Basic concepts of data protection and new information technologies

Poullet, Yves

Published in:
Problèmes législatifs de la protection des données

Publication date:
1987

Document Version
Publisher's PDF, also known as Version of record

ΣΥΜΠΕΡΑΣΜΑ

Η μετάβαση από την πληροφορική στην τηλεπληροφορική έχει προκαλέσει έκρηξη στις διαδικασίες επεξεργασίας των πληροφοριών, τόσο σχετικά με την συλλογή των δεδομένων, η οποία έχει γίνει περισσότερο δόλια, όσο και σχετικά με τα μέσα για τη μετάδοση και διανομή των πληροφοριών, καθώς επίσης, τέλος, σχετικά με τους ολοένα πλουσιότερους τρόπους επεξεργασίας.

Ενώπιον αυτής της έκρηξης είναι σαφές ότι το θέμα της προστασίας των πληροφοριών γίνεται καθημερινά όλο και πιο ανησυχητικό. Η απάντηση σε αυτή την ανησυχία δεν βρίσκεται, κατά τη γνώμη μας, στην ενίσχυση ακόμη περισσότερο επαχθών και ανεφάρμοστων διοικητικών διαδικασιών, αλλά στην επανεπιβεβαίωση των βασικών αρχών που τίθενται στη Σύμβαση του Συμβουλίου της Ευρώπης. Επομένως, αυτό που χρειάζεται, δεν είναι τόσο η τροποποίηση της Σύμβασης, αλλά η μεγαλύτερη *εμβάθυνση στις αρχές*, που ήδη περιέχονται σ' αυτήν.

Πρέπει να δοθεί πλήρης αποτελεσματικότητα στο δικαίωμα πληροφορήσεως του προσώπου το οποίο αφορούν οι πληροφορίες, μέσω της καθιέρωσης του δικαιώματος στη διαφάνεια, όσον αφορά τα κυκλώματα πληροφοριών μέσα από τα οποία κυκλοφορεί η εικόνα του προσώπου. Το δικαίωμα αυτό στη διαφάνεια είναι ιδιαίτερα σημαντικό, τώρα που οι υπηρεσίες τηλεματικής και τα κοινά δίκτυα διαφόρων επιχειρήσεων πολλαπλασιάζονται συνεχώς.

Το δικαίωμα πληροφόρησης του κυρίου του αρχείου (των δεδομένων) βασίζεται στην αρχή της σκοπιμότητας, η οποία δικαιολογεί την απόδοση ιδιαίτερης προσοχής στα δικαιώματα των διαφόρων παραγόντων οι οποίοι εμπλέκονται στην εκτέλεση μιας λειτουργίας. Η ίδια η αρχή της σκοπιμότητας προκαλεί έναν ειδικότερο στοχασμό, όσον αφορά ορισμένους τύπους επεξεργασίας (ηλεκτρονική μεταφορά χρημάτων, τηλε-διανομή, αρχεία εργαζομένων), όπου η εφαρμογή της αρχής αυτής επιβάλλει την εκ των προτέρων λήψη ορισμένων προφυλακτικών μέτρων (π.χ. απαγόρευση ορισμένων χρήσεων των δεδομένων).

Η καθιέρωση των δύο αυτών δικαιωμάτων και η εναρμόνισή τους δεν φαίνεται δυνατή χωρίς την διαιτησία των οργάνων προστασίας των πληροφοριών. Οι νέες τεχνολογίες πληροφοριών ενισχύουν τον ρόλο του ombudsman που διαδραματίζουν τα όργανα αυτά και τις υποχρεώνουν ταυτόχρονα να σκεφθούν από κοινού ως προς τις δυνατότητες καλύτερης διεθνούς συνεργασίας και να ενδιαφερθούν όλο και περισσότερο για τις τεχνικές που αφορούν την προστασία των ελευθεριών μας.

BASIC CONCEPTS OF DATA PROTECTION AND NEW INFORMATION TECHNOLOGIES

Background praper
prepared by professor Y. POULLET
Namur

INTRODUCTION

1. It seems to me that there are *five features* which mark the development of information technologies: *standrardisation, interactive services,* a *lack of openness,* the *internationalisation of data flows* and *increased capacity.*

2. So information-processing is no longer the exclusive preserve of businesses and organisations. The user-friendliness of the equipment means that it is no longer reserved for experts or locked away in areas to which access is restricted. Word-processors and micro-computers bring information-processing within the reach of secretarial staff and households. These facts lead us to raise three questions about our current privacy legislation, particularly about the principles laid down in the Council of Europe Convention.

