scientia potestas est" may be found in his Meditationes sacrae. But it is told that he himself learned this truth by reading the lost book Secretum secretorum - The secret of the secrets - which was a letter written to Alexander the Great from his sage tutor, Aristotle.

KNOWLEDGE IS POWER is the rule on which the information society has been founded. The Orwellian travesty of this rule - IGNORANCE IS STRENGTH - is the rule which may corrupt the same society. Information technology is doing to knowledge what the steam engine did to horsepower. But this escalating power must be governed and used by political wisdom.

This is a task with a double edge. In part we have to avoid using the technology to create a regime of control and rigidity which we do not desire. In part, we have actively to seek to exploit the power offered by the new technology to disclose new possibilities for organising our societies.

This paper will mainly deal with some of the social issues of control which have been realised by the new technology. But it may initially be prudent to emphasise explicitly that to create a better society, we cannot restrict ourselves to defeating the threats - we also shall have to make the possibilities come true.

2. The protection of individuals and the protection of groups

2.1 The continuum of personal data

The data protection legislation is designed for the protection of "personal data". In the different national data protection acts, the basic idea of "personal data" seems to vary very little - being any data which may be assigned to an individual. One of the more explicit definitions is found in the US Privacy Act, section 3 (a), which qualifies as personal the data of a record which include the name of the individual or

> "... the identifying number, symbol or other identifying particular assigned to the individual, such as a finger or voice print or a photograph".

This demonstrates that data are qualified as personal when a link may be established between the data and the individual. This link has to be of a certain strength - indicated by the phrase "identifying particular" in the US Act. Some data elements act as unique identifiers - like PINs, finger-prints etc.

There are a number of cases which discuss whether the link between data and individuals is of a sufficient strength to qualify the data as "personal". One early and almost classical example is the Swedish Volvo case (decision of the Data Inspection of 11 August 1974) concerning the use of a telephone debiting register for distributing internally in the company the cost of telephoning. In this case, there were 1.7 employees to each telephone extension available. About 2,000 extensions went to individual offices, while the remaining 2,000 were each at the disposal of two or more employees. The majority of the Board of the Data Inspection found the data in this system to be qualified as personal, and refused Volvo a licence. The case was, however, appealed to the King in Council, who decided in favour of Volvo.

> A similar case has been decided in Norway in respect of a system proposed by Mobil Oil. The Norwegian Data Inspectorate also found this to be personal data within the meaning of the Act (decision 12/80).

A name is actually not a unique identifier, but in everyday contexts the ambiguity creates no real practical problems. Also for more administrative purposes a name is adequate when combined with some other element like, for instance, date of birth, address or job.

A Swedish study has analysed the use of three different sets of data to match two registers:

- surname, christian name and date of birth
- surname and christian name
- surname, christian name and street name

In all three examples, a correct match of 98% was achieved. Cfr SOU 1978:54 p.96.

The opposite of personal data is anonymised data. It should be realised that these are not two categories of data, but actually the two opposite ends of a continuum of the same data. Data are qualified as anonymous when data serving as identifying particulars have been removed, and the link between the data and the data subject sufficiently weakened. The moment when this has been achieved is, however, not a fact to be ascertained by any simple process. It is an assessment of when the individual is included in a group sufficiently large for the data subject to get lost in the crowd.

Numerous examples can be found which illustrate the problem of drawing the line between personal and non-personal data. Having at one's disposal aggregated data, one may try through correlation techniques to identify the individuals. Attempts at such "back-door identification techniques" have been carried out by the Swedish Bureau of Statistics for demonstrational purposes, and have been largely effective (cfr Olsson/Block 1976).

The test concerned the municipality Upplands Vaesby in the Stockholm area, 26,000 inhabitants or 11,300 households. Using only a rough domicile identification, year of birth and income in increments of 1,000 crowns for the adults of a household, 65% of the households were identified. Using some more variables, as many as 91% of the households were identified - the unidentified being juveniles without income. Cfr Olsson/Block 1976:1228.

This may serve as a reminder that all data associated with persons are potential personal data, and that the same considerations and concerns which have resulted in the data protection legislation are relevant, though to a lesser degree, in relation to this larger set of data.

In the continuum of individual to aggregated data, an intermediate stage is the data on groups of different types. These are aggregated data, but related to a rather small population - like the employees of a certain company, the people living in a certain street or belonging to a certain society. Often the traditional protection against defamation or slander is extended to such groups when it is sufficiently small to make slander of the group a problem of the individual member of the group.

This traditional protection will certainly vary from jurisdiction to jurisdiction. But a curious example may be mentioned from Norway.

The case concerned the National Insurance Institution, which processes data relevant to social benefits. A computer consultant had publicly maintained that the security of the computer system was insufficient, and also that on one occasion data on diagnoses had been sold by one employee to a pharmaceutical company which had an interest in these data for marketing purposes. As this implied a criminal breach of confidentiality, the National Insurance Institution required the consultant to reveal his source. The consultant did not comply, claiming the right as a journalist to protect his sources - a position he upheld even when the Supreme Court confirmed that the source should be revealed. The person alleged to have sold the data was not identified by the consultant - nevertheless the consultant was found guilty of slander as the group of employees was sufficiently restricted for the claim to be a burden on each individual employee. This illustrates the traditional extension of the protection of individuals to groups in Norwegian law, and its relevance to the area of data processing.

It may be worth noting that this case through newspaper reports found its way into US statistics on computer crime. As will have been evident from the discussion above, no evidence of a computer-related crime having taken place was ever presented, and the consultant was found guilty of slander. But the problem created for the data processing unit of the National Insurance Institution has not found its final solution through the Norwegian court decisions.

Taking this traditional aspect into account, it may be easier to understand and accept the position in some jurisdictions - among these Norway - in respect of legal persons. The data protection legislation is extended to offer some protection to legal persons. The Norwegian Government Bill justifies this extension by pointing out the difficulties in regard to data on companies. A system containing data only on incorporated companies would not contain personal data, but if one of the companies was a personal firm, it would be personal data. The reasoning is akin to the one sketched above - the distinction between data on persons and groups may be quite difficult to make. The claim that there is in principle a difference between data relating to physical and legal persons may be difficult to defend from this point of view.

This is also emphasised by Hogrebe (1981:41), pointing out that the extension to legal persons solves the problems in certain situations which:

> "... are typically characterised by the fact that data on small entities are affecting individual persons who in a specific capacity (eg as owners or partners of a business, members of an associations) are so closely related to the entity in question that virtually any information on the entity is, or contains, implicitly information on such individuals. Such data technically do not qualify as personal data because they are not directly information 'on the personal or material circumstances of an identified or identifiable physical person'." (The citation by Hogrebe is from the German Federal Data Protection Act sect 2 (1).)

The way in which legal persons is included in the relevant national Acts (Austria, Denmark, Luxembourg and Norway) varies, and the Norwegian solution may be criticised for technical reasons (cf Bing 1979:81-82).

There are a number of cases on record where individuals have reacted strongly to being identified with a group.

One of the more extreme examples relates to one of the cable television experiments in the United States, which released statistics showing that a large fraction of their subscribers tuned into the "blue" channel (where pornographic movies were shown) at least once a week. In this way the prevailing "public" morality was confronted with the private morality practice, demonstrating a discrepancy which was some sort of quantified hypocrisy. Quite understandably, individual subscribers reacted at being qualified as some "probable" viewer of the blue channel - though the statistics were anonymous, the membership of the group became a problem in itself.

Less drastic, but perhaps more practical, was a study made by social scientists of a suburban area of Oslo. The Stovner Report disclosed massive social problems, especially among the juveniles. The population of this area reacted quite strongly, feeling that they had been branded as individuals - being members of the group, their children became "probable" delinquents, "probable" social cases.

Based on such statistics, it is not justified, of course, to conclude from an individual's membership of a group that one individual has certain personal characteristics. It is an error of the level of aggregation which makes it scientifically unsound. One can, however, understand and respect the resentment of an individual to the publication of aggregated data in this manner.

The two examples cited illustrate the nuisance which may be caused by such a confusion of the level of aggregation. But more severe problems may be created. An example may be taken from the Norwegian public debate with respect to the practice of the immigration authorities. Organisations of immigrant workers have maintained that an unjustified discrimination is being exercised with respect to persons from certain Asian countries. They maintain that the authorities have observed a certain pattern in criminality with respect to for instance, drug traffic, and are using this generalised pattern to examine persons from these countries more closely than from other countries - for instance European or North American.

It should be emphasised that the organisations for immigrant workers strongly argue that the authorities interpret their data incorrectly, and that the general pattern does not actually exist. But in our context we will use this example to approach one of the most severe problems in respect of data on groups: by being a member of a group, the burden of proof is reversed. By being a citizen of a certain country, you are found suspect until proven otherwise.

This is cutting to the very roots of the society based on law. One of the basic principles is that an individual is innocent until proven guilty. This is most stronglyemphasised with respect to criminal law, but it is a general principle.

In many countries, however, there are no or few restrictions on the type of evidence that can be used. One possible piece of evidence relates to the individual's membership of a certain group - the subscribers to cable television, the inhabitants of a certain suburb or the citizens from a certain country. Certain properties of this group are known, and a member of the group is presumed to conform to these probable characteristics until proof of the opposite has been presented. Formally the burden of proof is as before, as the authorities may maintain that they are entitled to take into account the membership of a certain group as evidence - even when it may be demonstrated that the argument valid for the group is not scientifically valid for an individual member of the group.

The formal rule may be the same, but for the individual the rule has been reversed: the individual is no longer judged on the basis of personal characteristics, but on the basis of characteristics of a group to which - more or less by chance - the individual happens to belong.

There is obviously a theory for calculating the probability of an individual being a member of the "suspect population" actually being guilty. But the results of probability theory are not intuitively obvious. Legal procedure rarely takes this theory into account, but relies rather on a general assessment of a judge or another authorised person. (For a critical discussion of circumstantial evidence and probability theory, see Stripinis 1983.)

This is actually one of the more severe problems of personal data processing. Computerised systems are extremely efficient for doing the type of classification and correlation necessary for specifying the characteristics of any set of persons. The criteria may be selected to find probable tax evaders, probable terrorists or probable traffic victims. This possibility should, however, not be allowed to defeat the basic ideals of our society - to confuse the individual with the group to which the individual belongs. The slogans of the French Revolution should be remembered - at that time "equality" was directed towards the privileges of the ruling class; today it may be directed towards being treated as part of a computer specified class rather than as a unique and equal member of society.

3. Police, surveillance and social control

Within many jurisdictions where a data protection authority has been established, conflicts with the police have resulted.

This should by itself not come as a surprise to anybody. The police is an authority charged with the task of controlling the population in several ways. The very nature of the task of the police implies that it is a massive user of personal data. For its investigations, data have to be collected - from many sources and on many individuals. Obviously the data subjects will not only be criminals, but innocent bystanders whose circumstances more or less incidentally have related to a crime or an issue under investigation.

