UIC John Marshall Journal of Information Technology & Privacy Law

Volume 3
Issue 1 *Computer/Law Journal - 1981*

Article 14

1981

Teledoc and Open Records, 3 Computer L.J. 457 (1981)

Peter Seipel

TELEDOC AND OPEN RECORDS*

by PETER SEIPEL

TABLE OF CONTENTS

* This article is a revised English version of a guest lecture given at the Norwegian Research Center for Computers and Law in August 1980.

> The right of public access shall now, according to a decision of the Board of the Municipality, also apply to the local computer file. In view of this, the computer terminal of the municipality (in the cellar of the Municipality Centre) will be exhibited to the public each Saturday between noon and one p.m. The current will be turned off so that there will be no risk that unauthorized persons can look into the system.

Grönköpings Veckoblad (The Grönköping Weekly, a satirical Swedish journal published monthly), October 1980.

I. INTRODUCTION

The right of access to documents that concern state and municipal administration and the administration of justice is known in Sweden as "the right of access to official documents" or, simply, "the principle of publicity."[1] In a comparative international perspective it may be said that the openness of recorded official information under Swedish law is unusually far-reaching. Above all, what distinguishes the principle is its long history: it was first recognized in the Freedom of the Press Act of 1766. Since then, the principle has been upheld except for a period of about four decades beginning in 1772 which was marked by royal supremacy.

Over the years the principle has been the target of criticism, and different views have been advanced on the proper balance to be struck between openness and secrecy. Public authorities have expressed their opposition to the principle. There are also problems of costs associated with the implementation of the right of access. Nevertheless, the right of access to official documents is today regarded as an indispensable element of the Swedish legal system and of the political life of the country. Swedes tend to have difficulty in understanding that other countries often apply the reverse

1. An overview of the right of access to official documents under Swedish law may be found in ADMINISTRATIVE SECRECY IN DEVELOPED COUNTRIES (D. Rowat ed. 1979). See the report on Sweden by Sigvard Holstad at 29-50.

principle, i.e., a principle of discretionary secrecy. They find it quite natural that many countries, such as Denmark, Norway, and the United States, have moved or are now moving in the direction of broader, legally enforceable rights of access.

This trend toward openness creates new opportunities for comparative studies of the structure and effects of different national laws on the right of access.[2] No such effort, however, will be made in this Article. Its scope is limited to the Swedish situation, but it is my hope that the survey will still be of interest to an international audience in that it will describe a fairly advanced national legal situation and shed some light on the global problems of openness in computer systems used by public bodies.

For most of its existence the right of access to official documents or, simply, the right of access, has been applied in a static information environment in which written and printed documents carry the information. During recent decades, however, the introduction of automatic data processing has brought about considerable changes and a corresponding need for new concepts. At the early stage the uses of computers in public administration, courts, and so forth were uncomplicated: they involved maintenance of files of a simple structure, usually stored on magnetic tapes, which were processed for a few well-defined and permanent purposes.[3] For instance, each county maintained population files storing information such as name, age, address, income, weapon licenses, and church membership. Files of this kind were used to produce printed listings, index cards, and various kinds of printed notifications. Even computer applications of this simple type caused difficulties for the application of the traditional rules on the right of access.[4]

The continuing development of computer technology and its applications have further emphasized the need for adjustments and rethinking. Large databases of a complex nature which can be used for planning, information retrieval, and decision-making in sundry activities give rise to new difficulties that are not always easy to deal with. To keep pace with such developments, the basic provisions on the right of access in Swedish legislation have recently been amended twice. These amendments became effective on July 1, 1974 and on January 1, 1978, respectively.[5] In the autumn of 1980, a public

2. *Cf.* ADMINISTRATIVE SECRECY IN DEVELOPED COUNTRIES, *supra* note 1, at 1-26. *See also* CIVIL SERVICE DEP'T, DISCLOSURE OF OFFICIAL INFORMATION, A REPORT ON OVERSEAS PRACTICE. (London: HMSO 1979).

3. *See, e.g.*, Aron, *Information Systems in Perspective*, 1 COMPUTING SURVEYS 213 (1969); J. MARTIN, COMPUTER DATA-BASE ORGANIZATION (1977).

4. SOU 1966:60, Offentlighet och sekretess, at 113.

5. Government Bills 1973:33 and 1975/76:160.

committee proposed a new statute which is intended to complement the existing basic rules and to clarify the right of access to public computer systems.[6]

One computer application of particular interest in the present framework involves exchange of messages and organization of "meetings" via geographically dispersed computer terminals. Systems of this type have been given different names depending upon the interest that is taken in them and their main orientation. Such names include teleconferences, computer-assisted text communication, electronic message systems, and electronic mail.[7] The term "teledoc" shall be used as a general term to refer to all such systems. The term is intended to remind one of words such as "telephone," "telegraph," and "teleprinter." The morpheme "tele" means that something takes place over distance, and the morpheme "doc" is intended to stand for "*d*ialogue and *c*onference" and for "*doc*umentation." The term, thus, refers to some important characteristics of this particular usage of computer networks.

Teledoc systems will probably become an important and widespread tool in administrative activities of various kinds. One existing international teledoc system handles about 25 million messages per year.[8] The technology to support fully operational teledoc systems is available today at a reasonable cost and will most likely be improved and refined to meet different needs and requirements. The obstacles to its further development and acceptance are varied. Some of them pertain to attitudes and work habits, others to organizational and legal matters.

Several important legal issues of teledoc systems have recently been illuminated by a project carried out at the Swedish National Defense Research Institute (FOA).[9] The teledoc system of the FOA, the so-called KOM system (originally KOM 79, presently KOM 81),[10]

6. SOU 1980:31, Offentlighetsprincipen och ADB.

7. A general treatise of various types of information exchange within groups whose members may be separated by both space and time may be found in R. JOHANSEN, J. VALLEE & K. SPANGLER, ELECTRONIC MEETINGS (1979).

8. Panks, *The EMS Revolution*, 34 Computerworld 14 (1980).

9. I am grateful to Messrs. Jacob Palme and Ake Lindwall of the Swedish National Defense Research Institute for providing me with valuable information on the KOM system and its uses. A detailed documentation of the system has recently (March 1981) become available in connection with the FOA's application to the Data Inspection Board for a prolonger license. *See, e.g.*, FOA rapport C 10166-M6(M9), Erfarenheter av användning av telekonferenssystemet KOM by Jacob Palme et al. Reports in English on the KOM system can be obtained from the FOA. A general description is found in the COM Computerized Teleconferencing System by Jacob Palme. Technical information can be found in FOA report No. C 10129E.

10. The original version of the system was named "KOM 79." This system can,

was the first operational teledoc system in Sweden—or at least the first system that came to public knowledge and obtained a license from the Data Inspection Board. Such a license or permit is a prerequisite for the use of systems of this kind.[11] The license granted to the FOA in January 1979, was valid until March 30, 1981. Similar licenses have also been granted to the computer center of the University of Stockholm and to the University of Linköping. In March 1981, the FOA's license was extended for an indefinite period.

In late 1979, three persons asked to be given access to KOM 79 under the Freedom of the Press Act (FPA). The requesters in particular wanted to study messages that concerned a certain matter, but they also sought access to the entire system with the exception of secret materials. (The role of secrecy will be discussed later.) Moreover, the requesters wanted to use one of the terminals without any interference or supervision by the officials of the Authority. The request was refused. One of the reasons given by the FOA was that the data in the system could not be regarded as "official documents" which are covered by the right of access. The refusal was appealed to the Administrative Court of Appeals of Stockholm that held that the data in KOM 79 could not be withheld from the public. The court, however, decided against the appellants in regard to their request to perform uncontrolled searches of the database from a terminal.[12] The Supreme Administrative Courts affirmed this holding on September 24, 1980.[13]

The teledoc system KOM and the case just referred to illustrate some basic problems of the right of access to computerized data. Many of the details of these problems will be treated later but, to begin with, a brief introduction must be given to the Swedish legislation on the right of access to official documents and the complementing legislation on official secrecy. In particular, attention shall be devoted to those parts of the legislation that concern automatic data processing.

---

according to a decision of the Data Inspection Board in March 1981 (DN:4203-80), be used until October 1, 1981. The new version, "KOM 81" or simply "KOM," was at the same time accepted by the Board. Much of this article deals with KOM 79. The different names, KOM 79 and KOM 81, will be used to distinguish between the original and the modified system.

11. PER-GUNNAR VINGE, FEDERATION OF SWEDISH INDUSTRIES, EXPERIENCES OF THE SWEDISH DATA ACT 13 (1975).

12. The Administrative Court of Appeals in Stockholm: Judgment, July 4, 1980, 661-1980.

13. RA 1980 2:42.

II. THE AIMS AND SCOPE OF THE RIGHT OF ACCESS

The basic rules governing the right of access to official documents are part of the Swedish Constitution and are contained in Chapter 2 of the FPA. The present statute was enacted in 1949.[14] Historically, the right of access was regarded as an accessory or a complement to the right to reproduce official documents in print and thus is an integral part of the freedom of the press. This point of view is still important, but the right of access has gradually gained independence and now fulfills purposes of its own that tend to place the original purpose in the background.