— Are these regulations not based upon the assumption that the premises on which information is processed and stored can easily be located from the outset?

— Can the scope of these regulations be extended to purely private and family uses?

— Is the ponderous nature of some of these regulations compatible with the «trivial» nature of the processing concerned?

3. A combination of the ever-growing processing capacity of computers and the scope for transmission provided by telecommunications networks has made it possible to set up data communication services in both the professional sector (access to data bases, teleprocessing, electronic mail) and the public sector (electronic cash transfer, viewdata services).

The use of these services calls for consideration of two points:

— As regards telematic services for the public in general, the personal data concerned occur through the use of the service itself: The confiden-

tial nature of the data *does not*, as used to be the case under virtually all privacy legislation, arise from the *original content* of the data bank (most of the information therein at the outset is commonplace), but stems from data about consumers' use of the service (for example a cable TV service which stores viewing time and the type of programmes watched), which adds to the data already there, making it possible to work out a typical profile of every user, or group of users, thus enabling what an OTA (U.S.) report calls «electronic surveillance» to be carried out.
— The use of the services for everyday operations brings a significant change in the nature of the operations themselves. We should like to demonstrate this by citing the example of electronic payment, but the same considerations apply to the simple operation of watching a television programme, when information on the choice of broadcast, length of viewing time, etc, is recorded by a cable TV operator's central unit.

The information value of a cash payment is virtually nil. By paying in cash a purchaser gives the seller no information at all about his identity, and the seller would have difficulty in establishing any correlation whatsoever between the individual purchaser and any particular payment. The bank is detached from the consumer activity, unless, exceptionally, the acquisition of an item involves the granting of credit.

Payment by cheque slightly alters the information value of the payment. The seller is aware not only of his customer's identity, but also of the link between the customer and a financial body, in this case the cheque-issuing body. The bank, for its part, as the trader's name appears on the cheque, obtains information about the existence of a commercial relationship between the customer and the trader. This information remains limited, as does the length of time for which it is retained, unless re- encoding and transcription operations take place.

When cash is transferred electronically, the payment acquires information value which bears no comparison with that available when other methods of payment are used. For example, a withdrawal from an automatic bank teller enables the bank to retain a record of not only the identity of the person making the withdrawal, but also the place and precise time at which the withdrawal was made. The use of a POS terminal tells the bank the identity of the trader, the amount and time of the transaction and even its nature.

On the other hand, the trader has immediate access to information about the funds available to his customer and the existence of an account with a banking organisation. The use of computer technology for the management of such information increases its value, as by collecting,

cross-checking and comparing the aggregate of this primary information, the holder can obtain a precise picture of a customer's consumption patterns and travel and of the relative amount which he spends in each category, etc.

4. The smart card which may constitute the means to carry out such electronic payments makes it possible to discuss the fourth feature of developments in new information technologies: — the absence of transparency. The lack of transparency factor concerns the card itself, that is to say in regard to the informational content transmitted by this means of storage. Moreover, the lack of transparency relates also to the information circuits induces by the use of the card. The card may be multi-zonal. Who may access each of these zones? The bank, the retailer...? What do they do with the data which they acquire?

Beyond the specific problem of the smart card, the lack of transparency/openness of information cicruits may be characterised in two ways:

— firstly, it is a consequence of data processing, a result of the existence of numerous processing and storage locations, of which the users of data communication services are frequently unaware. This plurality of storage locations and processing centres exists within an enerprose even a group of enterprises and the increasing generalised use of single identification numbers is a contributing factor, and in enterprises which are members of national or international network.

— secondly, it conforms the growing *diversification* of firms' activities, due to technological change: banks more or less everywhere have embarked upon the activites of information and travel agencies, firms which produce data-processing equipment manage electronic mail systems, feed data bases, etc. It is sometimes difficult to continue thinking in terms of sectors of activity and to define a single purpose for the processing carried out within a firm.