The data protection authorities have been launched into a society where the police authorities have a certain position - certain routines and established activities. One presumes that the police authorities are loyal with respect to the legislation governing their investigations. But even with this presumption, a conflict of interest with the data protection authorities seems inevitable. This is simply because the two types of authorities pursue different goals.

The data protection authority is concerned with personal data, and is inclined to restrict its recording and use. The police authority has an interest in accessing as much as possible of the data existing in a society, and for its own purposes stores and correlates personal data. This necessarily implies the use of data on innocent data subjects. Roughly one may say that the data protection authority would like to restrict the use of data to reduce the nuisance for as many innocent bystanders as possible, while the police would like to store as much data as possible in order to increase the identification of criminals.

Also the data protection authorities are concerned with those persons lacking the resources to defend their own interests - typically persons subject to social aid or police investigations. And the data protection interests are most pronounced where the use of data may imply decisions of a negative effect on the individual. Obviously both these characteristics are true for the persons whose data may be found in the police files - and naturally the data protection authorities regard such files with special attention.

The conflict which follows should be interpreted as a result of both authorities pursuing their rational goals. The conflict cannot be resolved unless one moves one step up in the hierarchy of goals set for a democratic society, and realises that the overriding goal is a balancing of power. The data protection agency is to "guard the guardians" - and the conflicts resulting from their criticism and comments are healthy signs of the society trying to adjust its goal structure in the perspective of information technology. Such an adjustment cannot take place unless the conflicting views are presented in a way which allows political assessment and resolution.

This is not said in order to minimise the conflicts which one may observe in several jurisdictions, including the Norwegian. It is said in order to emphasise that data protection authorities were introduced for a reason - and that this reason necessarily implies a re-examination of the policies of personal data processing. The police, being a heavy user of such data, must necessarily be a major subject for such a process. And in this perspective, the conflicts become less of a struggle between authorities and more of a normal, political process.

One of the examples of intensive use of personal data by the police, is the German example of "Rasterfahndung"- parallels of which certainly may be found in other jurisdictions.

An example may illustrate the method. In order to locate a known terrorist, Rudolf Clemens Wagner, the Hamburg police - in co-operation with the federal police - approached the Hamburg Electricity Board. Using data on electricity consumption, the purpose was to locate an

apartment with a certain pattern to its consumption, including breaks in certain periods. Authorised by a court decision, the police obtained tapes from the Electricity Board. The datawere processed and correlated in Wiesbaden until only a small set of subscribers was left.

The example is cited in the report of the Federal Data Protection Commissioner (1981:50, cfr Frøystad 1984 sect 2.6.1.4). Based on the action taken both by the Federal Commissioner and the Commissioners from States, rules for "Rasterfahndung" were developed, including restrictions on access to social security and medical data.

The example demonstrates how the police is able to use a powerful new technology in fighting a problem which the German society had identified as serious and destructive. The example demonstrates also, however, how the police by pursuing this objective actually combed through the city of Hamburg trying to find the terrorist suspected of hiding in the myriad of apartments and flats. This process obviously also implied the examination of data on numerous innocent persons. And a "match" in respect of the defined criteria would make this innocent person suddenly become subject to the suspicion of being a terrorist.

This is once more an example of the reversion of the burden of proof. But there are also different aspects to the example. For instance, this method requires that the data have sufficient quality; the data havenot been collected with respect to their use in a criminal investigation - the verification procedures and other associated procedures are not designed to secure a quality standard which such use requires. Research initiated by the United States Congress has revealed large fractions of the data collected in criminal history records to be inaccurate (though our source does not discuss the criteria for this assessment).

> The Congress' Office of Technology Assessment arranged for a researcher, Dr. Kenneth C Laudon, to check samples of criminal history records. In North Carolina, only 12.2% of the summaries were found to be complete, accurate and unambiguous. In California, 18.9% were complete, accurate and unambiguous. In Minnesota 49.5% met the same standards. A sample of arrest warrants from the 127,000 contained in the FBI hot file was checked for a single day in August 1979. Of these, 10.9% had been cleared or vacated, 4.1% showed no record of the warrant at the local agency and a small additional number of warrants had other problems. Assuming the validity of the sample, 17,340 Americans were incorrectly shown to be subject for arrest that single day. (Cf Burnham 1983:74.)

Data collected for routine purposes cannot be expected to have a high quality - and this implies that proper care should be taken to interpret such data when used for other purposes. One might actually suggest that at the moment research into the data quality of a modern society is required in order to assess the risk related to use, re-use and misuse of the numerous files and administrative systems.

There is also a slippery slope from criminal investigation to general surveillance. The Hessian Data Protection Authority has pointed to the problem of preventive criminal justice. This requires the police to keep track of a large number of persons who are not under suspicion of any crime, but for whom circumstances are making them prone to becoming involved in criminal action.

It is pointed out that to be subject to police observation ("polizeiliche Beobachtung"), the subject must be qualified in a certain way as a crime risk. But during the period of observation, which may be as long as months or even years, data are collected on the person's acquaintances, persons who themselves are not under suspicion. As the Data Commissioner remarks (Simitis 1985:60):

> "So koennen z.B. in die Datei (Personen, Institutionen, Objekte und Sachen)-Terrorismus die Daten von Buergern aufgenommen werden, die einen zufaelligen, ihnen moeglicherweise gar nicht bewussten Kontakt mit Angehoerigen des sog. 'terroristichen Umfelds' hatten ... Der Kreis der gespecherten Personen ist kaum abzugrenzen."

Obviously this is a new situation. When crossing a border or having a driving licence examined in a routine traffic control, the possibility will be created for a person to be identified as one of the persons on record in the surveillance system - and though not under suspicion for any concrete crime, the police officer in question certainly will take a special interest in this person. Again the burden of proof is reversed - belonging to the set of people related to those under observation and will possibly determine actions taken with respect to this individual.

Though the example is German, similar dilemmas exist within other jurisdictions. In Norway, one case relates to prostitutes. Being a prostitute is not illegal under Norwegian law, but living off the income from such traffic is criminal. It is, however, difficult to identify the pimps. As a strategy towards this objective, the police has a register of the girls. In this case, these girls have not violated any law - but as the register is part of the police systems for criminal investigations, they are not given access to their own records. And the police actually draws on these data with respect to certain cases, especially on the question of children's welfare where they are by law required to reveal any information relevant to the issue.

This is also a question of police observation, but the case emphasises another aspect. In these cases, the persons themselves are lawabiding - though perhaps not model citizens. Generally they should be given access to data relating to themselves, especially as this data may be decisive in certain situations. But this would defeat the objective of the police investigation, which in this case has been given priority.

As the latter case relates to prostitutes, the question of principle may perhaps not be appreciated. But the inclusion in police files for some legitimate relations to suspected criminals or for legal activity related to criminal activities are both examples of surveillance which bring individuals into an area of doubt. Without this individual being under suspicion of anything illegal, there are records which the individual cannot access or challenge, but the content of which can be used to make decisions of immediate effect on that individual.

It is obviously an important question of social policy whether to accept this kind of surveillance. This is not mainly a question of individual data protection, but more generally a question of what level of control is acceptable in a society and what degree of openness should be exercised in respect of criminal investigations. One should be careful not to take single cases as examples. There is no doubt that surveillance in isolated cases may be perfectly justified. But the information technology permits an explosive increase in such surveillance. Actually large fractions of the whole population may be recorded in such surveillance systems.

> A powerful tool for such surveillance will be the systems for optical coding of fingerprints, which would make it a matter of routine to match fingerprints lifted from the scene of the crime to all recorded fingerprints - both those from identified criminals and those unidentified prints recorded at some other scenes. The possibilities of tracing individuals and correlating identified fingerprints with those found at different places, will create a powerful technique for indirect surveillance.

Again it should be emphasised that this surveillance may focus on persons under suspicion for actual criminal acts, but does in fact include persons under no such suspicion. This is not something which only concerns the persons living in the shade of the underworld, but which concerns all members of a society - it is the general level of control in society which is the issue, not just the control of criminal elements.

This perhaps becomes more evident when taking the example into the area of preventive social medicine. One of the cases of the Norwegian Data Inspectorate (case 82/777-1) concerned a research project associated with the Health Council of Oslo, with the objective of relating certain behaviour patterns in small children with later anti-social behaviour or psychological problems. The method to be used was a match of police, school and health records. Using the police records, children with criminal behaviour were to be identified. The school and health records for these were to be analysed in order to isolate "danger signals". Then the school and health records for the whole population of children were to be searched to identify children showing "danger signals", but who were not part of the police records. A programme of social assistance by health services was to be developed for this risk group.

A licence was actually granted by the Data Inspectorate (1 February 1984), but with strong restrictions on using identifying elements in the records. No action on the individual level was foreseen, and the data were anonymised in order to reduce the risk of such action.

The objective of this project is obviously commendable, but the ethical objections are strong. The argument is again the same: an individual should be treated for what he has proven himself to be, not for what he possibly may become. We see the tendency towards a sort of benevolent tyranny where early warning systems for undesirable behaviour trigger correction mechanisms of therapy treatment. It is, of course, unfair to read such perspectives into the small and unpretentious project subject to a decision by the Norwegian Data Inspectorate. But such perspectives are nevertheless present and one should - especially in the year of 1984 - be permitted to emphasise this problem. Information technology is potentially a powerful technology for social control.

Brief mention may be made of a different perspective, that of the relation between employer and employee.

Personnel administrative systems are generally in use, and do create their own problems. In this paper, these systems will not be discussed in general. It will be assumed that such systems include a salary sub-system, data from check-in controls, data from telephone debit systems etc. But pursuing the arguments made above, one point will be made in respect of such systems - the argument related to the reversal of the burden of proof.

Employees usually have protection against unjustified dismissal. Under Norwegian law the employer has to show good reasons, and similar provisions exist in other jurisdictions.

The relationship between employer and employee is complex, and a detailed personnel administrative system would reflect this. Obviously the system would also reflect data unfavourable to the employee. Within the scope of the system, such data would be recorded as a matter of course and would be available for later examination.

Taking the hypothetical situation in which the employer for some unjustified reason wants to dismiss an employee, the system would be available. In the richness of recorded data, the probability might be quite high for finding some unfavourable item which may serve as the reason for dismissal, and which may be acceptable according to the statutory requirements. This is a possibility which has been discussed in the Federal Republic of Germany, though no concrete example of such misuse has been identified. (Cfr Borchgrevink 1984 3.1.1.)

In this situation, the employee may find the traditional protection of limited value. The data referred to by the employer are correct. The employee may maintain that his or her record is no less favourable than the average record for employees in the company. But this line of defence will probably be less than successful - the law does not require that the employer shall have <u>better</u> reason to dismiss others, only that the employer has <u>sufficient</u> reason to dismiss the employee in question.