The legislative history of the rules on the right of access shows that the lawmakers made certain arguments and stated certain aims that are now firmly established.[15] An illustrative example may be found in a report issued in 1966 by the so-called Publicity Committee.[16]

First, the Committee found that the right of access helps to create an efficient "government by the people" since the public can easily obtain information about the activities of state and local government organs. Second, control of decision-making and other activities of public bodies is facilitated. On the one hand, this creates greater confidence in the authorities since they carry out their activities in the open, and, on the other hand, the rule of law is safeguarded. Third, the right of access contributes to the efficiency of public administration. Decisions, methods, and means can be discussed with full knowledge of relevant documents. It may be mentioned that the organization and the forms of work of Swedish public authorities are important in this respect. Written documents play an essential role in government affairs, and the independence of the boards and agencies in relation to the ministries is also significant to the extent that documents become official. Fourth, the Publicity Committee gave attention to the value of the right of access for commercial and related activities in society. According to the committee, duplication of work may be avoided by allowing access to source materials and reports prepared by public authorities. The commercial benefits of the right of access, however, are more uncertain and disputed than the other effects. The successor of the Publicity Committee, the Committee on Publicity and Secrecy, which was set up in 1969, concluded that the right of access may result in commercial uses of interesting and valuable information. According

14. SFS 1949:105. (complete revised version in SFS 1979:936).

15. *Cf.* M. HEDBERG, Offentlighotsprincipen och ADB, ADBJ-rapport 1980, at 12-19, 102-112.

16. SOU 1966:60, Offentlighet och sekretess, at 71-74.

to the Committee, however, this consequence of the right of access should not be taken as an independent purpose but rather as a side effect that may not always be desirable.[17]

In all legal systems in which it exists, the right of access to official documents is a complex phenomenon; it must be evaluated and understood in light of other related and interacting rules.[18] For example, in Sweden, there are rules concerning indexes of adopted and concluded matters, filing of documents, archives, and similar matters. These rules have obvious effects for the scope of the right of access and the burden that is placed on those who seek information. There is a lack of coordination between these rules, which are distributed in several statutes and ordinances, and the rules in the FPA. There are also rules concerning open proceedings and meetings, and the rights of parties with a direct interest in a matter to obtain judgments, decisions, and related documents. Swedish law provides for such rights of a secondary or complementary nature in relation to the general right of access. There is also statutory support for the principle that documents should be communicated to persons who may be affected by them. Finally, there are certain obligations of public bodies, i.e., courts and public authorities, to provide information and advice in general. Swedish law does not impose absolute duties in this respect since the basic principle is that information regarding the contents of documents and the activities carried out shall be provided to the extent that it is expedient. Information services to the public are beginning to attract more attention. As a result, the Data Legislation Committee recently suggested further study on the relationship between the passive right of access and the creation of active systems for information dissemination.[19]

The right of access cannot be without limits. There are various opposing interests that offer reasons for exemptions and modifications. To begin with, there are legitimate needs for secrecy. Section 2:2 of the FPA exhaustively enumerates those needs that are recognized by the constitution. The list contains no elements of an unfair or surprising nature and is similar to corresponding enumerations in other national laws. Among the permitted restrictions on the right of access are those that are necessary to ensure the security of the state or to protect its relations with other states or international organizations, those that concern the state's central financial, mone-

17. SOU 1972:47, Data och integritet, at 49-50.

18. *See generally* ADMINISTRATIVE SECRECY IN DEVELOPED COUNTRIES, *supra* note 1.

19. SOU 1980:31, Offentlighet och sekretess, at 115.

tary or currency policy, those that involve activities to prevent or suppress crime, and those that protect personal or economic information of an individual. The list contains seven categories of protected interests.

The detailed secrecy rules are set forth in the Secrecy Act of 1980 which became effective on January 1, 1981. The previous Secrecy Act was signed into law in 1937. The Secrecy Act is a complex piece of legislation. Each chapter deals with a particular group of protected interests corresponding to one of the categories in section 2:2 of the FPA. Some of the provisions of the Secrecy Act refer to more detailed regulation in special statutes. Furthermore, the Government may issue prescriptions concerning the application of particular provisions.[20] Generally, the rules on secrecy in the Secrecy Act should be viewed as exceptions from the main principle of public access. Consequently, they should be applied restrictively so that an official document may not be kept secret unless there is an express provision to that effect.

Public authorities require "peace and quiet" to perform their work; therefore, release of preparatory documents and drafts can be premature and can interfere with the planning of work. The need here is for "secrecy of internal matters." Interests of this kind can be protected by not permitting access to documents that are regarded as unfinished or incomplete. They may, of course, be released if an authority considers openness motivated and well-advised. This area constitutes a gray zone in which disputes often occur and in which the authorities may interpret and apply the rules on the right of access in a favorable manner from the point of view of the information seekers. Under Swedish law part of the problem concerns the dividing line between the area where the right of access is guaranteed and the area where information services are provided by the authorities only to the extent that it is expedient.

Surprisingly, although the right of access to official documents is well established in the Swedish legal system, relatively little is known about its practical value and application. It is often accepted as a fact that access through representatives is more important than access obtained by individuals on their own behalf. The most important representatives are the mass media, and, therefore, it is not uncommon for journalists to look through the incoming mail of ministers and other authorities. Private persons can hardly go to such trouble since the right of access places heavy burdens on those seeking information. For instance, private individuals must take an active interest in public affairs, they must have the time to spend in

20. Sekretessförordning (1980:657).

acquiring this information, and they must know how to approach public authorities and how to identify documents and records that are of interest.

Conversely, the right of access also involves demands on the holders of information. The officials who handle matters regarding access must be familiar with the relevant rules and their application. They must also accept the purposes of the legislation on the right of access and do their best to fulfill them. In this respect deficiencies are evident. Individual officials are not always as familiar with the legislation as would be desirable. It is not uncommon for public authorities to exaggerate the need for secrecy and to shield their activities from outside inspection and curiosity. Sometimes care is taken not to include sensitive information in official documents: matters can be kept unfinished, oral communication can be relied upon, messages can be regarded as "private," and so forth. The benefits of a principle of public access to official documents are not always apparent—they must be explained and defended each day. Appeals to the administrative courts and complaints to the Parliamentary Ombudsmen involving withholding of official documents are quite frequent.[21] It is a matter of choice of perspective whether one should regard this as a sign of health or a sign of malady.

The Working Party for EDP and Law of the Stockholm Faculty of Law has recently completed a study of the particular problems with the application to automatic data processing of the rules on the right of access. The study was carried out by Mats Hedberg and has so far only been documented in Swedish.[22] Hedberg's investigation was performed as a case study involving surprise visits to various public authorities who were asked to provide information from their computerized files and databases. The questions had been prepared in advance so that authorities would know what to expect and in order to determine beforehand the data that could and should actually be supplied. The study indicated that computerization may inhibit openness. Perhaps the best conclusion is that the risks, which have long since been associated with lack of knowledge about the legislation and self-defensive reactions of authorities, tend to increase when ordinary documents are replaced by or complemented with new data media and automated procedures.

Unfortunately, not all responsible officials seem to have sufficient knowledge about the scope, contents, and structure of the EDP

21. *See generally* cases and decisions cited in H. STRÖMBERG, HANDLINGSOFFENTLIGHET OCH SEKRETESS. (Lund: Studentlitteratur 1980).

22. M. HEDBERG, *supra* note 15.

systems that are being used by the public authorities in question. More precisely, many do not know how data are structured and how they can be accessed. Traditionally, the Office of the Registrar has played an important role in handling documents and deciding on their availability.[23] The expansion of this role or function to cover computerized activities does not seem to have taken place without disturbances. There is considerable uncertainty in regard to the consequences of providing access to computerized data, such as, risks of violations of secrecy requirements, possible interference with day-to-day work, and undesired effects on the future of an open access policy because of additional costs. The combined effect of these uncertainties is a negative attitude towards the person seeking information. It may also be noted that as a rule computer systems have been built up without any concern for the needs or consequences of the right of access.

Computerization seems to involve certain risks that the right of access could be eroded, but it may also be viewed as an instrument which can be used to strengthen and further develop the principle of openness. The risks associated with EDP may be considered to be of a temporary nature and the best way of dealing with them is through conscious efforts to use the computer itself to provide easier and broader access to public information. Such ideas are beginning to gain ground in the Swedish discussion. The question is whether it is possible to proceed from the passive right of access guaranteed by existing rules to active information services that may involve participation of the citizens in the design and operation of particularly important information systems.[24]

III. THE PARTICULAR PROBLEMS OF ACCESS TO COMPUTERIZED DATA

Many difficulties arise when legislation concerning the right of access is applied in a computer context. Problems concerning definitions and construction of existing statutory provisions exist. In computer systems, data are stored and processed in a different way from the way in which it was handled in a manual environment. It is possible that the most difficult issues are associated with this introduction of new kinds of information structures and new ways of utilizing data.

In theory, solutions to problems of definitions and construction of statutes may always be found. Rules may be changed and ad-

23. *Cf.* B. WENNERGREN, HANDLÄGGNING 42, 44 (Stockholm: Liber Förlag 1978).

24. P. SEIPEL, ADB OCH JURIDIK. EN PROBLEMOVERSIKT. Rapport till Datasamordningskommittén, Ds Fi 1975:3, at 258-79.

justed to suit a new technology. Practical experience, however, should guide the choice and evaluation of proposed solutions. This leads to something of a dilemma, for it may be evident that existing rules are less than adequate, and serious problems may result from rapid introduction of new computer applications such as teledoc systems in public administration. Nevertheless, it may be necessary to allow such systems to be used in order to gain experience and learn more about their legal consequences. This may be part of the explanation why the original license to operate the teledoc system of the FOA was of a provisional character.