5. The circulation of information which telecommunications make possible means that, as well as there being a lack of openness about storage and processing locations, there is a need to take into consideration the *international dimension of information flows*. Computing services can now be provided regardless of frontiers, and information may be processed sometimes in one country, sometimes in another.

While international operations, which are acknowledged to be necessary, cannot be impeded by privacy regulations, which GATT describes as non tariff obstacles, it is still important that equivalent protection should be given in the different countries, so that no «data paradises» can be set up.

6. Lastly, the increase in processing and storage capacity means that a different type of research can be carried out, based not on individual identifiers

but on specified characteristics of a group of people. A case which springs to mind is that of the Germans' use of «Rasterfahndung» (matrix search) to track down a German terrorist, Rudolf Clement Wagner: the police were able to find him by cross-checking data about electricity consumption. Firms will use the same technique to enable them to improve targeting of their customers, to decide where to canvass for custom for particular products, etc.

7. It is against the background of this kind of consideration that the text of the Convention has been analysed. To sum up, do the basic concepts of data protection as defined in the Convention enable an appropriate response to be made to the fears aroused by the development of new information technologies?

The structure of our analysis is based on that of the Convention:

— definitions and scope of the Convention (Article 2 of the Convention);

— principles relating to the preparation and carrying out of operations (Articles 5 to 7 of the Convention);

— principles relating to the right of access of the data subject (Article 8 of the Convention);

— principles relating to the international data flows associated with these operations (Article 12 of the Convention).

I. DEFINITIONS AND SCOPE

8. I shall consider three concepts, *personal data, the automated data file* and the «*controller of the file*».

The concept of «personal data» is defined as «any information relating to an identified or identifiable individual». This definition brings within the scope of the Convention any technical means of identifying an individual, i.e. not just a person's name, but also an identification number, recognition of his voice, dynamic recognition of his signature, his fingerprints or any other identification process, as covered by the term «record» in the American Privacy Act.

The concept is also applied in cases where a means of identification may be used by a group, such as a family group (for example when viewdata terminals are installed in the home), in so far as the attitude of each member of the group is identifed with that of the group. When, as in the abovementioned cases, or in that of «Rasterfahndung», the main purpose of processing is the identification of a group of people with shared characteristics, it seems to us that the definition remains valid, since the processing concerns people who are identifiable not as such, perhaps, but as members of a group. We

shall return to these theories which demand that further thought be given to certain principles of the Convention (see no 14 below).

9. «*Automated data file*» means «any set of data undergoing automatic processing». This definition is based upon the procedure used for processing the information and even includes any form of data recording enabling certain operations to be carried out involving the data; thus a word-processor would be an «automated data file». It would certainly be useful to include in the definition one further criterion in order to avoid bringing within the scope of regulations certain everyday data-processing applications which clearly do not constitute a threat to the individual.

In this context, should we retain the criterion of prior organisation of personal data and exclude any non-structured application in data bases? It would be dangerous to conclude that this should be done. Modern processing methods make it possible to use automatic search techniques even on *unstructured texts*. Thus, a word-processing program may be linked to a program enabling certain items of data to be extracted and correlated. In other words, it is the criterion of *retrievability* — attached not to a program but the complementary set of programs — which must be adopted, as has been done by Norwegian legislation, for example.

10. A very different question arises in relation to the concept of automated data files. The Council of Europe's recent work on the implications of *telemetry, interactive media* and *electronic mail systems* refer to this, and the ideas which the Council came up with may be extended to any telematic service. The concept of any automated data file suggests that a centralised, easily located file exists. Yet in the case of electronic cash transfers, for example, access to the service and the transferring machinery requires numerous information - processing locations: local files at POS terminals, storage or storing centres — in both public and private networks (those of the technical agents) - regional bank computer centres, etc.

In so far as all these locations are in contact with each other within a distributed computer system and all of the processing operations are part of a single larger operation, it is important for the concept of a file no longer to be linked to that of the processing location; it should instead be linked to the idea of a functional unit, involving one or more processing operations. The concept of a «*logical file*» has emerged from the carried out within the Council of Europe; this would allow for «ultimate location, through retrieval methods, of all the data dispersed in a network in the context of legitimate storage and processing within any given organisation».