Again it is indicated how a general system of surveillance turns the traditional burden of proof and makes it necessary to discuss the adequacy of the established legal rules.

5. The vulnerability aspect

One of the relations between social policy and data protection is the problem of vulnerability. This is itself a complex issue which will not be explored in detail. But the vulnerability issue did in one sense grow out of the data protection issue, as demonstrated by two Swedish cases from 1974.

The Swedish data protection legislation (sect 11) gave the Data Inspection authority to licence certain cases of international data flows. In 1974 a licence was denied in two important cases, which have played a certain role in the subsequent international debate.

The first case (decision of 12 August 1974, Dnr 485-74) concerned a Swedish local authority, Joenkjoeping laens landsting (corresponding to a county or a district authority). In July 1974, this authority had introduced a register of patients. The authority required an amendment and extension to this register in order to emboss plastic patient cards. The Data Inspection did not have any comments in respect of the planned amendment of the register.

In respect of the embossment of cards, the Data Inspection did, however, point out that the embossment required a special licence. The decision of the Data Inspection Board in question related to the export of the register. The export would include 80,000 persons in the southern part of the county. The embossment would include the following data elements:

- PIN
- county, municipality, community
- name
- address

No company in Sweden was at that time able to emboss plastic cards, though this would become possible during the autumn of 1974. The county authority pointed out that a new hospital would be ready in August 1974, and that the use of patients' cards was co-ordinated with this new hospital. A delay until the cards could be produced in Sweden, or manually embossed, would be inconvenient.

The United Kingdom bureau in question (Rapid Data, Havant) and their Swedish representative (AB Carl Lamm) had emphasised their awareness of the importance of the security of the data for unauthorised access or use, and Rapid Data had specified their security measures.

The Data Inspection Board based its decision on three points.

Firstly, the Data Inspection Board stated that in this case it was a question of mass data, and that the assessment of data protection must take this into consideration. This was the first decision on mass export of personal data, and the Data Inspection Board was conscious of the importance of the decision as a precedent.

Secondly, the Data Inspection Board pointed out the risk associated with establishing total registers of the Swedish population through co-operation among several foreign bureaux having had mass data exported to them:

> "Through a co-operation among different foreign service bureaux, which in an authorised or unauthorised way have had access to data on Swedish citizens from registers, such population registers may over time become broader and deeper".

The Data Inspection Board pointed out that Swedish authorities did not have jurisdiction over such foreign registers, and that control by foreign authorities "at this time" could not be counted on. Security measures could not compensate for this lack of control - though the Data Inspection Board took care to emphasise that it did not imply that the measures in this case were inadequate.

Thirdly, the Data Inspection Board took note of the "unrest" in respect of population registers of which data subjects had little knowledge in respect of their objectives and use, an unrest which was even more pronounced in regard to such registers established abroad. Reduction of causes of public unrest was seen as part of data protection, and this was related to the lack of control pointed out in its second point.

On this reasoning, a licence was refused. Two of the board members expressed a dissenting view, pointing out that the data were not sensitive, and that arguments concerning costs should be given higher priority. The Data Inspectorate stressed the "national security" issue, as this was a case of mass export. In assessing the decision, it should also be considered that at this relatively early stage a restrictive policy might have less precedential effect than a permissive policy.

The second major case followed a few weeks later, on 27 August 1974 (Dnr 476-74). The applicant, Bonniers Foeretagsinformation AB, was affiliated to a major Swedish publishing house. This company co-operated in producing a catalogue named Swedish Tax Calendar (Sveriges Taxeringskalender). This catalogue would include all physical and legal persons with an income exceeding 60,000 SEK, estimated at approximately 200,000 entries. The data was furnished by county authorities on magnetic tapes.

In order to understand the decision, one should make perfectly clear that the publication of income is by itself not a violation of privacy. This information is made public by statute, and there is a tradition for some publications to communicate this information. The catalogue in question was the annual volume of a catalogue published for a number of previous years (the case does not go into details on this point, as this was not disputed).

The data to be included were:

- code for county and municipality
- PIN
- name
- address
- taxable State income
- taxable municipal income
- debited capital tax

The data was edited in order to relate husband and wife, and in order to make an alphabetical list of municipalities and counties. Capital was calculated according to statutory rules, and this processing took place in Sweden.

A contract was entered into with a British firm, Comtech, for photo composition of the data. This was in accordance with how this was carried out on earlier occasions. A computer expert from the graphic data processing company affiliated to the publisher (Bonniers Grafiska Informationsbehandling AB) brought a magnetic tape to Comtech, where the photo composition took place. The expert then brought the tape and the photocomposed films back to Sweden, where the actual printing took place.

Also in this case, no Swedish company could meet the requirements of speedy printing. Bonniers offered to have the processing placed under surveillance by their representative at Comtech.

The Data Inspection Board decided in accordance with the decision in the embossing case, using identical phrases. One of the members of the Board expressed a dissenting opinion. He pointed out that the risk of unauthorised use should be related to motivation of possible foreign organisations. The resulting publication could be purchased across the counter in any bookstore, and it would therefore be improbable that a foreign organisation would take the trouble to make unauthorised penetration.

It would therefore be arguable that this decision stretches the objectives of national data protection legislation further than the former decision. Their order is, however, hardly an accident. Given the precedential value of the former decision (which in Scandinavian law is quite strongly based on the principle of equality within public administration), the second decision is quite understandable. But it is nevertheless a development in a restrictive direction.

These are two examples of decisions concerning foreign service bureaux. The cases are, however, abnormal in one very important aspect - they are both examples of mass export of data - data on 80,000 subjects in one case and, in the other case, approximately 200,000 subjects. The national security aspect was important in both decisions. And in decisions on wholly national registers, the Data Inspection Board did show the same restrictive attitude towards registers of large fractions of the population.

A negative decision in regard to Reader's Digest (a register for direct mail within Sweden, processed also in Sweden) was appealed to the Cabinet, and there overruled. After a change of government, however, the Data Protection Act was amended to take special account of just these type of registers. Today the Data Inspection Board has a specific authority in respect of this type of register - an authority which may be seen to exceed that of data protection in a narrow sense.

Therefore these two cases cannot be adequately assessed within the context of data protection or transborder data flows. They herald the priority given in Sweden to the vulnerability issue, which is the context of the national security interest. As is well known, the Swedish reports on the vulnerability of the computerised society have given rise to further and more general work in Sweden, and the Data Inspection Board as well as representatives of the Data Inspection have been heavily involved in this work.

Vulnerability is obviously related both to data protection and transborder data flows as well as protective trade measures - but, equally obvious, there is a more general political issue. It would therefore be quite misconceived to see in these two early decisions the current state of affairs in respect of export of data to foreign computer bureaux - and after the statutory amendment, one may also maintain that the legal context has been changed in a relevant way.

Independent of these two Swedish cases - which have been discussed in some detail - one may see the reasoning behind a sort of data protection on a national rather than on an individual level. A nation also has some interests akin to the interests basic to data protection - and the Swedish reluctance to disseminate data on large fractions of the population may be compared to the interest in confidentiality on the individual level.

Such comparisons are rather facile, and should not be considered as more than a metaphor. But permitting the metaphor, one may actually find one more parallel in some of the views voiced by third world countries.

Information on countries are not only to be found within their territories, but also in other countries. This information varies from general social, historical and commercial information to intelligence reports.

A special category of information may be that learned through Earth resource satellites, which will include information on the outlook with respect to crops of different kinds, droughts and blights, growth rates of forests and breeding of cattle in addition to information indicating mineral deposits or similar natural resources. This is information of interest to the country in the territory of which a crop may be ripening or a bauxit field may be located. But it is not available as a matter of course - the information is primarily available in that country which has launched the satellite.

It is understandable that a nation may want to have available the information relevant to its own territory. We will not pursue this example further than noting this interest, and point out that this may be seen as a parallel to the "access to one's own file" - the principle of openness which is basic to the data protection of individuals.

And with these rather vague indications we may leave the discussion of the international aspects, having perhaps underpinned a hypothesis that in developing a "new informatic world order" we may see data protection policies being taken one step further - from the area of individual protection to the areas of social and national policies.

6. Conclusions

The issues discussed in this paper are heterogenous, and it may be precarious to offer a conclusion.

Introducing the problem, it was stated that the distinction between personal and non-personal data really was a continuum rather than a binary sort. And this continuum may also be seen with respect to the policy issues involved. The most evident issues are related to the protection of the individual - the traditional "privacy" aspects. But as soon as the data protection policy debate was started, it could not be contained within the constraints of this individual perspective. The relation between the individual and groups became an issue. The control and surveillance techniques and regimes of the society as a whole are at stake. The data protection authorities have to define the limits to their authority - and by doing this, they also qualify issues of social policy for general debate.

It is therefore a continuum from individual privacy through data protection to social and national policies. It is no surprise that the information society will have a political discussion on which objectives information should serve. But all the issues have not yet been formulated, the policy is in the making - and this paper has only pointed to a few of the issues which seem to emerge, and which will imprint our future political debate.

Acknowledgement

The research basic to this paper (which has been contracted by the Council of Europe) has been sponsored by the Stiftung Volkswagenwerk.

Bibliography

Bing, Jon (1979) 'Personal Data System' - A Comparative Perspective on a Basic Concept in Privacy Legislation"; in Bing/Selmer 1980:72-91.

Bing, Jon/Selmer, Knut S (1980) A Decade of Computers and Law; Norwegian University Press, Oslo.

Borchgrevink, Mette (1984) Arbeidmiljø og databehandling: arbeidsrettslige aspekter, Norwegian Research Centre for Computers and Law (ms).

Burnham, David (1983) The Rise of the Computer State; Weidenfeld and Nicolson, London.

Frøystad, Dag (1984) "Inclusion of personal identification numbers (PIN) and other matching elements"; part of the study Data Protection in Practice, Norwegian Research Centre for Computers and Law (ms).

Hogrebe, M E (1981) "Legal Persons in European Data Protection Legislation: Past Experiences, Present Trends and Future Issues"; DSTI/ICCP/81.25, OECD, Paris.

Olsson, Lars/Block, Hans (1976) "Bakvaegsidentifiering av personuppgifter"; Nordata 76, Helsinki 1976: 1225-1236.

Simitis, Spiros (1983) Zwoelfter Taetigkeitsbericht des Hessischen Datenschutzbeauftragten, Wiesbaden.

SOU 1978: 54 Personregister-Datorer-Integritet; Stockholm.

Stripinis, Daniel (1983) Probability Theory and Circumstantial Evidence; Complex 8/83, Norwegian University Press.