The report of the Publicity Committee in 1966 contains an interesting and succinct statement of the particular problems of the right of access in computer systems.[25] Machine-readable data are generally less permanent than data stored on paper. The particular risk is that data may be erased or changed, even though the data should have been preserved in order to make the right of access meaningful. Secondly, according to the Committee, data in computer systems are not as easy to scan and understand as data contained in ordinary documents. Thirdly, requests for information that do not coincide with the uses that the authorities themselves make of the data may be costly and the delays considerable, if the information can be supplied at all. These concerns of the Publicity Committee in 1966 are still of interest today and their practical importance has certainly grown.

The Committee on Publicity and Secrecy devoted much of its attention to the protection of personal privacy in the computer framework. Its first report, entitled "Data and Integrity"[26] set forth a suggestion for a data protection law that later became the Data Act of 1973. The concern for privacy protection also put its mark on the Committee's proposals in the area of rights of access to official documents. The Committee considered the threatened invasion of privacy posed by the computer so serious that it wished to restrict access to all kinds of computer files. Actually, the Committee's proposal meant that the right of access to computer recordings would be more restricted than the right of access to ordinary documents. The Committee formulated a basic "principle of equal access" so that the information-seeking public and the authorities, the data holders, would have equal access to data in computer systems. The principle, however, was interpreted in a way that was favorable to the information holders. A person seeking information only had a right of access corresponding to that which an authority already

25. SOU 1966:60, Offentlighet och sekretess, at 113-14.

26. SOU 1972:47, Data och integritet.

had. Furthermore, the right of access only extended to data gathered by the authority to meet the needs of that authority.[27] In the Committee's final report, the limit to the right of access was defined by the legal right of the authorities to use data:

> OSK [i.e., the Committee] proposes that any authority possessing computerized information should be legally bound to make it available only if that authority is allowed to use the information for official purposes and naturally provided, also, that it should not be kept secret. The way to bring about this has been to set up a rule stating that any EDP-recording should be regarded as an official document in the care of a specific authority only if the authority itself is allowed to transfer the information to documentary form. Instructions given to an authority may limit, not the technical access to information but the legal access. OSK feels that the authority should be put in such a position that it cannot be forced to hand out information on demand which the authority according to its instruction may not use in its activities.[28]

Thus, according to the Committee, in order to decide whether data may be withheld, both the practical possibility of transforming machine-readable data into documentary form and the legal right of an authority to withhold the information must be examined. This suggested version of a principle of equal access was criticized for leaving too much room for discretionary decisions by the authorities as to when data should be transferred and for deviating from the traditional rules on the right of access to ordinary documents. The Ministry of Justice, in preparing the Government Bill, found that the committee had gone too far in its ambition to protect personal data from being used without control.[29] The bill, which has now become the law, suggested a solution that interprets the principle of equal access in a way that is more favorable to the public.

To summarize, there are at least four circumstances associated with computer systems that complicate attempts to adjust the traditional rules on the right of access.

(1) Knowledge of existing problems and the effects of various rules is still incomplete.
(2) New applications of EDP (teledoc systems, for instance) give rise to new problems.
(3) Integration of different applications of EDP leads to more complex situations and increased demands for sophisticated legal rules.

---

27. *Id.* at 66-67.
28. SOU 1975:22, Lag om allmänna handlingar, at 26.
29. Government Bill 1975/76:160, at 85-88.

(4) Computer processing of data causes new problems with regard to the safeguarding of secrecy.

IV. A CLOSER LOOK AT THE RIGHT OF ACCESS UNDER THE FPA

A. Traditional Documents

The concept of a document plays a central role in Chapter 2 of the Freedom of the Press Act. The term covers written presentations of various kinds as well as such items as maps, drawings, and pictures.

The principle of publicity applies to all documents that are official. An official document is any document that is kept by a state or municipal authority and that has been either received or drawn up by the authority. Thus, the one basic requirement is that the document is in the keeping of an authority, and an additional condition is that the document has been either received or drawn up.

The criterion of "being kept" is satisfied if a document is physically in the possession of an authority. It does not matter whether the document has temporarily been taken away by one of the officials. According to the main principle, a document is considered to have been received when it has reached an authority (i.e., arrived at the premises) or when it has been handed over to a competent official (even if this takes place in a private home, for instance).

The rules on the concept of drawn up are more complicated, and the FPA distinguishes between different categories of documents. Documents are considered to be drawn up when they have been dispatched, or when measures have been taken to make them known to an external party. Documents that are not dispatched but that are for internal purposes only, are considered to be drawn up when the matter concerned has been finally settled by the authority. If such documents do not relate to any particular matter, then they are considered to be drawn up when they have been revised and approved by the authority.

Special rules apply to certain types of documents. Thus, indexes of matters, journals, files, or other lists that are maintained continuously are considered to be drawn up when they are ready for entry or posting. This means that indexes and files of this sort can be accessed as soon as they exist as a concept and are prepared to receive entries; it is not necessary that they contain any.

As was mentioned above, there is a need to exempt drafts, internal notes, tentative working papers and the like. Memoranda, i.e., notes that have been put together solely to present a matter or to prepare it for decision and that have not been dispatched, do not be-

come official documents in the hands of the authority that prepared them unless they are filed together with the other documents of the matter for the purpose of being kept. Notes that contain factual information that is relevant to a matter (e.g., notes on a discussion with the parties to a case), however, should be filed and kept.[30] Drafts of decisions of an authority, drafts of writings from an authority, and comparable draft documents that have not been dispatched are not regarded as official documents unless they are filed and kept for the future. Drafts of this kind may or may not be related to a particular matter. There are a number of other special provisions for certain types of documents. Some of them pertain to machine-readable media and will be discussed in a subsequent part of the survey.

Official documents are, according to the main rule, public in nature, and therefore, should be freely accessible to all Swedish nationals.[31] Exempted documents are listed in the Secrecy Act of 1980, in related statutes, and in prescriptions of the Government. The Secrecy Act regulates both the release of documents and the obligations of officials not to divulge secret information. It regulates relationships between the public and the authorities as well as relationships among the authorities themselves. The Secrecy Act often sets time limits that define the maximum period that a certain type of document may be kept secret. Earlier release is possible if there is no risk of damage or abuse. A person concerned may also suspend secrecy that is in his or her exclusive interest. The main principle is that no document should be kept secret unless its release could, on careful consideration, cause a specific damage.[32]

After receiving a request for access, an authority must examine whether the document at issue is official and whether it is public or secret. In principle, the authority has no right to investigate either the identity (including the nationality) of the information seeker or the reasons for the request. It may, however, be necessary for the authority to obtain such information in order to be able to evaluate the risk of abuse or damage according to a specific provision in the Secrecy Act. In practice, those who seek information often ask for more than the handing out of a particular document; they often require assistance in identifying the documents that are of interest to them. Issues such as how much support and aid they should receive and how precise requests for information and documents must be

30. *See generally* B. WENNERGREN, *supra* note 23, at 89; H. STRÖMBERG, *supra* note 21, at 11-12.

31. For all practical purposes, they should also be accessible to foreigners. *See* section 14:5 of the Freedom of the Press Act.

32. SOU 1975:22, Lag om allmänna handlingar, at 27.

are not regulated in Chapter 2 of the FPA. It is firmly established, however, that the principle of public access does not include a right to require that the authorities carry out investigations and researches.[33] This means at least three things:

(1) Requested documents must be sufficiently identified. The condition is, of course, met if the requester knows the formal identification of a case or matter (a docket number, for instance). Other means of identification can also be accepted.

(2) The authorities are not under any unconditional obligation to collect information from documents in order to illuminate a certain matter or activity.

(3) The authorities are, however, under an obligation to search out documents that have been identified by the requester although the search may involve time-consuming and costly work.

Clearly, there is room for uncertainty, and the above principles can be construed differently and in ways that are more or less in the spirit of the principle of public access. It should be mentioned once more that general information services of the public authorities are not included in the right of access; the Secrecy Act states that the authorities should inform the public about the contents of documents to the extent that such services do not interfere with their normal work. Similar provisions about information which should be provided to the public may be found in the General Ordinance for the State Authorities of 1965[34] and in the Decree on Service to the Public of 1972.[35]

Two particular matters of significance for the principle of public access should be mentioned in this context. One concerns the extent to which the activities of the authorities are substantiated in documents. The other concerns the registration of official documents. Obligations to document activities and decisions are now regulated in a haphazard fashion. Provisions can be found in statutes such as the Public Administration Act of 1971[36] and in the detailed instructions for the authorities. The regulation of documentation is not part of the legislation on rights of access; however, it is presently being reviewed by a legislative committee.[37] To the extent that documents are created and kept, they constitute archive materials and cannot be destroyed without the support of

33. *See, e.g.*, cases cited in *infra* notes 56-57 and the accompanying text.

34. SFS 1965:600.

35. SFS 1972:406.

36. SFS 1971:290 (*e.g.*, § 16).

37. Förvaltningsrättsutredningen, Ju 1978:09.

decrees issued by the Government which regulates the weeding out of documents.