11. In the same way, in order to cast more light upon the influence the network has on the processing of data required or created when the electronic

payment service is used, it is important to redesignate the «*controller of the file*», particularly in the context of telematic services, «*controller of the network*», responsible for all the personal data recorded in the network, i.e. what we have just called the «logical file».

The idea of a single person being answerable to data subjects and responsible for all the processing involved in setting up and carrying out an electronic service and for the compliance of this with data protection regulations is similar to that which has developed in relation to civil responsibility in the event of error or fraud during performance of a service. It is based on the same concern to make it easier for the user of these services to obtain information about them and to have access to them and to remedies; it is quite naturally the body which grants access to the service which is considered to be responsible for the entire network.

Can the concept of «controller of the file» be applied to an individual who, while making *purely private use* thereof, keeps on a micro-computer his diary, address list and other personal information? The question arises because of the standardisation of the use of computers, as already mentioned. The limits imposed by the Convention on the freedom to process data cannot apply to purely private information-processing, since this would constitute an infringement of individual freedom. However, this does not exclude the possibility of some data-processing carried out at home during paid activity (by people such as tele-workers) being brought within the scope of regulations.

Lastly, it is difficult to apply the concept of «controller of the file» — a person competent «to decide what would be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them» — to the area of *electronic mail services*, since it is up to those using the service to decide on the content and destination of messages. It is helpful to consider the need to apply the privacy regulations to these services, which are indeed private correspondence services, so that electronic mail enjoy the same guarantees of confidentiality as those provided by legislation, and even by national constitutions for written correspondence. These guarantees require all carriers, whether public or private, to take precautions to prevent third parties from intercepting messages and to prohibit message decoding by any unauthorised person.

II. PRINCIPLES APPLYING TO THE SETTING UP AND USE OF PROCESSING SYSTEMS

12. We shall consider three principles:

— that data should be *collected fairly and lawfully* (Article 5a);
— that data be stored for *specified purposes* and not be stored for longer than is required for those purposes (Article 5b, c, and e).
— that of *data security* (Article 7).

A. The principle that data should be collected fairly and lawfully

13. It was emphasised in the introduction that, particularly where telematic services are concerned, the most *sensitive* data are created through the use of the services. Hence the importance of making the user aware of the data items collected when such services are used and of the purpose for which they are processed. This gives rise to two ideas, firstly that of the «*transparency*» *of information circuits* and of their nature, and secondly that of the *free and informed concent* of the data subject, once he has been duly advised of the existence of these processing operations. These two ideas justify the regulations which certain countries have adopted on certain telematic services (such as Denmark's law on payment cards and the American Cable Communication Policy Act), obliging firms which offer such services to provide extensive information about the data collected, the network and the processing operations carried out within it.

This principle acquires particular significance in relation to smart cards. It is not admissible for such cards to carry secret, coded information, unknown to the holder. The latter must be aware of the types of information which may appear on the card and must know who is allowed to read it. *Data Protection Commissioners* could possibly take an interest in the manufacturing techniques for smart cards. Thus it might be possible for certain areas of information held on a payment card to be read only by traders, and not by banks, and others to be read by banks, but not by traders. With all the more reason, the same principle applies to medical and other cards with memories.

B. The principle of purpose specification

a. ...and expert systems

14. The development of *artificial intelligence* and *expert systems* promotes thoughts about the principle of purpose specification. These systems use

automated procedure imitating the human reasoning of an expert: thus it will be possible, using an expert system, to assess whether an applicant for credit is financially solvent and to deduce certain additional information on the basis of minimum data about a consumer or group of consumers.

On the subject of this kind of system, it is traditional to recall the rule laid down in Article 2 of the French law, according to which «no administrative or private decision involving assessment of human behaviour may be based exclusively on an *automated information-processing operation* providing a definition of the profile or personality of the person concerned». We believe that two things are needed to supplement this reference to the law. Firstly, this law could justifiably be extended to the use of expert systems to identify not just individuals, but groups of individuals. Secondly, it would be helpful if the person concerned were to be told of the existence of an expert system and of the fact that this was to be used as an aid to decision-making, and if the quality of the system could be checked beforehand (licence system) or if a court could order that it be checked.

b. ...and public telematic services

15. An analysis of the regulations (either projected — such as the American EFT Privacy Act — or already adopted) on *telematic services* gives rise to some further thoughts about the application of the principle of purpose specification. The first and most important of these relates to the prior definition through regulations of the types of processing allowed to those who offer such services. Article 9 of the German «Bildschirmtextvertrag», which applies to *public viewdata services*, lays down that the provider of the service may only process data required for his invoicing purposes and to obtain statistics about his customers. It prohibits the transfer of data to third parties and the preparation of *type profiles* of customers without their consent. It also limits the length of time for which data may be stored.