THE NATURE OF THE NEW TECHNOLOGIES: THEIR EFFECTS ON OUR CIVILISATION, THE ROLE OF THE LAW

by

Mr M CAPURSO
Cassation Judge (Italy)

The subject of my speech is too broad to be fully dealt with in an oral communication, however detailed. All human activities are affected by the new information technologies, and the technologies themselves constitute an almost unlimited area of research, offering prospects of countless uses and aims.

I must therefore confine myself to discussing my subject in general terms. However, I shall analyse certain arguments on account of their special significance.

The emergence of the new information technologies has been described as a revolution comparable to the invention of printing, the telephone and photography as well as the steam engine and electricity. These comparisons are valid in so far as such inventions were powerful factors for progress. But they are also limited for, although it must be acknowledged that printing fostered written language and that the cinema and television gave prominence to images, it is undeniable that the new technologies are capable of combining all these techniques and improving them both qualitatively and quantitatively.

Informatics and telematics (which marries informatics with telecommunications) enable vast quantities of information to circulate in writing, speech or images in a highly precise and infallible manner. If we consider what speaking, writing and seeing have always meant for civilisation, we are bound to recognise the fundamental value of information in our lives. Apart from the technological aspect, moreover, information conditions man even biologically, for our cells live on information circulating in the microcosm. Clearly, therefore, information is the essential element, indeed the basis, of our lives. Consequently, the development of any human ability to obtain, select and process information has a profound effect on civilisation by enabling people to live better thanks to a relevant and comprehensive knowledge of things. As man extended his knowledge of the world, indeed of all that exists, he learnt to control it. This indisputable fact provides the foundation for a theory that any power in the future will no longer be based on the possession of territories, means of production or economic interests but rather on the control of information.

This theory is recalled in the science fiction novel "1984" by the Englishman Orwell. On a more strictly scientific level, however, it is due to the investigations and discoveries of an American of German descent, Wiener, and his disciple, Shannon, who have been called the fathers of modern cybernetics. The very nature of the new information technologies provides the real dimension of the phenomenon which these technologies constitute.

The French Academy defines data processing as "the science of the rational processing of information". According to another definition, computer science is an electronic methodology which uses figures. These definitions serve to supplement each other, one by emphasising the logical process, the other by indicating the electronic vehicle of the methodology. Both, however, make it clear that the methodology is one that is reminiscent of the functions of the brain, indeed of the essence of thinking. Any research in the field of computer science opens up unlimited scope for progress.

As we know, large quantities of information have been assembled down the ages, and it can easily be seen that, for reasons of time and space, it is almost impossible to assimilate all the information at our disposal. Consequently, we would need an almost unlimited time-span and a brain with enormous capacities, which probably does not exist, in order to acquire and process such information. But we also know that the new technologies enable us to do this, as years of study can be reduced to hours or even minutes. Although difficult to believe, this is a fact. While recalling the ancient philosophers who complained that life was too short to enable them to learn much, we can be sure that in the near future the time available for learning will be lengthened thanks to the new technologies. Of course, these technologies will not do away with time or give us eternal life; but they will enable us to increase our life-span as far as knowledge is concerned. The same applies to the other dimension of human life, namely space. Telematics will enable us to reduce space to virtually nothing by providing us with the means of consulting libraries or (through tele-conferences) of meeting other people without even leaving our offices.

Undeniably, therefore, all this will have a marked effect on society, which is wholly concerned by the new technologies. We are all clearly conscious of being confronted with a full-scale revolution that will completely change our civilisation and culture. The facts of the matter have in recent years been examined by specialists in a wide variety of fields - economists, jurists, administrators, doctors, sociologists and even artists.

The Club of Rome, in Italy, recently received two reports. The first was "Microelectronics and Society - For Better and For Worse" by G Friederichs and A Schaff; the second was "Information Technology and Civilisation" by H Hinose and J R Pierce. The authors considered the repercussions of the new technologies on our political, social and cultural life and on our civilisation as a whole. The conclusions do not agree. As usual, some think that everything will go badly, whereas others are optimistic. On the one hand, there are those who deny the revolutionary significance of the phenomenon, placing the new technologies on a par with other discoveries; on the other hand, there are those who combat illusions about the prospects offered by these new technologies by saying that the die is already cast and pointing out that "computer power" is firmly in the hands of those who hold economic sway outside Europe.

I do not wish to enter into a controversy (because of the time it would take and because some of these propositions are clearly bound up with pseudo-problems), but I think we ought to remind ourselves of what history teaches us, namely that progress cannot be resisted. Moreover, we have seen that the new technologies represent a powerful factor for the development of civilisation. The best thing, therefore, is to be practical and to say that, just as with all other scientific discoveries - from the motor car to atomic energy - the new technologies are neither good nor bad in themselves; everything depends on how they are used. Consequently, the new technologies need to be controlled in order to be properly used. My thoughts therefore go first and foremost to the need to regulate this phenomenon which has burst out in the form of spontaneous vegetation - and that is not just because I happen to be a lawyer.

Various fundamental principles on the protection of privacy in the face of electronic data processing have been proclaimed in Europe. In this matter, thanks to the initiatives and support of the Council of Europe, the European Communities and OECD, through various conventions, resolutions and recommendations adopted since 1973, the situation seems satisfactory. By following the harmonisation guidelines laid down by these well-known organisations, almost all member States have adopted legislation on the protection of privacy to counter the dangers of intrusion by electronic data processing or by data banks. Other countries are in the process of doing the same.

In order to take stock of this legislative activity, the Council of Europe, it will be remembered, held an international conference in Rome in December 1982 on the problems raised by the drafting and application of the laws concerned. A similar conference took place in Madrid a few months ago. The present Lisbon Colloquy on European Law is a further token of the Council of Europe's keen interest in the new technologies. Computer science involves a series of relations which the law is called upon to regulate.

As we have seen, there has so far been spontaneous vegetation, but in the face of the growing development of the new technologies further problems may be expected to arise to which the law will need to seek solutions in order to prevent this luxuriant vegetation from becoming a jungle. On this point I should like to make two remarks.

First of all, it will, I am sure, be necessary to work out new legal concepts if these new problems are to be properly circumscribed, so as to avoid the danger of case-law - in the absence of new rules of law - hindering or slowing down the development of the new technologies. The existing rules of law which the courts are expected to apply even when confronted with novelties date from a bygone age when progress was not as fast as it is likely to be in the near future. For that reason, it will be necessary for lawyers to make a close study of the new technologies in order to predict which of their effects will need to be regulated. Close co-operation between lawyers and computer scientists is desirable for the purpose of laying the foundations of a new legal culture relating to automated information. In this connection I venture to mention that in my own city of Pisa, where a faculty of information science was set up in 1969, I recently sponsored an initiative of this kind which I can assure you has proved a remarkable experience.

My second remark is that because the new technologies are developing at a great pace, thanks to the possibilities their methodology offers to researchers, it is impossible to imagine the phenomenon being regulated by the ordinary processes of legislative production. These processes are too slow, and there is a danger of a law on the new technologies becoming obsolete as soon as it comes into force. In my view, after a framework of fundamental principles has been fixed in the matter, a high-level institution comprising politicians, computer scientists and lawyers should be set up for the purpose of drawing up rules as quickly as possible, as soon as a problem arises.

All this may seem strange or excessive from the point of view of our present legal culture. I am convinced, however, that it is the only reasonable way of dealing with the legal problems raised by the new technologies. Moreover, the discourse should be extended, on account of a certain parallelism, to include public institutions and their relations with the public. Two schemes have been conducted in the United States and Japan for the purpose of consulting the public on general issues by means of telematic networks. Such schemes, even though not yet common, serve as an alarm bell that can warn us of the dangers of the impact of the new technologies on the public rights of the individual. They could alert us, for example, to a possible change in election methods and, hence, to a decrease in direct participation by the public in discussions on election candidates' political programmes.

The increasing scope offered by informatics and telematics for obtaining and processing information enables us to verify the assertion that information is the key to democracy (the title of a study by a French professor, A Sauvy). In a democratic society it is necessary to ensure the fullest possible access to information, and as the new technologies permit an ever greater and efficient flow of information, they will contribute to the enhancement of democracy itself. It is important to ensure, however, that information is genuinely free and that it reaches the public properly and fully.

Almost all the democratic countries of Europe have legislation on the supervision of personal data files. In France there is the CNIL. In Italy there is a parliamentary committee that has powers to inspect the police files at the Ministry of the Interior. In the Federal Republic of Germany there is a commissioner for data protection who reports any irregularities to parliament. These forms of supervision are confined to personal data, and they should be extended to all information stored in electronically processed files.

The new technologies even affect education. In this field, too, new rules should be drawn up to counter the dangers of unsupervisable use of informatics in schools. The magazine "Nouvel Observateur" recently included a supplement ("Spécial Futur") on children and computers. It referred to "homo informaticus" and "magnificent mutants" in connection with schoolchildren whose learning is based on computer science. There is a danger of computers impairing children's ability to reason by providing them with results without any effort of deduction on their part. It is therefore necessary that children should be able to programme their computer research in such a way as to exercise their intellectual faculties and even reason with and through the machine.

As far as women are concerned, I might be tempted simply to say that there are no remarks to be made on the implications of the new technologies for women, because in any democratic society equality between men and women is guaranteed. Everyone is well aware, however, that if this fundamental principle is to be meaningful and effective it needs to be supported by the concept of equality of opportunity. An analysis should therefore be made of the already apparent effects of the new technologies on society in order to ascertain whether there are any examples of discrimination between men and women. It should first of all be mentioned that the literature on this subject is very meagre. This may be a sign of a lack of interest. Nevertheless, thanks to the action of women's associations, the problem has been brought

to the public's attention. In this connection it may be noted that the European Parliament instructed one of its committees to conduct an enquiry into the position of women in Europe. The committee, which was composed of female members of the European Parliament under the chairmanship of an Italian, Mrs Cinciari-Rodano, tabled a 600-page report in January 1984.

Among the 18 subjects which the committee investigated, one (no. 6) related to the introduction of the new technologies and the consequences thereof for the employment of women (Rapporteur: Mrs Spaak, Belgium). In connection with the committee's work, two international conferences were held. One took place in Manchester (United Kingdom) in May 1980 and dealt with "Equality for women - results, problems and prospects". The other organised by Mrs Roudy, the French Minister for Women's Rights, was held in Paris in January 1983 and dealt with the impact of the new technologies on female employment.

Among the committee's conclusions, which were addressed to the Commission and Council of the Communities, there was a recommendation to take urgent steps to alert all women's movements to the problems involved. Here, I have pleasure in emphasising that the present colloquy is an outstanding example of an immediate response to the problems raised by the European Parliament. As for the committee's other conclusions, I would mention a demand that the Community bodies abandon the neutralist attitude towards women adopted so far in documents and proposals on employment and the new technologies and that they explicitly regard women as a fundamental dimension of the issue.