Registration of documents is now regulated by the Secrecy Act of 1980. Registration is not a prerequisite for the official nature of a document; however, it is of considerable practical value for the information seekers. If a document is not registered in a journal or index, then it may not be possible to know of its existence. The present position is that official documents must be registered unless it is evident that they are of small concern for the work of the authority. For official documents that are *not* to be kept secret it is possible to let arrangement of the documents replace registration so that problems will not arise as to what documents have been received or drawn up. Registration is considered particularly important for secret documents. The registers are, of course, open. They should contain information such as the date when the document was received or drawn up, the document number or some other identification, the party who has sent in or received the document, and a summary statement of the subject matter of the document. Information belonging to the two last-mentioned categories may be excluded if it is necessary in order to keep the register open to the public without risk of violations of secrecy requirements.

Secret registers may be maintained for certain documents whose very existence must be kept secret. Such registers are extremely rare, however, since in most cases basic information can be provided about the existence of secret documents. Notices may be put on documents stating their secret nature and the applicable provision on secrecy. The effect is only a caution (a "warning signal") for a document bearing a notice may nevertheless be found to be available to the public. The secrecy of a document does not depend upon the existence of a notice of secrecy.

Upon request, a document must be made available on the premises immediately or as soon as possible for inspection and copying. There is no charge for such access; however, the requester must pay a stipulated fee if he chooses to have a copy made (usually a few crowns per page). Access cannot be denied to documents that are only partly secret. If the document containing secret parts cannot be made available in such a manner that the secret parts are not revealed, then the authority must provide a free-of-charge copy that contains only the open parts. To eliminate risks of damage or abuse that constitute grounds for secrecy, an authority may condition the handing out of documents upon restrictions or conditions that make it a criminal offense to reveal or use the document and the information contained in it in certain ways. Otherwise it is not permitted to impose such restrictions or conditions.

Decisions to withhold documents or to make their release dependent upon restrictions and conditions can be appealed. Normally, appeals are made to the administrative courts of second instance and to the Supreme Administrative Court. It is explicitly stated in the Freedom of the Press Act that proceedings should be expedited. There are no restrictions on the right to appeal a case to the court of highest instance; however, decisions to make documents available cannot be appealed. If a private party suffers harm through the release of an official document, then the remedy consists of making a complaint that the document was released unlawfully to the Parliamentary Ombudsmen or to the Chancellor of Justice.

B. Computerized Data

The nature of machine-readable data has raised the issue of whether computer media can be considered documents. During the 1960's, the Supreme Administrative Court decided two cases involving the scope of the Secrecy Act of 1937 with regard to magnetic tapes for computers.[38] Data stored on such tapes were considered secret according to certain provisions in the act. It could be argued that both decisions implied that the document concept should be construed broadly so as to cover machine-readable data. Neither case, however, was based on such reasoning, and the Secrecy Act of 1937 referred to both "documents" and "facts." The issue was explicitly discussed only by the minority in the case decided in 1965. The two chief justices concluded that technological developments led to the usage of various types of recordings, such as punched plates and cards, rolls for machines that record speech, and other types of mechanical and electronic recordings which replace traditional written documents. According to the minority, the term "document" refers to written documents. The term must not, however, be construed narrowly. Instead, the term "document" should also be understood to cover new forms of storing "information materials," including magnetic tapes for computers.

In a case decided by the Supreme Administrative Court in 1971,[39] the issue of whether magnetic tapes may be regarded as documents came to the fore. The case concerned a population file maintained by a county and did not involve the possible application of the Secrecy Act. A private firm had requested that a copy be made of the file but the County Administration Board refused to grant the request. The Board argued that magnetic tapes could not

38. RÅ 1965 ref 25; RÅ 1969 ref 11.
39. RÅ 1971 ref 15.

be considered to be documents and consequently could not be available under the principle of public access. Magnetic tapes, the Board stated, should be regarded merely as a means to produce documents which then may be official and available to the public. The Supreme Administrative Court followed the reasoning of the minority in the 1965 case and found that the word "document" need not be construed narrowly but may cover all kinds of methods and media that are used to record and keep information. The Court pointed out in particular that if the problem were not solved in this way, the usage of new data storage media would considerably limit the right of access guaranteed by the Swedish Constitution. The County Administration Board then consented to making a copy of the tape available. In doing so the Board apparently assumed that the right of access includes a right to obtain copies of data in machine-readable form. The Supreme Administrative Court had been silent about the manner in which requests for access should be met, and the question of whether machine-readable copies must be distributed has remained uncertain despite the 1971 decision.

The Swedish case serves as an interesting comparison with a similar case from the United States involving the application of the Freedom of Information Act of 1966 (FOIA). In 1979, the U.S. Court of Appeals for the Ninth Circuit held that the FOIA applies equally to computer tapes and written public records.[40] Neither the Swedish nor the American decision is surprising, however, since the right of access would soon be rendered meaningless if data stored on computer media were generally exempted. On the other hand, the inclusion of machine-readable data is only the first obstacle to be resolved, and many problems pertaining to existing differences between automated and manual methods of organizing and processing data still remain.

The first problem is determining how to incorporate computers and computer-readable media into the existing rules on the right of access. Three alternatives have been discussed in Sweden:

(1) Computer media might be subsumed under the document concept. In this case, identical rules would be applied to all categories of storage media.

(2) Computers and computer media might be regulated separately and by special rules. Such regulations would be identical to those applying to ordinary documents but would take into account the particular characteristics and problems of automated data processing.

40. Long v. Internal Revenue Serv., 596 F.2d 362 (9th Cir. 1979) *cert. denied*, 446 U.S. 917 (1980).

(3) Computer media might be considered to be "documents." Regulations applicable to ordinary written media would have to be amended so that the term "document" would apply to both media.

These alternatives have been considered in connection with the 1974 and 1978 revisions of Chapter 2 of the FPA. The discussion is still not complete since the committee presently engaged in revising the public access rules, the Data Legislation Committee, recently suggested special legislation to deal with the right of access to recordings for automatic data processing. The proposal of the Data Legislation Committee will be discussed below.

The Committee on Publicity and Secrecy proposed that recordings for automatic data processing be regulated separately. In its 1972 report, the Committee introduced the concept "official recordings for automatic data processing" to complement the traditional concept "official documents."[41] In so doing, the Committee chose a different solution from its predecessor, the Publicity Committee, which had suggested in 1966 that the rules applying to ordinary documents be extended without any amendment to cover computer-readable media.[42] The Committee on Publicity and Secrecy criticized this approach claiming that it would leave a number of problems of construction and application without clear solutions. For example, it would be difficult to determine when computer-readable data would be official and what form such data should take for distribution.

The Ministry of Justice did not follow the strategy suggested by the Committee on Publicity and Secrecy in its continued effort to revise the Freedom of the Press Act. Instead, preference was given to alternative three described above. As a result, identical *basic rules* now apply to traditional documents and computer media, and computer media are by definition "documents." Section 2:3 of the FPA states that "a document is a presentation in writing or in picture form or a recording which can be read, listened to or in any other way perceived only by technical means." The basic rules for all kinds of documents have therefore been tailored to include computer media. Special rules to determine when recordings for automatic data processing should be considered to be "in the keeping" of an authority and when such recordings can be said to have been "received" have also been promulgated.

The concept of "keeping" requires more than mere physical presence. For instance, an authority should not be able to refuse access on the ground that data that it uses via its terminals are stored

41. SOU 1972:47, Data och integritet, at 15 & 72-74.
42. SOU 1966:6, Offentlighet och sekretess, at 12 & 130.

in the computer of another authority or of a private service bureau. A criterion that fulfills the same functions as physical presence in a simple sense must be formulated. The FPA has accomplished this by stating that a recording is considered to be in the keeping of an authority if the recording is available to the authority for transformation into such a form that it may be read or otherwise perceived. For instance, a recording (computer-readable data) is considered to be kept by an authority if it can be accessed via a computer network and read on a terminal or if the authority can use the computer of another authority to transform the recording into a print-out. Although the second method may result in a delay, this is of no principal significance.[43]

The Committee on Publicity and Secrecy suggested a somewhat more narrow definition of the concept of "in the keeping of." In its 1975 report the committee placed emphasis on the legal right of an authority to transfer information into documentary form. The regulation presently in force is more generous toward the public in that it emphasizes "factual access." This means that, to the extent that there exists a practical possibility of transforming machine-readable data into ordinary readable form, the public cannot be denied access on the ground that there exist laws, prescriptions, instructions, agreements, or other similar restrictions that prevent the authority itself from accessing certain recordings. Thus, in order to limit the right of access of the public, it is necessary to technically prevent the authority itself from transforming particular data into readable form. This may be accomplished through access control in on-line systems, through withholding of computer programs, or by various other means. In the case of computerized files containing personal data, however, the public has no right of access to recordings that are unavailable to the authority itself because of certain legal restrictions. This exception makes it possible for the Data Inspection Board to impose effective restrictions on the usage of personal data with respect to the right of public access.[44]

Recordings can be received by an authority in a manner similar to the way that ordinary documents are received. For example, someone may give a magnetic tape to an official. Transmission in computer networks, however, may be more involved, and in those situations the rule for traditional documents is inappropriate.[45] According to section 2:6, paragraph one of the FPA, a recording for EDP is considered to have been received by an authority when an-

43. Government Bill 1975/76:160, at 89.

44. *Id.* at 88 & 122.