This desire set out in these laws to define in advance the type of data adjudged relevant, the length of time for which they may be stored and the various uses to which they may legitimately be put may offend some people, who favour allowing the firm or «controller of the file» to define the purpose of the processing carried out, subject to subsequent checks by judges or by supervisory bodies. The principle of subsequent checks has been adopted in the legislation of a good number of countries, such as the Federal Republic of Germany, Austria, Denmark, Norway, etc. It seems to us that new doubt has been cast on the principle of freedom to define the sort of processing thought to be relevant in relation to public interactive services, because of the fear induced by

both the nature of the data stored and the method of collecting them, fears which are also reinforced by data protection.

16. The second idea is connected with the prohibition of certain telematic services, such as home opinion polling. Similarly, certain types of processing ought to be forbidden with the exception of processing for billing purposes, such as the processing of data generated through the remote use of video games, insofar as this would make it possible to perceive the user's phychology.

17. The third is the distinction drawn between, on the one hand, the *contracting parties* to the service, i.e. the provider of the service and the person given the right to use it, and, on the other hand, the other parties involved in the performace of the service; in relation to EFT, the American draft (the EFT Privacy Act) refers to the «EFT Service Providers», i.e., in this case, the traders who have terminals on their premises, the feeder centres which are shared by different service providers, carriers, etc.

Regulations on the processing done by the second category are more stringent. A strict limit is imposed on their right to store data for the purposes of their service, and they are prohibited not only from making commercial use of the data, but also from creating pools of information which could be useful to members of the network. In this context we find again the legislative distinction drawn in certain countries (for example the Federal Republic of Germany, Austria and Denmark), between firms which process data as part of their own activities and those which do it on behalf of others and which are subject to stricter regulations (requiring permission).

c. ... and the tendency to conclude cooperation agreements

18. This distinction seems all the more necessary with the increase in cooperation agreements between enterprises offering telematic services. This observation extends beyond the framework of public telematic services. The need to define common transmission norms and to propose to different enterprises within a sector, even all of them, communication services (electronic mail servies, shared data bases, etc.) explains why there is a great increase in the creation of services which are common to several enterprises, and sometimes set up in separate and distinct enterprises. Such cooperation agreements may also be explained by the investment costs necessary for creating such services. They help share the research and development costs.

19. Accordingly, the transmission of personal data within these networks can only result in the creation of vast information centres shared by those availing of the network.

d. ... and the diversification of firms' activities

20. To conclude our thoughts about the principle of purpose specification, we should like to highlight one consequence of the diversification of firms' activities which arises particularly from their use of new technologies. In this respect, the example of the media is noteworthy: *the printed press* has very frequently moved into the audio-visual field, offering *on-line* information services, etc. There are few banks which, within the framework of telematic banking services, do not offer travel agency services, and even provide commercial information. This trend away from specialisation gives rise to a fear that the data processed in the context of one activity could also be used for another, adding to the information collected about individuals. In the same way as some legislation requires certain firms (for example Canadian legislation in respect of telecommunications firms) to keep separate accounts in order to avoid any overlaps, it is important that the authorities responsible for the supervision of data should, for the sake of the principle of purpose specification, insist that a clear distinction be made between different types of processing and that different «controllers of the file» be made responsible for the processing carried out for each of the firm's activities.

C. The principle of security

21. The particular nature of the processing operations which are part of a telematic service means that the locations at which processing is carried out are scattered and that it is completely impossible to provide *physical security systems* in certain locations (e.g. automatic bank tellers in public places).

The obligation laid down down by the Council of Europe Convention to take appropriate «*security measures*» makes it necessary to consider the whole information transmission network(s), including the card giving access thereto. In particular, if a card with a memory is involved, the service provider agrees to take every precaution to prevent anyone other than authorised persons from gaining access to the information stored in the memory (CNIL, 5th activity report, 1985, p. 150). The use of certain security keys (coding) could be made compulsory for certain information transmission operations.