In my view, this proposal is particularly noteworthy as it serves to counterbalance the tendency to deny the existence of a problem of discrimination between men and women, while recalling the principle of equality without taking account of realities. The committee addressed to parliament a draft resolution in which it emphasised its finding that between 1981 and 1984 the position of women had deteriorated because of several factors, including the unknown quantity of the introduction of the new technologies, which consequently constitutes a danger to female employment. The committee added that one of the lessons to be drawn from its study was that a network of training schemes should be set up to initiate women in the new technologies.

At this juncture I am fully aware that the various views I have expressed represent but a part of what ought to have been said. For example, I should also have mentioned such things as: the effects of the new technologies on health, with reference to what is already being called technostress; offences committed by means of computers, or computer crimes; the entirely automated factories of the future; and the dangers inherent in the military applications of the new technologies.

In conclusion, I would once more emphasise that all human activities are affected by the new technologies and that the law must play its part in opportunely regulating the effects of this phenomenon that is of great importance to our lives and our civilisation. To this end, we should work out and study the elements of a new legal culture which matches the nature of the new technologies.

NB This communication was largely based on a report submitted at the «Journées Européennes Francophones» (Tours, 1 and 2 June 1984), organised by the «Union Professionnelle Féminine - Fédération Française des Clubs de Femmes de carrières libérales et commerciales et de professions diverses».

PRIVACY LEGISLATION, DATA PROTECTION AND LEGAL PERSONS

by

the International Chamber of Commerce

INTRODUCTION

In its position paper "Information Flows - An International Business Perspective"*, the ICC urged Governments to join with them in promoting policies which encourage the freedom of business communication and to review those that create barriers and hindrances. Perhaps the best known laws affecting data flows are those concerning data protection which have been introduced by many European countries, primarily to defend the privacy of individuals. They cover the rights of "physical persons" to keep certain aspects of their lives private, free from outside interference or unwanted publicity, ensuring that others should only collect and use correct and relevant data about them on a fair and open basis. This paper addresses the issue whether such laws, as some do, should apply in the same way to legal persons, particularly to incorporated businesses ("business legal persons").

Although the data privacy problem of physical persons may have appeared greater than it turned out to be, the ICC recognizes the importance of protecting the privacy interests of physical persons and it respects the differing legal systems and traditions that ensure their protection. However, the ICC considers that protection of business legal persons in the same way as physical persons is inappropriate, unnecessary and harmful.

This paper examines the consequences of applying to business legal persons the regulations which have been designed to protect the privacy interest of individuals. It then mentions other, more adequate ways of protecting the data of business legal persons and finally discusses certain arguments sometimes put forward in favour of inclusion of legal persons in privacy legislation.

THE PRINCIPLES OF DATA PROTECTION REGULATIONS FOR PHYSICAL PERSONS

The two principal international instruments on this subject are the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data ("The Convention") and the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flow of Personal Data ("The Guidelines"). The principles of data protection set forth in these instruments are virtually identical, and those principles form the basis for almost all national legislation on the subject.

The title of the convention itself draws attention to the fact that this kind of legislation was originally instituted because of fears that computerization of personal data could raise the potential for a breach of personal privacy through a misuse of those data.

*) ICC Position Paper N° 3, Document N° 373-22/4 Rev. 4

The basic principles set out by these documents can be summarized as follows:

- personal data shall be collected, stored, processed and communicated only for specified and lawful purposes;

- the personal data shall be accurate, up to date, adequate, relevant and not excessive.

The procedures contemplated to promote the application of these principles include the following:

- any data subject is entitled:

  . to be informed by any data user whether he holds data related to that individual,

  . to examine such data upon request, and

  . to obtain correction or deletion of such data.

APPLICABILITY OF DATA PROTECTION PROCEDURES FOR PHYSICAL PERSONS TO BUSINESS LEGAL PERSONS

In examining the issue of data protection, it should be borne in mind that while the computerization of information and personal data may raise concerns for the privacy of physical persons, such computerization often produces considerable benefits for the persons who are objects of data gathering. For example, the computerization of airline reservations, electronic telephone directories, and banking and credit card services has provided an unprecedented quality of service that would not be otherwise possible.

Data protection legislation has to strike the right balance between the constraints it imposes and the freedoms it seeks to defend. Whether in the eyes of the ICC this has been done rightly in existing legislation for the protection of personal privacy is not an issue addressed in this paper. However, the ICC is convinced that in the case of business legal persons the balance is substantially different from that relating to individuals.

Although business legal persons do not have an "intimate personal life", they have, of course, data that they wish to maintain confidential. However, general regulations as described above are not the best means of protecting data about business legal persons.

Business legal persons expect that competitors, suppliers, government departments, and even individuals will keep computerized files about them. The computer is accepted as a normal tool for the efficient storage and sifting of information, a regular and, these days, essential part of

./.

business life. Companies maintaining such computerized files have a strong interest that the information contained in those files be timely, accurate and relevant, because decisions directly affecting the operations of these companies are based on this information. Apart from a few specific situations, such as credit rating, business legal persons have less interest in the accuracy and relevance of computerized files about them maintained by other business persons. Generally, business legal persons would not expect to be informed when computerized files about them are started by other business persons. To the contrary, they would strongly object to being obligated by law to notify other business legal persons that they were starting files on them, let alone to disclose the contents of such files with a view to implementing a right of correction or deletion of data.

Business legal persons are primarily interested in collecting, processing and using data - including data on other business legal persons - which will promote their own legitimate business interests. Applying data protection laws to data on business legal persons in the same way as they apply to data on individuals would result in an obligation to comply with one or several of the following requirements: registration of files, application for a licence, duty to inform other business legal persons of their inclusion in a file, obligation to give them access, obligation to erase or correct inaccurate, irrelevant or out-of-date information, obligation to disclose the release of data to others, and the obligation to record all transfers or uses of data.

Complying with such requirements could result in allowing competing firms access to confidential information, thus harming a company's position. The protection of confidential business information is of great interest to all enterprises and essential to the functioning of the economic system.

Complying with such requirements would also certainly make applications of information-management systems far more expensive and cumbersome. For example, two of the most common corporate files are those containing customer accounts (Accounts Receivable) and supplier accounts (Accounts Payable). Each of these files necessarily refers to legal persons, and each has many sub-files within it which could contain transaction histories, credit ratings, types of supplies either purchased or sold, and other information which is pertinent to a firm's business. Imposition of the legal person requirements would potentially expose each and every transaction which a company has with its suppliers and customers to review. Such transactions are numerous and would present a potentially unbearable burden on productivity if subject to review.

It thus becomes evident that the task of data protection authorities would be greatly increased with the effect that the data protection interests of individuals could not be properly looked after.

To the above arguments can be added that, to date, as far as is known to the ICC, there have been no cases of abuse of business data that would have been avoided by including business legal persons in data protection legislation. Nor is there any pressure from the business community for protection by such an inclusion.

./.

OTHER WAYS OF PROTECTING THE DATA OF BUSINESS LEGAL PERSONS

To the extent there is a need for the protection of data of business legal persons, a variety of other protective measures can be relied upon. They are already provided for in many countries, or they can be established under existing law. Examples of these are specific legislation on theft of business information, the legal obligations of employees concerning their employers' secrets, copyright law, the law of torts, contractual obligations, company law, credit rating legislation, banking legislation, and regulations applicable on government data files.

If further measures are needed with respect to specific problems, the ICC would be able to support solutions that strike an appropriate balance among the various interests that may be affected.

As par. 33 of the appendix to the OECD guidelines asserts, "... the notions of individual integrity and privacy are in many respects particular and should not be treated in the same way as the integrity of a group of persons, or corporate security and confidentiality. The needs for protection are different and so are the policy frameworks within which solutions have to be formulated and interests balanced against one another..."

ARGUMENTS SOMETIMES PUT FORWARD IN FAVOUR OF APPLYING PRIVACY REGULATIONS TO LEGAL PERSONS

It is sometimes asserted that people acting in groups enjoy the same rights as they do as individuals and therefore "groups" should be included in privacy legislation along with individuals. This argument fails to distinguish between the legal person as such and its members or its founders or those in some other way associated with it. Lists of members of clubs or employees of legal persons, for example, would or could be protected by normal (personal) data protection procedures. On the other hand, the tendency of many legal systems is to require disclosure of shareholders, officers, boardmembers and similar corporate information rather than to protect such information. The rationale is that in order to be able to enjoy the privilege of limited liability of shareholders, partners or members, substantial amounts of information have to be disclosed to protect those that do business with such entities.

The ICC submits that any data that falls between these two categories can be protected without recourse to the radical solution of inclusion of legal persons in general and business legal persons in particular. This protection could be provided under legislation designed to safeguard personal privacy.

Another alleged problem lies in the case of very small business legal persons. Here again, a distinction should be made between the shareholders and the legal person itself. Most of what is said in the preceding paragraphs applies here. To the extent that any real problem would remain, which is doubtful, this could be solved by a provision in privacy legislation which gives data on small legal persons, the disclosure of which could be tantamount to disclosure of sensitive personal data, the same general protection as individual data.

./.

A third argument often made is that in many computerized systems, personal and corporate data are intermixed and segregation would be impracticable. It is suggested that it might be claimed that the file is of corporate data and therefore beyond the scope of privacy legislation. The "leak", it is said, could then be plugged by bringing legal persons within the scope of the legislation. However, there is seldom any difficulty in segregating the data of legal and physical persons. Moreover, mingling data would not exempt the file from individual data protection legislation.

Another argument is that in those countries where legal persons already have been included in general privacy legislation, few problems have arisen for the business community. The ICC submits, however, that there has been insufficient experience in the implementation of such legislation to rely on this argument, particularly as the data authorities have rightly concentrated their limited resources on the protection of the data of individuals.

CONCLUSION

The balance between the need for data protection and the need to use data as efficiently as possible is very different for business legal persons than it is for individuals. To the extent data protection is required for business legal persons, this should be handled in each specific context in the form best suited to the specific situation. In many countries this has already been done in a quite adequate way.

Therefore, the data of legal persons, and specifically the data of business legal persons, should not be protected by the same legislative provisions which aim to protect the privacy of individuals.

In countries where such "inclusive" legislation exists or may conceivably be contemplated, National Committees or Councils of the ICC are advised to seek opportunities of acquainting governments with these matters with a view to making appropriate amendments to existing or draft laws. Minimizing unnecessary regulation would promote the international harmonization of laws affecting business information flow and contribute to the better use of information technology for the benefit of all.

GENERAL REPORT

by

Professor S SIMITIS
Data Protection Commissioner for the Land of Hesse,
(Wiesbaden, Federal Republic of Germany)

1.