45. *Id.* at 136-37.

other party has made the recording available to the authority so that it can be converted into a readable form. Thus, the concepts of "keep" and "receive" are both based upon the practical possibility of producing a version of data that can be read or otherwise perceived.

Situations may occur when an authority allows an unauthorized person to process or store data that are then made available to the authority. For instance, the unauthorized person may be ordered to convert texts into machine-readable data that are made available to the authority that ordered the conversion. In situations like this it would be inappropriate to consider the recording to have been "received" by the authority. Consequently, section 2:6, paragraph three, of the FPA states that technical processing or technical storage of a document that has been supplied by an authority does not classify the document as "received" by the authority. Note that the provision covers documents in general and not just EDP recordings.[46]

Special rules for recordings have been deemed unnecessary to incorporate the concept of draw up. The rules that apply to ordinary documents apply equally well to recordings.

The rules that have been examined so far are the main rules for EDP recordings. A closer look at some complementing details that may be found in special rules for recordings as well as in general rules will be helpful.

Section 2:4 of the FPA deals with letters and similar personal messages. These are considered to be official documents if they deal with matters or issues that are the concern of an authority and are not intended for the addressee in another capacity than as an employee of the authority. Thus, a message to a person in his capacity as a trade union representative and not as a public servant does not become an official document even if it concerns an issue that is handled by the authority. This exception to the rule for personal messages is of significance in the context of teledoc systems.

It was noted in Section IV.A. above that a special rule to decide when "indexes of matters, journals, and such files or other lists which are maintained continuously" should be considered to be drawn up and consequently be official and accessible to the public. A drawn up file usually occurs when "continuous" indexes and files have been prepared for entry or posting. This rule covers more than dockets and similar journals. In fact, use of the term "file" makes the rule applicable to all kinds of EDP applications that involve ordered collections of machine-readable data. Before the 1978 revision

46. *Id.* at 137.

of the FPA the scope of the term "file" was uncertain.[47] The present text of the provision and the accompanying clarifications in the preparatory legislative reports provide the following information.[48] According to the explanatory part of the Government Bill, the provision applies to files which are continuously being updated and which have an undetermined lifetime. The provision does not apply to files that are created to solve a specific task that is limited in time and that has a short lifespan. Files of this latter type follow the rules for recordings in general and are therefore treated differently from files subject to the special rules. The general rules are discussed below.

1. The main rules in section 2:7, paragraph one, of the FPA are applicable. For example, a recording, including a computer file, will be considered to be drawn up when it has been dispatched, when the subject matter has been settled, or when the recording has been approved or otherwise made ready by the authority.

2. EDP recordings containing certain kinds of information will be subject to special rules. While the relevance of these rules is still somewhat uncertain, they are mentioned for completeness.

a. Recordings that contain judgments or other decisions, according to the relevant legislation, must be pronounced or dispatched. In addition, if the recordings contain minutes or other information relating to such decisions, then they are considered to be drawn up when the decision has been pronounced or dispatched.

b. Recordings may also contain minutes or similar records kept by an authority. With certain exceptions such recordings are considered to be drawn up when the minutes have been approved or otherwise made ready by the authority.

3. Recordings that have been prepared exclusively to present a matter or to prepare it for decision and that have not been dispatched become official documents in the hands of the authority that prepared them only if they are filed and kept for future use. They become official documents when their subject matter has been settled. Section 2:9, paragraph one, of the FPA states that recordings can be treated as memoranda. In addition, the explanatory section of the Government Bill states that items such as research papers and indexes to collections of facts and collections of statistical source data may be treated as memoranda. To the extent that factual information is added to a matter, a recording cannot be considered to be a memorandum.

---

47. P. SEIPEL, *supra* note 24, at 222-41.

48. Government Bill 1975/76:160, at 92-93, 143-44, 168-69.

4. EDP recordings that constitute drafts of the decisions of an authority, drafts of writings of an authority, or comparable documents and that have not been dispatched are not considered to be official documents unless they are filed and kept for future use. Unfinished manuscripts are included in this category. The Government Bill explicitly mentions EDP recordings which constitute intermediary products without independent interest.

Section 2:10 of the FPA contains a special rule for situations in which documents are handled outside of an authority. The provision covers documents in general but is of particular importance for EDP recordings. It states that documents that are being kept by an authority on behalf of another party (a public authority or a private firm) merely for technical processing or technical storage shall not be considered to be official in the hands of the authority that processes or stores the documents.[49]

Section 2:11, subparagraph one, of the FPA states that letters, telegrams, and other documents of a similar nature which have been delivered to or drawn up by an authority exclusively for the communication of messages shall not be considered to be official documents. This provision has been included in the FPA to protect ordinary letters and telegrams as well as notes and print-outs which are made by the Post and Telecommunications authorities in connection with the forwarding of letters and telegrams. The provision complements section 2:10 of the FPA which does not have an equally broad coverage with respect to recordings and other documents created in connection with transmissions. The phrase "other documents of a similar nature" broadens the scope of the Act. Copies and extracts of messages that are not protected under section 2:10 may therefore be protected under section 2:11 of the FPA.[50]

EDP recordings that are official documents can be exempted from the right of access in the same manner as ordinary documents. This exemption is a result of specific provisions in the Secrecy Act of 1980. In principle, the Secrecy Act does not distinguish between ordinary documents and EDP recordings. There are a few exceptions, however, such as Chapter 7, section 16, which concern computerized files containing personal data. On the other hand, the secrecy problems that occur in the framework of computer systems are not identical to the problems in manual data processing systems. Special attention must be paid to the possibilities of linking, selecting, and retrieving data, to the need for access controls in online systems, and perhaps most importantly, to the problem of as-

49. *Id.* at 171.
50. *Cf. id.* at 172-73.

sessing in advance which usages of data are sensitive and should therefore be viewed as breaches of secrecy according to the Secrecy Act. In particular, it should be recalled that the Secrecy Act is based mainly on the principle that no document may be kept secret unless its publicity could, on careful consideration, cause specific damage.[51] This test becomes particularly difficult when requests are made for data in computer systems and, generally, when secrecy problems of computer systems are evaluated. These difficulties will be illustrated by the subsequent discussion of the concept of a "recording."

In a request for data from computer systems, it is generally accepted that an authority may decide the manner in which a recording is made available on the premises of the authority. The main requirement is that the recording can be inspected, copied or otherwise studied.[52] This means that an authority can choose between providing information in the form of a printed listing and providing information on a computer terminal display. The requirement that data be made available immediately, or as soon as possible, however, may be interpreted to mean that an authority cannot delay the fulfilling of a request by offering a print-out when data can be read immediately and more conveniently on a CRT terminal. This conclusion is uncertain, but it finds support in section 2:12, paragraph two of the FPA. Under that section, an authority may refer the requester to another authority in the vicinity provided that the latter authority can make the recording available without significant inconvenience for the requester. In regard to requests for copies of recordings, section 2:13 of the FPA states that an authority is under no obligation to distribute copies of EDP recordings in forms other than print-outs. In other words, the right of access does not mean that data can be obtained in machine-readable form. The reason for this restriction is that the availability of machine-readable data increases the risk of invasion of privacy.[53]

It is of no significance whether or not the authority that keeps the data uses a computer of its own. The required computer processing must, in principle, be carried out even if "external" equipment must be used. The information seeker, however, may have to accept delays and the request may even be denied if there are considerable obstacles such as high costs. In this situation the requester may remove the obstacle by contributing to the costs or

51. *Cf.* SOU 1975:22, Lag om allmänna handlingar, at 27.

52. *Cf.* SOU 1980:31, Offentlighetsprincipen och ADB, at 78; Government Bill 1973:33, at 82.

53. Government Bill 1975/76:160, at 181.

by arranging computer time.[54]

Matters are even more complicated for software facilities. Interest is focused on the obligation of an authority to write or to adjust computer programs, or, more generally, to assist the requester in obtaining certain data.

In 1974, the Supreme Administrative Court decided a case in which a person seeking information from the computer files of a County asked that certain data be selected from a magnetic tape.[55] The court found that the right of access depends upon whether the requester's instructions for the selection of data requires the authority to perform significantly more work than that required for the printing of the data. Since programs that "covered" the requested selection existed, the court concluded that no extra work was necessary and that the data that had been requested should be sorted out and printed. A closer look at the decision reveals that the two issues to be considered are what work in terms of programming and related activities can be demanded, and what selections, mergings, and so forth of data can be requested.

A decision rendered by the Supreme Administrative Court in 1976[56] sheds light on both issues. The case involved a situation in which standard programs were available but these programs had to be used with particular control cards in order to produce the required print-out of recordings. The court found that the authority, the Central Bureau of Statistics, was under an obligation to produce the control cards and to complement the programs. This would be equivalent to the work required to locate and sort out traditional documents. In addition, the court stated that an authority must perform the extra programming necessary to exclude secret parts from a print-out. Since this authority had to use different programs for different files in order to produce print-outs, however, it had no obligation under the FPA to bring the data concerning each individual into one list.