As there is a major public interest in this field, the legal obligation should derive from direct or indirect regulation (approval licence). The latter solution, more flexible and more in line with technical developments, would fit in with a recommendation made to the European Community (see the MOVILLE-POULLET report drawn up as part of FAST: «LA DEMANDE FINALE EN TELEMATIQUE») that feeder centres (technical agents in particular) be labelled on the basis of a security plan drawn up by standardising agencies,

which should carry out their work in association with the data protection authorities.

III. THE RIGHT OF ACCESS

22. The right of access is to be interpreted in the broadest sense, in the light of any measure which aims to ensure that the data subject is sufficiently well aware of the information held and processing operations carried out by the «controller of the file» and of the procedures through which remedies may be sought if incomplete, false or irrelevant information is held.

A number of recommendations in respect of interactive services, the aim of which is the «transparency» of both the information collected and the routes followed by it in the course of the operation, have emerged from the study of the principle that data should be collected by fair and lawful means.

The existence of a «controller of the file» makes it possible to designate a single person to grant the right of access and to correct the information in question throughout the network. Particular attention must be paid to the effective exercise of the «*right to monitor*», because of both the diversification of firms' activities and the increasing number of co-operation agreements between firms providing telematic services. The «right to monitor» requires the right to know about the third parties to whom the information is communicated as well as the right to oblige these third parties to rectify wrong, incomplete or superfluous information.

23. The creation of an ever-increasing number of public interactive services suggests the possibility of new *methods of implementing the right of access*. In the context of public telematic services, could service providers not be obliged to make available, free of charge on a screen page, all the information on processing usually sent in writing (nature of the data processing), and even to enable the user to make direct use of his right of access through an intermediate terminal?

IV. INTERNATIONAL ASPECTS

24. Of course, only 10% of international data flows involve personal data. Yet, such flows are obviously increasing: on the one hand, certain interactive services are being made internationally available, and, on the other hand, telecommunications are considerably increasing the number of connections between computers in different countries.

Hence the desire of international agencies like the Council of Europe not

only to define common data protection standards enabling countries which have adopted equivalent standards to reject any restriction of international flows on the grounds of data protection, but also — and this second task remains to be carried out — to promote *rules under private international law* laying down uniform criteria in respect of the choice of applicable law and, particularly, the *scopes* of national legislation.

To be convinced of the utility of laying down substantive rules of private international law, suffice it to reflect on the, by no means exceptional, situation where personal data relating to a citizen of country A are collected in country B, processed in country C and unlawfully accessed by a citizen of country D by means of a portable terminal connected to a network in country E. Which law do we apply if the data subject complains about the use made by the citizen of country D in country F. The law of the data subject, the law where the data are processed, the law of the users' terminal situated occasionally in country E or, finally, the law of the country where illegal use causing damage occured?

25. Perusal of Article 12 of the Council of Europe Convention leads us to a further idea. This article provides for derogations from the provisions in respect of the freedom of international flows for certain data or types of processing, insofar as the legislation of the country concerned does not provide *equivalent protection*. The numbers of such derogations are increasing in respect of public interactive services. In the EFT field, for example, the Danish Payment Act obliges banks which provide such services to carry out their processing within the country, unless otherwise authorised by the Minister of Industry; the Austrian bill on viewdata services makes it compulsory for foreign data feeders to abide by the provisions of the Austrian Law on data protection.

This trend makes it necessary to find a better definition of «equivalent protection»: does it mean identical or just similar protection? Who will determine if the protection offered by a particular country is equivalent to that offered by another country? Should only general data protection laws be examined for this purpose or should other specific laws or texts be looked at which make it possible to find an equivalent solution in a concrete case? In any case, in these areas where the provision of services necessarily has an international dimension, the importance of laying down common standards in order to avoid any nationalistic regulatory «reflex action» is emphasised.

26. Should encouragement be given to the adoption of flexible instruments such as the sector's own *codes of practice* (for example, the Code of Practice put forward by Eusidic in respect of electronic mail)?