Let me begin by expresing my gratitude to the rapporteurs for their thoughtful and critical contribution. I am quite sure that the initial reaction of many of those who received the invitation to the Lisbon Colloquy was rather sceptical. Data protection has been for a long time on the agenda of the Council of Europe and there is certainly no lack of international meetings dealing over and over again with the various protection problems. All four reports illustrate, however, that the Lisbon meeting does not fit into the usual scheme of data protection debates. Its purpose was neither to join the chorus of praise to the successful attempts at both the national and the international level to establish protection rules nor to concentrate exclusively on one of those small details which apparently are the only worthwhile object of a really serious discussion on the implications of data processing. To put it bluntly· what led to the Lisbon Colloquy was not the conviction that after a long and often complicated development, beginning in 1970 with the first data protection law, the Hessian, and highlighted by the 1981 Council of Europe Convention, an efficient protection can at last be guaranteed. Rather, it was the increasing doubts as to whether the failure of all the existing protection concepts should still be denied.

At first certainly a rather amazing statement. Year after year the list of laws and drafts aiming at better protection grows longer. In addition, a single look at the most recent documents, the Portuguese, Swiss and Italian proposals, shows how widespread is the readiness to acknowledge the necessity of specific rules governing data processing. There are, of course, still differences of opinion on a number of particular questions, for instance the inclusion of "legal persons" or the existence of particularly "sensitive" data, but on the whole, data protection has lost its exotic touch. While in the seventies any attempt to provide legislation was thought to be a daring experiment, data protection has become in the eighties a more or less normal part of the legislative programme. But paradoxical as it may sound, the signs of a deep crisis are no less evident. For at least three reasons data protection has entered a critical stage. All three have been mentioned at various points by the rapporteurs. Let me try and sum up.

2.

2.1

Probably the most obvious reason is located in the deficiencies of the legal infrastructure. All attempts at establishing data protection rejected from the very beginning, despite the differences of approach, restricting it either to the public or to the private sector. Data protection was seen and

treated as a general problem of data processing, irrespective of the qualification of the controller of the file. Consequently, preference was given to rules which made it possible to include all controllers. Technically no problem, particularly for continental legislators. They had only to apply well-known, traditional methods. Both the existing and the majority of the new laws are therefore characterised by extremely abstract language. The advantage is clear: as long as the law does no more than refer to general duties like the obligation to avoid any excessive storage, to process data only for legitimate purposes or to respect the interests of the data subject, widely differing controllers can be easily included. Their expectations may vary substantially; nevertheless none of them can act outside the framework of legitimate purposes and they all have to consider carefully the particular implications for the data subject. But even where a less traditional approach was chosen, like in Sweden, the result remains the same. Licensing is a measure applicable to every controller. The legislator largely avoids arguing in terms of substance and shifts, with the help of purely procedural rules, the responsibility to a particular agency. What the requirements of data protection really are, only becomes evident therefore in the process of granting the licence.

The flexibility of legislative reaction may thus have been maximised; the efficiency of protection was, on the contrary, minimised. Experience shows that where the laws dealt with processing in abstract terms which were more or less equal for all controllers, these same terms were increasingly interpreted in a way which permitted the controllers to uphold most of their previous processing policies. No wonder, since the interpretation of the expectations expressed by these vague and very general terms was left to the controllers. It was and it still is, for instance, their privilege to indicate the necessary amount of data and to delimit the implications of their legitimate processing purposes. Nearly all laws foresee, of course, control procedures. Where, however, the legislator, like in the case of data protection, aims at a substantial change in the specific policies of both the private and state agencies, it is not so much the subsequent control that counts but the direct as well as mandatory revision of the existing information expectations and processing policies. Therefore, as long as there prevails a lack of precise substantial rules clearly based on the particular conditions under which the different agencies pursue and fulfil their specific purposes, the reaction consists, as experience shows, in purely defensive strategies. It is no wonder that the reports of the data protection authorities rarely include lists of either state or private agencies having substantially reduced the amount of stored data. It is equally not surprising that large parts of these reports consist of cases where the control authority had to argue against the vigorously defended assumption of various agencies that their processing practice was well within their legitimate purpose and by no means affected the interests of the data subject in a way incompatible with the policies of the data protection acts.

Licensing systems are at first, of course, in a far better position. Since the licence presupposes an exact knowledge of the processing intentions and conditions, the legal restraints will always be phrased in a very precise way, deliberately restricting the decision powers of the controller of the file. But the really decisive question is the price to be paid for

this precision. Licensing systems are necessarily linked to a potentially increasing amount of administrative costs. The larger the number of files, the higher the costs. Each system has to be considered carefully, and for each system appropriate rules have to be developed. The moment therefore the number of files reaches a certain amount, the decision becomes unavoidable as to whether the increasing costs are simply irrelevant or whether in view of the continuously rising costs the licensing system should be restricted to a few selected cases. The latter tendency obviously prevails. The system may thus persist. Nevertheless, it can no longer claim to offer a satisfactory answer to the quest for a permanent and efficient control of all data processing.

2.2

The second, no less important reason is the changing political context. When in the beginning of the seventies the first data protection laws were enacted, the purpose was clear: their provisions were seen as the legal answer to the political and social threats attributable to both a changing data processing technique and the constantly increasing information expectations of state and private agencies. Data protection is thus far more than an attempt to domesticate a particular technique; it is the quest for an information policy which, irrespective of the techniques employed, deliberately reduces the information pressure on the individual and abstains as much as possible from the use of personal data. However, governments have not followed this path. On the contrary, they confronted the individual with more and more demands for personal information. In addition, they made increasing use of the information possibilities offered by automated processing. Instead of reducing the proliferation of personal data within the administration, access was facilitated and barriers which were regarded as unsurmountable were simply dismantled.

The reasons are rather obvious. Under the influence of a deteriorating economy, governments grew increasingly interested in a rationalisation of the services offered by state agencies as well as in an efficient control of all individuals profiting from those services. Both purposes can only be achieved in the final analysis by processing personal data. In order to find out, for instance, whether the conditions for social security payments are really fulfilled or whether taxes are paid correctly, the only way to do so is to retrieve the data of the persons concerned and to use all additional sources of information making it possible to obtain a complete personal profile. In fact, social security and tax authorities are simply employing the method often described as the "Rasterfahndung" method (automated comparison of various files) of the police. But even where, like in the case of a reorganisation of social security, no administrative measures affect specific persons, data processing remains the only appropriate instrument. Convincing conclusions on necessary changes can only be reached by carefully comparing the purposes and means of social security with the day-to-day experiences and with the claims and expectations of the protected persons. The institutional reform presupposes, in other words, a careful analysis of personal data. The diaphanous patient is the first and foremost condition for establishing new, cost-saving policies. Data processing presents no particular problems where

most of the information needed is already stored in data banks operated by the administration. Government has only to combine existing information in the light of the specific purposes of the tax or social security authorities. It is therefore not surprising that both the increased use of personal data and the changing attitude with regard to data processing have been repeatedly identified with the welfare state. For many, the crisis of data protection reflects in fact the crisis of the welfare state. The same openly activist state having first collected and retrieved an ever-increasing number of data, rearranges the information material in order to cope with the obvious deficiencies of its policies. The Swedish example is significant enough. Sweden was one of the very first states advocating an efficient data protection and developing new and original mechanisms with a view to better control of processing. Sweden is, however, also a most remarkable example of a radical review of the processing limits. It is, nevertheless, far too simplistic to reduce the problems caused by a revised attitude on the part of governmental agencies to the welfare state. The case of the United States is no less instructive than the Swedish experience. No doubt the administration lacks a comparable system of data banks. But this indisputable fact has neither influenced the attempts to use automated processing for an efficient control of individuals nor questioned its success. Like in most other countries, taxation and social security signal the turning point in the attitude of the administration and like everywhere else the authorities were interested in gathering and processing a maximum of personal data. The way they chose was, however, different. They for instance simply considered buying commercial files providing exactly the basic data they needed for their purposes.

Though the changing attitude has often been noted, the results were scarcely criticised. For reasons which are easily understandable. The prevailing notion in all demands for a revised access to data is the fight against fraud. The authorities, so the standard argument goes, are not concerned with everyone but just with a few individuals who are obviously acting against the law. The attention focuses, in other words, on those who profit unlawfully from the social security services or systematically avoid complying with their tax obligations and not on the normal law-abiding citizen. But what for many may seem perfectly convincing is, in fact, a short-sighted superficial approach to the processing problems. Even if the access to data, up to now clearly separated, is accepted, it can only be tolerated if the information used is correct. The experience of the data protection authorities in more than one country shows, however, that among all the obligations foreseen by the data protection laws the one permanently causing difficulties is the duty to correct erroneous or false data in order to secure accurate and up to date information. Broadening the access amounts therefore at the present time to deliberate proliferation of false or at least doubtful data.

In addition, all attempts to reduce fraud are linked to additional classifications of individuals. Probably the most striking feature of automated processing is that it makes it possible through the multifunctional use of the data stored to classify again and again the data subject. However, once a new group of persons is formed, all further reflections on these persons are inevitably linked to the fact that they belong to a certain

category. They are consequently judged first and foremost on the basis of membership of this category and not in view of their individual characteristics. To the extent therefore that classifications cannot be avoided, they must only be permitted if the group has been defined in an absolutely unequivocal way. To choose a wording tolerating or even provoking different interpretations amounts to the acceptance of a life-long labelling. However, particularly in cases of control of social security payments, the operation of the provisions legitimating the collection and the processing of data is such that a large number of persons having nothing whatsoever to do with a real fraud can be easily entered with the group of defrauders. Moreover, though the purpose of the processing is in most cases clear, the access is not restricted to the one particular situation having led to the demand for additional information. On the contrary, the various regulations open the way for other uses by simply establishing a processing privilege for a certain agency instead of providing it only for specific, strictly delimited aims. The example of the provisions against illicit employment is one of many. The chances for an efficient data protection are thus once more seriously endangered.

2.3

A third and last reason for the crisis of data protection is the modified technical infrastructure. Despite the indisputable differences of approach and regulation, all data protection laws are reactions to the profound changes in the processing technique caused by computerisation. None of these laws can, in other words, be understood without being constantly aware of its technological background. Consequently, the efficiency of data protection depends to a decisive extent on the ability to keep pace with technological development.

However, the technological premises of data protection laws are in at least two respects outdated. Automated processing was for a long time seen as the beginning of an unavoidable centralisation of information. All discussions on the importance of automation were therefore linked to the assumption that the processing had to take place within a system of centralised data banks. Characteristically enough, the same governments that presented the first laws on data protection elaborated detailed plans for a series of data banks concentrating the information needed by the administration. It is no less significant that the need for protection in the private sector was disputed by pointing to the lack of a comparable centralisation. But what in the seventies was thought to be a normal consequence of automation is in the eighties no more than a symptom of a technology reflecting, not the reality, but the history of automated processing. Decentralisation is the main and most important feature of the present processing methods. Little by little, the existing data banks are being replaced by small autonomous information systems. Moreover, processing is constantly being simplified and adapted to specific individual work conditions. An increasingly distributed data processing and not a growing centralisation is the dominant aspect. Multifunctional terminals integrating the various communication instruments change not only the structure of work but also the conditions of data processing. The result: nearly all the decisive elements of the data protection laws are obsolete. Neither does, for instance, the concept of a file correspond to the reality of processing; nor can control be secured any longer by instruments based on the existence of a centralised processing.