In the following year, the Supreme Administrative Court decided another case which concerned the printing out of a particular selection of addresses from the total population file, the RTB file, of the Central Bureau of Statistics.[57] The court concluded that the principle of public access gives a right to request a selection of data from one file (the RTB file) that refers to persons in two other specialized files. In particular, the court found that the extra work

54. Government Bill 1973:33, at 81; Government Bill 1975/76:160, at 89.

55. RRK 1974, R74 2:26.

56. RRK 1976, R76 2:70.

57. RÅ 1977, Ab-310.

was made necessary because data was stored in different files by the authority. The right of public access could not be set aside because the authority had chosen, for practical reasons, to store basic data in a separate file.

Viewed together, the three decisions rendered by the Supreme Administrative Court illustrate the difficulties of dealing with EDP recordings. They reflect basic problems that concern the ways in which data can be organized and used with the aid of computers. The issues have been dealt with on various occasions by the Swedish lawmakers during the 1970's. A closer look shall be taken at relevant parts of the explanatory report of the Government Bill which led to the latest revision of Chapter 2 of the FPA.[58]

An understanding of the concept of a "recording" is fundamental. This concept should not refer to a separate data storage medium, such as a magnetic tape or disc, nor should it refer to an isolated data element, such as a number. It is necessary, in order to define the concepts, to take into consideration the purpose of the right of access, which is to enable inspection of information that is controlled by an authority. From this point of view, it is of subordinate interest whether the requested data constitute a selection from a large collection of data, a merger of data from several files, or a result of some other type of processing. Thus, according to the Government Bill, each set of data that "factually belongs together," or that together provides meaningful information, should be considered to be a separate "recording." It may even be stated that any set of data that may be requested constitutes a recording. An authority is not, according to the main rule, entitled to inquire into the purpose of a request or the context in which the requested data are to be used. The situation thus is quite different from the one involving traditional documents in that traditional documents contain "packages" or "chunks" of data that are relatively easy to distinguish, the existence of which does not depend upon subjective choices and technical facilities for processing data. In the computer systems of the authorities no such "stable packages" exist. The question then is which packages of data should an authority be under an obligation to put together for presentation and not which "data packages" does an authority have that can be requested.

The question of whether or not a recording can be requested is quite similar to the question of which obligations are placed on the authorities with respect to the processing and retrieval of data that are "in their keeping." It must be remembered that the basic principle is that both the information seekers and the authorities should

58. Government Bill 1975/76:160, at 89-91.

have equal access to information. A request need not be granted if it refers to data that are not considered to be available to the authority itself. How, then, should "availability" be understood?

"Theoretical" availability would mean that any set of data that an authority, in theory at least, can obtain from its computer systems should be available to the public under the FPA. Availability, however, is defined in a more narrow, practical sense since a certain selection or merging of data is considered to be available to an authority if, and only if, the data set can be produced by routine measures. If more complicated work must be performed to meet a request for data, the writing of a new computer program, for instance, then these data are not considered to be available to the authority. Whether the measures that have to be performed are termed "programming" is not decisive. It may be that writing a program or adjusting an existing program can be considered to be a routine measure. Moreover, the person seeking information may himself make a required program available, in which case the authority must arrange for the program to be run if it is merely routine. Just as in the case of arranging hardware resources, the requester may have to accept a delay and may have to contribute to the costs in order to overcome "significant obstacles" to obtain a requested recording. In summary, the key concept is "routine measures." This still leaves room for a certain amount of discretion as to which requests are covered by the right of access under the FPA.

There are at least two advantages associated with the solution which has now been described. First, there is no immediate need to decide whether a request involves a need for "programming." This is significant since the word "programming" is not very precise. The spectrum of activities ranges from the detailed step-by-step description of procedures to be carried out by a computer to the providing of parameter values to a report generator. Shaping a query in an on-line information retrieval system using Boolean operators and full text searching may be more difficult than introducing minor changes into an existing computer program. Consequently, it seems well-advised not to give the terms "program" and "programming" any central role. The second advantage is that a solution based on the notion of "routine measures" is flexible with respect to future developments. The Government Bill of 1975-76 points out that continued advances in the areas of hardware, software, and data-bases will broaden the right of access to the information resources of the authorities. Hardware and software developments may tend to change the principle of equal access to give increased weight to the theoretical availability of sets of data.

The application of the Secrecy Act to EDP recordings requires

that the question of exemptions be answered for each recording, or for each set of data that is requested. Sometimes a whole file may be exempted, as is the case with certain files of the police authorities, or data that are being used in certain activity may be protected generally and unconditionally.[59] In many situations, however, it will be more difficult to decide in advance the consequences of the Secrecy Act for the right of access to EDP recordings. For example, this may occur if a person wishes to inspect the data-bases of an authority from one of its terminals.

In 1979, the Supreme Administrative Court denied a person's request to use a terminal to inspect, without supervision, the automated docket of the Administrative Court of Appeals in Jönköping.[60] The appellate court had granted a right to inspect the file with the aid of a court official. The refusal was motivated by security reasons since the two computer terminals of the court could be used to read as well as to register data, thus making it possible for someone who used the terminal to change or erase data. The court considered it a difficult or impossible task to check afterwards for tampering. Citing the Committee on Publicity and Secrecy, the court emphasized that computer processing performed by parties other than the authorities themselves must often involve risks that data are destroyed or changed. In addition, the court emphasized the expense and interference with the court's ordinary work if it were to let the public use its terminals. Since the two terminals were not protected against unauthorized input the judgment offers only limited guidance. The opinion does not touch upon a possible duty to protect against tampering with data, nor does it mention the possibility of permitting access via other terminals that do not allow more than reading of data. In the case involving the teledoc system KOM 79 these issues have been treated in greater detail.

V. THE TELEDOC SYSTEM OF THE FOA

A teledoc system is used for the communication of messages in the form of text between users of computer terminals. It permits activities that are similar to both exchange of letters and telephone calls between two persons. Moreover, the system can support "conferences" involving a large number of participants who do not have to be present at their terminals at the same time. The computer administers the contributions and commentaries of the users. A teledoc system may also be used for work on reports and similar products on which a number of individuals cooperate to complete a

59. Secrecy Act, § 8:8, ¶ 1.
60. RÅ 1979 2:34.

text. It can be used for referenda and similar polls, for the posing of questions to a broad circle of persons, for advertising, and for notifications.[61] Teledoc systems may be usefully combined with other computer applications such as text editing, information retrieval, and planning and statistics.

The teledoc system of FOA is a so-called database system. It allows communication between hundreds of users at locations across the country. Even very simple terminals may be used, such as "typewriters" with a built-in acoustic system that can be attached to ordinary telephones. From a technical point of view, the system is advanced and a joint European research project on data networks, the so-called COST-11 project, has recently engaged a Swedish firm for further development. The specifications of the system have been worked out by the FOA, which obtained the first license to operate the system from the Data Inspection Board. Without going into details, a few words may be said about the application of the Swedish Data Act of 1973 to the KOM system.

When the FOA first applied for a license in 1978, the Data Inspection Board turned the application down. Perhaps the most crucial reason was that the Board considered the description of the usage to be so vague that it was impossible to issue any prescriptions for the system. These prescriptions are given for each "file of personal data" and concern such things as the purpose of the system (the file), its contents, its uses, and security measures. The Board also referred to various problems caused by the proposed system in regard to working conditions and the right of access to official documents.

The FOA renewed its application and provided more precise information about the intended system. A license was granted in March 1979. It may be noted, however, that one of the members of the Board, the representative of the federation of the white-collar workers (TCO), expressed his reservations. The Board granted a provisional license which terminated on March 30, 1981. A new license for an indefinite period was granted after certain changes in the system, which is now called KOM 81 or, simply, KOM, were made. The text file of the system is no longer regarded as a "file of personal data" under the Data Act.

The FOA is the "responsible keeper" of the system (the file) which may be used by employees of the FOA and by the personnel of other public authorities, organizations, and private companies that are involved in various projects with the FOA. Both KOM 79

61. *See* the FOA reports cited in *supra* note 9. *See also* decisions of the Data Inspection Board March 21, 1979 (DN 114-79) and March 10, 1981 (DN 4203-80).

and its successor KOM 81 consist of a number of files. Certain changes were made in the older structure which permitted retrieval of recordings on the basis of the text contained in individual messages. The present files are described below.

1. The User File provides information regarding all the users of the system. In addition to such data as each user's name and password, the file contains references to index files for all activities in which each user participates and all letters to and from a user. For each reference to an index file, the user file registers whether that user is allowed to read and write or only to read. The user file can also automatically transmit to a particular computer all or some messages to a particular person.

2. The Activity File contains information regarding all activities in the system. This information consists of sets of messages that are exchanged among users who form a particular group. The file states the purpose and the organizer of each activity, as well as the procedure for becoming a participant in the activity. Some activities, in which it is not possible to write messages directly, are reserved for messages that are obtained from other activities. These then function as collections of particularly interesting or important messages from other activities.

3. The Index File consists of one subfile for each activity and contains references to the messages of each activity. Each reference states the message's author, addressee, location in the computer, time of validity, connection to other messages, and various other data. For messages that have been received from other teledoc systems, the source and the time of transfer are registered. The index file also contains references to the keyword file.

4. The Key Word File lists key words or similar brief descriptions of the messages that are stored in the system. Data concerning individuals may not be used as key words.