It is certain that such flexible methods of regulation are of great use in a constantly changing domain. Nevertheless the final say should rest with the

public authorities responsible for data protection, and it should be noted that a sectoral approach in so far as it suggests that account should be taken of a particular sector is dangerous. An approach based on *the type of operation* in question would be preferable, in so far as, on the one hand, the diversification of an enterprise's activities, and on the other hand, the accomplishment of operations often involves actors from different sectors (e.g. in EFTPOS transactions there are consumers, retailers and banks involved). The interests of all the actors involved in the carrying out of an operation should therefore be taken into account.

27. To develop this theme, there is also a fear that the adoption of international private standards for data protection may be used as a means to forestall and exert pressure on data protection authorities. By way of response to this type of possible pressure, it is imperative that data protection authorities be aware of the urgent need to work together on the elaboration of effective rules for *the international level*. It is at *that* level and not the national level where the major data protection factors and issues will be played out in *tomorrow's society*.

CONCLUSION

28. The move from data processing to data processing via telecommunications has caused a rupture in the procedures for processing information both in regard to the collection of data which has become more insidious and in regard to the means for transmitting and distributing information, as well as, finally, in regard to the means of processing which have become richer.

Faced with this rupture, it is clear that the issue of data protection becomes more preoccupying with each day. The response to this preoccupation is not, it seems to us, to be found in a further strengthening of burdensome and impractical administrative procedures but in a reaffirmation of the basic principles set out in the Convention of the Council of Europe. This would entail not so much an amendment (s) of the Convention, but rather further analysis of the principles already contained in it.

The data subjects right to information must be given its fulleffectiveness by enshrining the right to be aware of the information circuits through which our image circulates (circuit transparency); this transparency right is particularly important at a time when telematic services and networks shared by several enterprises are multiplying.

The file keeper's right to information rests on the finality principle which justifies according particular attention to the rights of the different actors involved in the carrying out of an operation. The finality principle also suggests

more specific reflection in regard to the different types of processing (electronic transfer of funds, tele-distribution, workers' files) where the application of the finality principle merits certain preliminary precautions (e.g. prohibition on certain uses to be made of the data).

The grant of those two rights and their reconciliation appears impossible without the *arbitration of the data protection authorities*. The new information technologies reinforce their ombudsman role and at the same time oblige them to reflect together on the possibilities for better international cooperation and to be increasingly concerned about the techniques which condition the protection of our freedoms.

CONCISE BIBLIOGRAPHY

J. BING, Impact of Developing Information Technology on Data Protection Legislation, Report prepared for ICCP, OCDE, 1986.

J. BING, International Services Bureaux and T.D.F., Complex 1/85, Norvegian University Press, Oslo.

J. L. BROWN, Implications of the informational nature of payments, Computer Law Journal, 1980, 2, 153 et s.

H. BURKERT, Datenschutz und Informations - und Kommunikationstechnik: Eine Problemskizze, G.M.D., Bonn, 1985.

D. H. FLAHERTY, Protecting Privacy in Two-way Electronic Services, Mansell, London, 1985.

D. FROYSTAD, Data Protection in practice: Identifying and matching elements, Teresa (17), Complex, N.R.C.C.L., Oslo, 1984, Complex 8/84, Norvegian University Press, Oslo, 1984.

H. GODSCHALK, Datenschutz am point of sale, Computer und Recht, 1987, No 7, 416 et s.

D. A. MARCHAND, Privacy, Confidentiality and Computers: National and International Implications of U.S. Information Policy, Telecommunications Policy, Sept. 1979.

Office Technology Assessment, Electronic Surveillance and Civil Liberties, Congress of U.S., Washington, 1985.

Y. POULLET, Privacy et services électroniques d'information, in Electronic Information Services: Legal Aspects, Report prepared for the Legal Observatory of the European Commission, Jan. 1987.

Y. POULLET, TEF et protection des données à caractère personnel, Rapport présenté au 6ème séminaire de droit de la consommation, EFT and Consumer Protection, L.L.N., 1987.

S. RODOTA, Protezione dei dati e circulazione delle informazioni, Riv. Crit. del Diritto Priv., 1984, No 4, 721 et s.

J. SCHNEIDER, Datenschutz und New Medien, NJW 1984, 390 et s.

A. WESTIN, Privacy Issues and the Implications of Home Banking, American Banker, June 3, 1981.