Furthermore, the technological development has led to new, far more efficient and comprehensive collections of personal data. Video and telemetry exchange are only two of a whole series of examples. With every step towards interactive systems, personal expectations, habits and preferences are recorded and integrated into an information system making it possible to obtain a most perfect profile of the data subject - from his favourite movies, his travel plans, his banking operations to exact indications on when he leaves or returns home. Never before have the possibilities of an exhaustive control of individual behaviour been so good. Moreover, instruments like the voice recorder and the already realistic possibility of storing the picture of an individual invisibly at different places in order to follow his movements, illustrate that along with the intensified control opportunities the possibilities for manipulative interferences constantly grow. However, each of these techniques was developed notwithstanding the existence of data protection laws. Once more, therefore, the changing technology challenges the actual protection rules and demonstrates the necessity of reviewing them.

3.

In brief, data protection is at a turning point. Occasional, small corrections are of no use. What is really needed is a new concept which takes into consideration both the changed political and technological premises. The difficulty should, however, not be underestimated. Data protection is not one out of many routine legislative tasks. Regulations for data processing touch the fundamental principles of a democratic society. Both the legitimacy and the legality of data processing depend therefore on its implications for the capacity of the individual to act and to participate.

Data protection is consequently incompatible with all political concepts which equate social reality with models realisable through a series of administrative measures. For any such view, data processing is an instrument permitting the best possible adaptation of the individual to expectations defined without his participation and regardless of his particular interests. The individual is no longer a subject of the social process but only the object of social policies. No wonder, therefore, that "preventive" actions, particularly in the police and social security fields, became the real battlefield for data protection. The list of examples is long, from GAMIN to the Norwegian project on social therapy and to the German attempts at guaranteeing a diaphanous patient. "Prevention" is always on the edge of a virtually unlimited data processing. The ritualised references to the solidarity principle or to public interests not only legitimate the intended action, they also prove to be a master key to whatever data files are needed.

Data protection is nevertheless not a late revival of the nineteenth century fiction of an omnipotent, absolutely sovereign, individual. Both the early remarks of the United States Privacy Protection Commission on "captive populations" and the reports of the data protection commissioners have shown how unrealistic is the assumption that data protection could more or less be reduced to the consent of the data subject and to a series

of rights ensuring individual control. Neither the employees of a big enterprise nor the customers of a bank nor the patients of a hospital have the power to influence data processing just because their consent has to be sought. The value of regulatory instruments like the informed consent of the individual depends entirely on the social and economic context of the individual activity. The lesson of standard contracts cannot simply be forgotten because the very same individual is not addressed in order to conclude a contract but to provide information which plays an essential role in all contractual strategies.

Data protection is therefore no more than a preliminary condition for a capacity to act, limited by objective as well as by subjective factors. However, the extent to which the individual can exercise this capacity depends decisively on the possibility of realising these limits and of examining each of their aspects critically. Both aims can only be achieved as long as the individual can follow closely the data processing and understand its implications. Data protection is, to this extent, an indispensable element of the ability to render communication with a democratic society possible.

However, once the link between data protection and such communication is seen, data protection appears as part of a larger system of rules governing the allocation of information within a democratic society. Significantly enough, both the first law, the Hessian law, and the latest, the Quebec Act, include protective measures as well as specific provisions against monopolisation of information. They may vary from a few rules on processing for research purposes or on the balance of information between parliament and government to a broad acknowledgement of the freedom of information. They nevertheless underline the importance of a comprehensive view of the different allocation aspects for the democratic structure of society.

4.

Data protection laws combine normative and technical barriers. The former are the necessary means making it possible to define the limits of processing, the latter a complementary but no less indispensable instrument securing the efficiency of regulation. Any new concept will, therefore, notwithstanding its own particular aspects, preserve this combination. The role and structure of both elements must nevertheless be reconsidered.

As far as the normative part is concerned, data protection must range from general provisions to a series of regulations based on a clear delimitation of specific areas of processing and therefore closely adapted to the conflicts typical of each of these areas. The efficiency of protection depends primarily on the ability to cope with the demands arising out of the particular processing context. Neither in the security field nor in the field of personnel information systems can convincing answers be found as long as the premises, purposes and implications of processing by security agencies or employers are not taken into consideration. Both the access to the data and the control of retrieval may constitute general protection principles. However, their real meaning can only be discerned in light of the concrete processing situation.

It is for this reason that the processing of employee data was chosen as one of the main subjects of this colloquy. Personnel information systems restructure the employer-employee relationship. They in fact lay the basis for a consequent personnel planning enabling the employer to treat the labour force with exactly the same criteria as is used for all other productivity factors. Data processing leads to the best possible adaptation of labour to the expectations of the firm's policy. At the same time, however, the multi-functionality of the data increases the risks emanating from the labour relationship, makes the employee far more vulnerable and reduces his chances to defend his personal interests. The existing provisions on data protection offer no assistance. The problems created by the use of personnel information systems can only be tackled by a regulation which departs from the specific situation of the employee and which places the rules on processing into the general context of labour relations. The approach may differ from country to country, as the example of co-determination in German law shows, but the aim remains the same: to adjust the protection to the specific aspects of the employer-employee relationship.

But again: personnel information systems are only one of many examples. The same demand for a conflict-oriented, functional approach leads once more to particular rules whenever the conflict-field is equally clear and delimited. Both the forthcoming use of chips in the banking sector and the implications of video and telemetric exchange can be quoted as additional regulation cases, along with the by now well-known example of the security authorities. They all confirm the necessity of a radical change in the orientation of legislative policy. Protection must not be sought solely through a few general rules but with the help of a carefully woven network of specific provisions, taking account of the particular features of the various applications of data processing. General rules can therefore have no other function than to fill gaps and should not perform a regulatory task clearly outside their capacity.

Only as long as a conflict-oriented approach is strictly observed will data protection cease to circumvent one of the most crucial but up to now generally repressed questions: whether certain parts of the information process should not be excluded from automation. The reverse side of the multifunctional use is a separation of the different information items from the original collection and storage context. But what may often seem acceptable becomes intolerable where, as in the case of personnel evaluations, the context is a necessary part of the information. As soon as the evaluation is disconnected from the particular conditions under which it took place and the specific purposes which it was meant to serve, the information is distorted. Data protection must include provisions excluding or even reversing the automation process, indicating in other words cases strictly reserved for manual processing and bound by adequate rules. Automation is not a one-way street.

A last remark with regard to the technical barriers. Information technology has up to now been dominated by the expectations of the potential users. They were borne in mind when the demand for "a comfortable processing" was articulated. Their reactions were carefully calculated when the

advantages of automated processing were praised. Consequently their information needs were seen as the main and decisive incentive in all attempts to design both hard- and software. From that moment, however, data protection became an accepted principle of political and legislative action. The constellation of factors which determined the development of automation must be changed. Instead of exclusively viewing the existing or assumed interests of the potential users, producers of both hard- and software must concentrate their attention equally intensively on the implications for the data subjects and therefore try to transform the demand for data protection into technical devices accompanying the production process and integrating barriers into the products which allow for a better protection. It is certainly neither possible nor admissible to assume that data protection can be reduced to a purely technical problem, but it is desirable and feasible to analyse carefully all the different aspects of protection in order to reorganise the production process and to increase the security measures. The functional separation of data banks, an internal transparency for better external control and measures against the dangers stemming from the expanding software market are only a few of the orientation factors for a revised production technique.

Moreover, the inclusion of data protection into the production process may very well lead to the reconsideration of (up to now) undisputed technical aspects of data processing. Compatibility has, for instance, never been questioned. It was, on the contrary, always presented as an essential condition permitting the user to select freely the technical elements of the automated processing, thus enabling him to combine the most different products. However, once the necessity of a clear separation of certain information systems is admitted, the inaccessibility becomes a crucial point in all data protection regulation. Compatibility can therefore no longer be solely evaluated from the standpoint of the potential user; it must also be examined on the basis of the consequences for access to the various data banks.

But whatever the results of the quest for a new data protection concept may be, the lesson of the past 15 years should never be forgotten. Even the most convincing rules are no more than provisional answers to the problems of data processing. No wonder, therefore, that laws like the Icelandic law explicitly limit their application to a very short period of years and foresee the obligation for the government to submit a new draft on time. An efficient protection requires rules guaranteeing the individual's capacity to act and to participate, notwithstanding the changes of technique and policy. Whether data processing evolves well within a democratic society or follows the path to an authoritarian society depends on the readiness of the legislator to accept the provisional character of his decisions and to ensure their flexibility.

LISTE DES PARTICIPANTS / LIST OF PARTICIPANTS

CHAIRMAN/PRESIDENT

Mr J C DE CARVALHO MOITINHO DE ALMEIDA, Directeur du Cabinet de Droit européen, Av. Oscar Monteiro Torres 39 1°, P-LISBONNE

GENERAL RAPPORTEUR/RAPPORTEUR GENERAL

Mr S SIMITIS, Der Hessische Datenschutzbeauftragte, 19, Mainzerstr., FRG-6200 WIESBADEN

RAPPORTEURS

Mr J BING, Norwegian Research Centre for Computers and Law, Niels Juels Gate 16, N-0272 OSLO 2

Mr H CORELL, Chief Legal Adviser, Ministry of Justice, S-103 33 STOCKHOLM

Mme M GEORGES, Chargée de mission, Commission Nationale de l'Informatique et des Libertés, 21, rue St Guillaume, F-75006 PARIS

Mr S RODOTA, Professeur de droit civil à l'Université de Rome. 90, via Castelfranco Veneto, I-00191 ROME

AUSTRIA/AUTRICHE

Frau Oberrat Dr. Waltraut KOTSCHY, Bundeskanzleramt-Verfassungsdienst, Ballhausplatz 2, A-1014 WIEN

Rat Dr. Georg SPRINGER, Bundeskanzleramt-Verfassungsdienst, Ballhausplatz 2, A-1014 WIEN

Dr. Alfred DUSCHANEK, Legal Adviser, Bundeswirtschaftskammer, Opernring 1/E/7, A-1010 WIEN

Dr. H RAAB, BMJ Finanzen, Hintere Zollamtsstr., 4. A-1030 WIEN

Dr. J CERNY, Osterreichische Arbeiterkammer, Prinz-Eugen-Str. 20-22, A-1041 WIEN

BELGIUM/BELGIQUE

Mr Claude DEBRULLE, Conseiller juridique à l'Administration de la Législation du Ministère de la Justice, Place Poelaert, 3, B-1000 BRUXELLES

Mr Jean MERNIER, Directeur général de l'Office régional Informatique, Membre de la Commission consultative de la protection de la vie privée, Rue des Primevères, 4, Bte 002, B-1348 LOUVAIN-LA-NEUVE.