5. The Text File has one subfile for each activity and each user. It contains the actual texts of the messages belonging to a certain activity and of the letters to and from a certain user. Texts are only stored and copied as units, and it is not possible to retrieve information from them. Thus, texts can only be retrieved from the text file with the aid of references from the index file, the key word file, and the activity file. In KOM 79 it was possible to retrieve information directly from the text of messages. This meant that in KOM 79 the text file had to be specially protected and that the FOA was under an obligation to let persons know whether the text file contained any information about them.

6. The Statistics File is a support file for charging fees and for statistical analyses of the uses of the system.

Each computer file containing personal data should, according to the Data Act, have a preestablished purpose that has been accepted by the Data Inspection Board. A teledoc system such as KOM 79/81 constitutes one file according to the terminology of the Data Act. The original license covered the following purposes: (1) collection and dissemination of information within the framework of the FOA's activities; (2) preparation of matters that are normally handled by the FOA; (3) contacts within and between the personnel organizations of the FOA; and (4) evaluation of the functioning of the system.[62] The purposes of KOM 81 have been described in somewhat broader terms but the practical differences are probably small.

The KOM system is protected by various security measures. There were a number of restrictions regarding access to information about persons in the text file of KOM 79. These restrictions followed the first decision of the Data Inspection Board, which held that the text file came under the Data Act. The restrictions meant that messages could only contain information that related to the activity of the FOA. Therefore, certain sensitive facts listed in section 4 of the Data Act, such as the fact that someone has committed a crime, were unconditionally banned. Evaluative statements were only permitted in messages written by the person concerned or in messages that concerned activities in which the person concerned had a right to read as well as to write. There were certain exceptions with regard to promotion and other personnel matters. The systematic collection of data about one or more persons was not allowed, unless the data was supplied by persons participating in a poll. Collecting the names of persons who were members of a board, a project group or similar unit, or who were the authors of writings belonging to a certain subject area that was of interest for a particular activity was also permitted.

To prevent unauthorized retrieval of personal data in KOM 79 and to allow persons to know what had been written about them

62. According to its application, the FOA wished to carry out "research" concerning the usage of the system. The Board apparently considered this activity too broad and changed it to "evaluation." This change in language, among other things, indicates that the Board in 1979 had a very hesitant attitude toward teledoc systems. The 1981 decision marks a clear change in this respect. Thus, the purpose of the file is now described simply as "files of personal data which are required in connection with a system for computer-assisted communication of text." The new policy has met some opposition and the representative of the white collar workers union (TCO) has once more registered a complaint.

under section 10 of the Data Act, special rules had to be promulgated to properly identify persons in messages. Given names or initials were required to be stated. A user was only allowed to retrieve information from messages that he was allowed to read, messages either written by the person himself or addressed to the person or included in activities in which the person had a right to read. The elimination of the capability to retrieve information directly from the text file has made things considerably easier but there are still a number of restrictions on the methods of retrieving and reading messages. In both the new and the old system, user access is controlled through personal passwords. Furthermore, the texts of messages are stored in enciphered form so that even the people who perform system maintenance and who are responsible for its overall evaluation will not be able to understand.

The author of a message may set a time limit for its validity. Likewise, the organizer of an activity may decide that all messages included in the activity are only to be kept for a certain time. There is a general obligation for the employees to see to it that all factual information that is significant for the preparation of a matter is printed out and kept for the future. The system has a special "archive instruction" to facilitate the fulfillment of this obligation. It is also possible to decide in advance that all messages belonging to an activity are to be printed out and kept.

According to the FOA's directives for the usage of the system there are four different types of "tele-meetings."[63]

1. A "tele-meeting" is a meeting in which all users of the system may enter as participants, i.e., an open meeting;

2. A "limited tele-meeting" is an activity in which only a particular group of persons may enter as participants;

3. A "closed tele-meeting" is an activity in which only a limited circle of persons participate; and

4. A "protected tele-meeting" is an activity in which the names of the participants are known only to the participants.

KOM handles about 6,000 messages per month. Half of these messages are letters that are read by only one person. The normal length of a message is between ten and twenty lines, but there are also messages that are considerably longer. Users are usually active at the terminal twice a day and it is common to have ten users connected to the system at the same time. There are approximately 220 persons who use the system at least once per week and approximately 400 persons who use the system at least once every month.

63. These directives refer to KOM 79 and were issued in June 1979 (No. 10:4).

VI. COURT RULINGS ON ACCESS TO DATA IN KOM 79[64]

The KOM system supports many kinds of FOA activities, such as research and investigations, discussions, person-to-person communication, and preparation of decisions and decision-making. Outside parties are also involved since the permit allows users outside the FOA to be linked to the system. The activities are more or less open and KOM is used at different stages of work on various matters.

In November 1979, three persons asked for access to data relating to the acquisition of a new computer by the Stockholm Computer Center for Higher Education and Research (QZ). This center services the FOA as well as a number of other institutions. The request caused some confusion at the authority, a reaction that is probably typical as demonstrated by the inquiry by Mats Hedberg mentioned earlier. The request was denied on the ground that data in the system must be regarded as "memoranda" which are not official documents according to the exemption rule in section 2:9, paragraph one of the FPA.

The requesters appealed the issue to the Administrative Court of Appeals in Stockholm and extended their request to include the right to study the conversations and communications involving the purchase of the computer, the right to gain access to the entire KOM 79 system, and the right to use a terminal to inspect the system without supervision by officials of the authority.

The FOA further clarified the grounds for its refusal in a writing to the court. The authority emphasized that the FPA recognizes the need to protect information at the early stages of preparation of various matters. Teledoc systems may contain materials of many kinds, including materials that can be considered to be official documents. The authority called attention to personal data that may not be accessed by the authority itself because of the restrictions imposed by the Data Inspection Board and to messages related to the activities of the organizations of FOA personnel. Neither of these two categories of data could be regarded as official documents. As for the two tele-meetings at issue, the FOA concluded that there was no specific matter involved and that the two meetings only concerned the FOA's activities in general. Even if the two meetings were regarded as concerning specific matters, however, the data contained in them did not constitute official documents. The data were regarded as memoranda that had neither been dispatched nor taken care of to be kept for the future. Since, according to the FOA,

64. *See supra* notes 12-13 and cases cited therein.

no formal matter was involved, the issue was simply how to label the meetings. The FOA determined that the meetings ought to be looked upon as "a symposium." The messages were to be regarded as memoranda, recordings of interventions, and notes taken by someone recording the symposium. From the point of view of the authority, recordings made during a meeting should be looked upon as a basis for possible future minutes. From the point of view of the participants, the recordings should be considered personal working documents. Thus, recordings could only become official documents if they were finalized or in some other way made ready by the authority pursuant to section 2:7, subparagraph three, of the Freedom of the Press Act.

The FOA also argued that the system did not contain any "public" meetings since only particular users were allowed to participate. Most of the meetings were related to matters that had not been concluded, such as research projects which had not yet resulted in reports, and which, consequently, had not generated any official documents. On the other hand, the FOA emphasized that the rules on making print-outs would guarantee the right of access to recordings that constitute official documents. The conclusion of the FOA was that the applicants could not be given access to the entire system, nor could they be given access to certain meetings. Thus, there could be no talk about using terminals to inspect the system.

The requesters objected that the FOA's manner of labeling activities could not change the fact that the communication of texts was involved. The criterion of the recordings "being kept" was fulfilled since they were available to the FOA in a readable form. The crucial issue, which the applicants claimed the FOA had avoided discussing, is that the case involved a situation in which messages were being exchanged between several public authorities. It was also the FOA's duty to design the system so that inspection could be allowed without risks of violation of secrecy requirements. The FOA's neglect to do so could not be used as a legitimate argument to refuse usage of terminals by the public without control or supervision. There was no risk of unauthorized input or changes of data since the system afforded adequate protection.

The Administrative Court of Appeals consulted the Data Inspection Board which issued the following statement:

> It must be taken for granted that KOM 79 is being used by the FOA in accordance with the license obtained from the Board and only for the permitted purpose. Consequently, data in the system must concern the activities of the FOA and be available to at least one of the officials of the FOA in readable form. An exclusion could be made for the activities of the organizations of the personnel:

messages in such activities ought to be exempted according to section 2:4 of the FPA which deals with private letters. For other messages the following rules ought to apply:

(1) All messages that are made available in the system by parties outside the FOA must be considered to have been received by the FOA according to section 2:6 of the FPA. Such messages are therefore to be regarded as official documents which must be handed out upon request.

(2) In regard to messages that are created by officials of the authority, official documents may result in two ways:

(a) There may be messages which, via a terminal or some other means, are available to authorities and to private persons outside the FOA. These messages are official documents since they have been dispatched according to section 2:7, paragraph one of the FPA;

(b) Other messages are available only within the authority itself.

(i) If such messages are related to a particular matter, they should be regarded as official documents when the subject matter has been finally settled.

(ii) If such messages are not related to any particular matter, they should be regarded as official documents when they have been approved or otherwise made ready, or as soon as they have been entered into the system. Internal messages of this kind thus become official documents as soon as they are written into the system.

The reasoning of the Data Inspection Board as it concerns messages that are "drawn up" by the authority does not seem to leave any room for exemptions of the kind mentioned by the FPA, such as memoranda and drafts.