Mr Jean SPREUTELS, Conseiller au Cabinet du Ministre de la Justice, Av Kamerdelle 88, B-1180 BRUXELLES

Mr E van den MEERSSCHAUT, Premier Conseiller aux services du Premier Ministre, Membre de la Commission consultative de la protection de la vie privée, Rue de la Gare, 51, B-9470 DENDERLEEUW

Mr J VELU, Avocat général à la Cour de Cassation, Professeur ordinaire à l'Université libre de Bruxelles, Avenue Kamerdelle, 77, B-1180 BRUXELLES

CYPRUS/CHYPRE

Mr R GAVRIELIDES, Senior Counsel of the Republic, Attorney General's Office CY-NICOSIA

DENMARK/DANEMARK

Mr J REIMANN, Head of Section, Justitsministeriet, Slotsholmsgade 10, DK-1216 COPENHAGEN K

FRANCE

Mme Charlotte PITRAT, Commissaire du Gouvernement, Mission à l'informatique, 24, rue de l'Université, F-75007 PARIS

Mlle Alice PEZARD, Direction des Affaires Juridiques du Ministère des Relations Extérieures, 37, quai d'Orsay, F-75700 PARIS

FED. REP. OF GERMANY/REP. FED. D'ALLEMAGNE

Dr. Wolfgang von POMMER ESCHE, Oberregierungsrat, c/o Bundesministerium des Innern, Hohe Strasse 73, FRG-5300 BONN

Dr. KUEPPERS, Ministerialrat, Bundesministerium für Arbeit und Sozialordnung, Rochusstr. 1, FRG-5300 BONN 1

Dr. U DAMMANN, Regierungsdirektor, Stefan Lochner Str. 2, FRG-5300 BONN 2

GREECE/GRECE

Mr A MARINOS, Conseiller d'Etat, 26, rue Efroniou, GR-16121 KAISSARIANI

ICELAND/ISLANDE

-

IRELAND/IRLANDE

Mr D LINEHAN, Department of Justice, EEC/Law Division, 5th floor, Block 1, Irish Life Centre, Lr. Abbey Street, IRL-DUBLIN 1

Mr James CASEY, Professor of Law, University College Dublin, IRL-DUBLIN 4

ITALY/ITALIE

-

LIECHTENSTEIN

Apologised/excusé

LUXEMBOURG

Mr R FABER, Ingénieur en chef à l'ARBED SA, 4 rue Pierre de Coubertin, L-1358 LUXEMBOURG

MALTA/MALTE

-

NETHERLANDS/PAYS BAS

Mr P J HUSTINX, Ministry of Justice, Postbus 20301, NL-2500 EH THE HAGUE

Mr D RAVESTIJN, Ministry of Home Affairs, Nassaulaan 10, NL-2264 CR LEIDSCHENDAM

NORWAY/NORVEGE

Mr Erik NYGAARD, Executive Officer, Department of Legislation, Ministry of Justice, Akersgt 42, PO Box 8005 Dep, N-OSLO 1

Ms Sissel Berdal HAGA, Head of Section, Department of Civil Affairs, Ministry of Justice, PO Box 8005 Dep, N-OSLO 1

Mr H SEIP, Director, The Norwegian Data Inspectorate, Box 8177 Dep. N-OSLO 1

PORTUGAL

Mr J SEABRA LOPES, Directeur-général, Ministère de la Justice, Av. Oscar Monteiro Torres 39, P-1016 LISBOA CODEX

SPAIN/ESPAGNE

Mr M SANTAELLA, Conseiller juridique au Ministère de la Justice, La Maso 29, ESP-28034 MADRID

SWEDEN/SUEDE

Mr Jan FORSSTROEM, Head of Section, Ministry of Justice, S-103 33 STOCKHOLM

Mr Nils RYDEN, Head of Division, Data Inspection Board, DI Box 12050, S-102 22 STOCKHOLM

SWITZERLAND/SUISSE

Mr Dieter FÜLLEMANN, Service de la protection des données, Département fédéral de la justice, Bundesrain 20, Buro 335, CH-3001 BERN

TURKEY/TURQUIE

Mr Seref ÜNAL, Juge d'inspection, Direction générale des affaires juridiques, Ministère de la Justice, TR-ANKARA

UNITED KINGDOM/ROYAUME UNI

Miss C STEWART, TI Division, Room 816, Home Office, 50 Queen Anne's Gate, UK-LONDON SW1H 9AT

OBSERVERS/OBSERVATEURS

CANADA

Mr Stephen SKELLY, Assistant Deputy Minister, Legal Services, Department of Justice, Kent and Wellington Street, Ottawa, Ontario K1A 0H8

Mr J W GRACE, Privacy Commissioner for Canada, Offices of the Information and Privacy Commissioners of Canada, Tower "B", Place de Ville, 112 Kent Street, 14th floor, Ottawa Ontario, K1A 1H3

Mrs Inger HANSEN, Information Commissioner for Canada, Tower "B", Place de Ville, 112 Kent Street, 14th floor, Ottawa Ontario K1A 1H3

FINLAND/FINLANDE

Mr Ilmari PIETARINEN, Chief Inspector, Ministry of Finance, Snellmaninkatu 1 A, BP 275, SF-HELSINKI 12

HOLY SEE/SAINT SIEGE

Rev. Père Antonio da SILVA, Directeur de la revue BROTERIA, rua Maestro Antonio Taborda 14, P-1293 LISBONNE

Professeur Jorge MIRANDA, Faculté de droit de Lisbonne Cidade Universitaria, P-1699 LISBOA

UNITED STATES/ETATS UNIS

Mr F R CRUPE, Director of the Information Industries Division, Office of Service Industries, US Department of Commerce, Room 2800, 14 Street and Constitution Ave., NW WASHINGTON DC 20230

EUROPEAN COMMUNITIES/COMMUNAUTES EUROPEENNES

Mr E GURA, Administrateur principal, DG XIII-B, Luxembourg-Kirchberg, rue A de Gasperi, Batiment "Jean Monnet" (B4-036), LUXEMBOURG

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT/
ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES

Miss Martine BRIAT, Information Computers and Communications Policy Division, 2 rue André Pascal, F-75775 PARIS Cedex 16

Mr François ROUSSEAU, Principal Administrator, Legal Service, 2 rue André Pascal, F-75775 PARIS Cedex 16

INTERGOVERNMENTAL BUREAU FOR INFORMATICS/
BUREAU INTERGOUVERNEMENTAL POUR L'INFORMATIQUE

Mr Lucio CLAVIJO CALDERON, Assistant to the Director of Policies, PO Box 10253, I-00144 ROME

Mr G R PIPE, TDRS, van Eeghenlaan 24, NL-AMSTERDAM

INTERNATIONAL CHAMBER OF COMMERCE/CHAMBRE DE COMMERCE INTERNATIONALE

Dr. Ray AUSTIN, International Adviser, UNILEVER PLC, Unilever House, Blackfriars, UK-LONDON EC4P 4BQ

Dr. Brandolino BRANDOLINI D'ADDA, President, Selezione dal Reader's Digest, Via Alserio 10, I-20159 MILANO

Mr Kevin HOLLAND, Data Protection Consultative, 25 Berkeley Square UK-LONDON W1X 6AB

Mr Herbert van TONGEREN, Data Protection Programs Manager, IBM Europe, Tour Pascal, Cédex 40, F-92075 PARIS-LA DEFENSE

GUESTS OF THE MINISTER FOR JUSTICE/INVITES DU MINISTERE DE LA JUSTICE

Sr. Luis Oliveira e Castro, Chefe da Divisão de Estudos da Comunicação Social, Rua Inocêncio Francisco da Silva, Lote 7, r/c Dt°, 1500 Lisboa

Drª. Maria Odete Santos, Deputada, Assembleia da República, Palácio de S. Bento, Lisboa

Cons. Antônio Payan Martins, Juiz do Supremo Tribunal Administrativo, Rua Cidade de Cádiz, 18-4° Dt°, 1500 Lisboa

Cons. Alberto Sampaio da Nôvoa, Juiz do Supremo Tribunal Administrativo Alameda Conde de Oeiras, Lote 53A, Oeiras

Dr. Feliciano Flor, Subdirector do Centro de Identificação Civil e Criminal Ministério da Justica, Rua Gomes Freire, 174, 1100 Lisboa

Dr. Sérge Lecercle Sirvoicar, Secretário-Geral Adjunto do Ministério da Justica Praca do Comércio, 1100 Lisboa

Dr. José Antônio Ferreira Marques, Advogado, Rua Rodrigues Sampaio, 69-2° E 1100 Lisboa

Dr. Fernando Duarte, Subdirector-Geral do Gabinete de Planeamento e de Coordenação do Combate à Droga, Cais do Sodré, N°. 8-3° Esq°, 1200 Lisboa

Dr. Osório de Castro, Bastonário da Ordem dos Advogados Portugueses, Largo de S. Domingos, 14-1°, 1000 Lisboa

Dr. Luis Lingnau da Silveira, Adjunto do Provedor de Justiça, Av. 5 de Outubro, 38, 1094 Lisboa

Mr Antonio Gomes Lourenço Martins, Procurador Geral Adjunto, R Escala Politecnica, Lisboa

SECRETARIAT

Mme Marie-Odile WIEDERKEHR, Head of the Public Law Division, Directorate of Legal Affairs

Mr Giovanni BUQUICCHIO, Head of the Central Section, Directorate of Legal Affairs

Mr Thomas Lawrence EARLY, Administrator, Public Law Division, Directorate of Legal Affairs

LIST OF COLLOQUIES ON EUROPEAN LAW OF THE COUNCIL OF EUROPE

1.	London, 1969	"Redress for non-material damage"
2.	Aarhus, 1971	"International mutual assistance in administrative matters"
3.	Würzburg, 1972	"The responsibility of the employer for the acts of his employees"
4.	Vienna, 1974	"Legal representation and custody of minors"
5.	Lyons, 1975	"Civil liability of physicians"
6.	Leiden, 1976	"Legal services for deprived persons, particularly in urban areas"
7.	Bari, 1977	"Forms of public participation in the preparation of legislative and administrative acts"
8.	Neuchâtel, 1978	"Standard terms in contracts"
9.	Madrid, 1979	"The liability of the state and regional and local authorities for damage caused by their agents or administrative services"
10.	Liège, 1980	"Scientific research and the law"
11.	Messina, 1981	"Legal problems concerning unmarried couples"
12.	Fribourg, 1982	"Principles and methods of preparing legal rules"
13.	Delphi, 1983	"International legal protection of cultural property"
14.	Lisbon, 1984	"Beyond 1984: the law and information technology in tomorrow's society"