The Administrative Court of Appeals found that an authority is free to decide how recordings are to be made available to the public. An authority is under no obligation to allow information seekers to handle terminals by themselves. Such a limitation on the principle of public access serves to eliminate risks that texts in the database are changed and that data is made available in violation of secrecy requirements. The court found the remaining arguments of the Data Inspection Board persuasive but the judgment is worded differently. Thus, the court concludes that, unless specific provisions on secrecy apply, recordings that have been entered into KOM 79 by external parties, authorities and private parties, should be considered to be publicly available. Messages that are created by the FOA and that are available to external parties should also be considered to be available to the public; however, a recording that is connected with a matter handled by the FOA is not publicly accessible until the recording has been dispatched or when the subject matter has

been finally settled. Messages concerning the activities of personnel organizations are not official documents.

The decision of the Administrative Court of Appeals is not clear. It appears to confuse the different rules relating to the concept of "draw up" in the second chapter of the FPA. In addition the reasoning of the Administrative Court of Appeals is not as clear as that of the Data Inspection Board. The court, for instance, says nothing about messages that are created within the FOA and that are *not* made available to external parties. Should not such materials be made available to the requesters? The court may have taken notice of the way in which the requesters characterized the data involved: all data were said to have crossed boundaries between authorities. This description is incorrect. What about messages that are connected with matters handled by the FOA? Does not the fact that such messages are made available in the system to external parties mean that they have been dispatched ipso facto? Is something more required? What?

The case was appealed to the Supreme Administrative Court with respect to the right to use a terminal. The appellants argued that such a right cannot be lawfully denied and that the principle of public access would be seriously distorted if such a right were not granted. The appellants claimed that it is possible to construct computer systems with access controls and other security measures and to install special "presentation terminals" for the general public. Deficiencies in this respect should not be permitted to limit the principle of public access. The new technology does not mean anything qualitatively regarding the right to gain access to documents in archives. There is, it was argued, no difference in access between having a text available on paper and having it on a CRT screen to the right of public access. In the case of conventional documents, there is no requirement that an official be present and turn the pages. The public may handle the documents themselves. The same principle must apply to EDP recordings in order to avoid negative effects. The right of public access may be weakened. A requester will have no possibility of not revealing the nature of the requested information. The personnel of the authorities will not have time to assist the public in using terminals, especially in the future when practically all information will be stored in computer systems.

The Supreme Administrative Court decided this case in September, 1980. A database, the court stated, contains many kinds of recordings. It should therefore be looked upon as a collection of information similar to an archive containing ordinary documents. The right of public access does not mean that information seekers can

visit archives, look for certain unspecified documents, and bring them out of the archives. It is necessary to identify documents in advance and this principle should also apply to databases. In particular, for each request it must be ascertained whether particular provisions in the Secrecy Act prevent access. The court concluded that the FPA does not give a right to use a terminal to search out facts in a database. The requester must ask for specific recordings and only those recordings should be made available after examination of their information contents.

VII. A PROPOSED STATUTE ON THE RIGHT OF ACCESS TO EDP RECORDINGS

In the autumn of 1980, the Data Legislation Committee (DLC) released a report entitled "The Principle of Publicity and ADP."[65] The report discusses the regulation presently in force and proposes a new statute on the right of access to recordings for automatic data processing. Another section of the report deals with active dissemination of information, or the need to supplement the right of public access with information services of the public authorities. The subsequent discussion will deal with the proposal and, in particular, its implications for teledoc systems.

A. The Nature of the Proposed Statute

The DLC proposal is not intended to be constitutional law. The Committee considers the procedure required to change such law too slow and prefers a supplemental law at a lower level which can more easily be adapted to changes in technology and to new requirements and possibilities.[66] This legislative method is not without its risks and may violate principles set out in constitutional law. The Committee is, of course, aware of these problems and has attempted to solve them by careful formulation of certain sensitive provisions.

The purpose of the DLC proposal is to illuminate and clarify the rules of access to EDP recordings for both the authorities and the general public.[67] To achieve this goal, the statute contains numerous references to laws and decrees that concern EDP recordings. Thus, references are made not only to provisions in the Freedom of the Press Act and the Secrecy Act, but also to other statutes such as the General Ordinance on Archives (1961:590) and the Data Act (1973:289). In this respect, the DLC proposal contains nothing new

65. SOU 1980:31, Offentlighetsprincipen och ADB.
66. *Id.* at 18 & 44-46.
67. *Id.* at 19.

but merely brings together and directs attention to legislation which should or may be applied to the EDP systems of the public authorities. The proposed statute also contains a number of provisions that aim at clarifying the current interpretation of the rules on the right of access. It is particularly this effort which may be contrary to the principle that lower level legislation should be in conformity with the constitution or, more precisely, the rules in the FPA that guarantee the right of access to official documents. The Committee has not been completely successful in avoiding the pitfalls. Certain interpretations of the FPA are questionable and several uncertain provisions in the DLC proposal may be harmful to the right of access.

The DLC proposal deals only with EDP recordings, although many of the rules could just as easily apply to documents in general and provide valuable guidance. For this reason the Committee has discussed the possibility of broadening the statute in the future to include ordinary documents as well as recordings.[68] The legislative strategy to regulate EDP systems separately can be questioned, but it is apparent that EDP systems require particular attention because of their present uncertainty. From this point of view, the DLC proposal seems both useful and reasonable.

B. Basic Principles

Section 3 of the DLC proposal cites two related basic principles that are to guide practices in computer systems in the public sector. According to the first principle, the right of access to recordings stated in the FPA and in the DLC proposal should be taken into consideration when computer systems are designed, changed, and used. This means that authorization schemes and access controls ought to be devoted such special care as the principle of public access motivates.[69] For example, it should be possible to routinely exclude secret information when recordings are made available. It should also be possible to allow information seekers to use terminals for retrieval without supervision.

The second principle expressed in section 3 of the DLC proposal states that recordings should be available to the public to the same extent that they are available to the authority. This availability refers to "practical availability" and is based upon the possibility of accessing information through "routine measures." On closer scrutiny one finds that the scope and intended impact of the suggested principle are uncertain. It would require extended and costly efforts to restructure all existing EDP systems of the public authorities in

68. *Id.* at 54.
69. *Id.* at 41, 53, 78 & 85.

order to create a situation in which all requests can be met without delays and fees. From this point of view, then, the principle of equality may look disturbing to many public authorities. On the other hand, the principle explicitly refers to obstacles posed by the Secrecy Act. This may prove to be a weak spot since for many EDP systems it can easily be claimed that it is not possible to foresee the secrecy problems and structure the systems accordingly. Such difficulties could be used as excuses not to take any measures at all to implement the principle of equal access.

C. Registration and Documentation

Section 4 of the DLC deals with the registration of recordings that have been received or drawn up by an authority. It contains nothing but a reference to the relevant provisions in the Secrecy Act. To a certain extent this means that insufficient attention is devoted to many complicated problems associated with the registration of EDP recordings. Registration of conventional documents and of recordings in EDP systems pose quite different problems and, as will be discussed shortly, the committee has found it necessary to complement the existing rules for registration with special rules on the documentation of EDP systems used by the public authorities.

There are a number of reasons why registration of EDP recordings requires special attention. Data bases and telecommunications have radically changed the ways in which information is recorded and made available. The implications for the three key concepts in the Freedom of the Press Act, that recordings are "in the keeping of an authority," that recordings have been "received," and that recordings have been "drawn up" by an authority have already been discussed. The unavoidable vagueness of the concept of a "recording" should also be recalled, as well as the equally vague nature of the concept of a "matter." Briefly, when is an activity of a public authority to be classified as a "matter" and how should activities be structured in terms of one or more "matters?"[70] The criteria are vague and may permit an authority to decide rather arbitrarily how its activities should be divided into matters. The use of computer databases probably increases the uncertainty and may lead to negative effects for the right of access.

In the KOM 79 case, the Data Inspection Board and the Administrative Court of Appeals were faced with difficulties in attempting to structure and define teledoc systems in terms of the rules on the right of access. The appellate court opinion is based on schematic reasoning, and the question may be asked whether more flexible so-

70. Government Bill 1975/76:160, at 97.

lutions should be sought and whether such solutions can fit within the present rules of the FPA. The arguments set forth by the FOA in its writing to the court indicate the nature of the problems: Can teledoc systems contain recordings that must be viewed as memoranda and drafts? Are there "meetings" in the system that can be said to be "closed" to the general public? Can communication through a teledoc system be viewed as a "symposium" in which the participants take notes and in which data may be regarded as a basis for possible future minutes to be drawn up by the organizing authority? These issues shall be investigated although some of them go beyond the issue of registration of recordings.

A recording should be considered to be in the keeping of an authority when it is available for transformation by "routine measures" into a form that can be read or otherwise perceived. It is not necessary, however, that the recording has actually been accessed and used by the authority. The Data Inspection Board points out in its writing to the court concerning the KOM 79 system that it is sufficient that the recording is available to at least one of the officials of an authority. The physical location of the data base, as well as its public or private nature, are of no significance. One of the consequences of these rules appears to be that, in principle at least, the public can claim access to recordings in a data base run by a private organization in another country to the extent that a Swedish public authority has access to the database. At the present stage it is difficult to foresee the various problems associated with the extension of the right of access in data networks.

A recording emanating from the outside can hardly be considered to be in the keeping of an authority before it has been received. Someone outside the authority must have created a recording (a message or a file) and taken steps so that it can be routinely converted into readable form by the "receiving" authority, or by at least one of the officials of the receiving authority. On the other hand, it does not mean that the receiving authority must actually know that the recording has been made available, nor does it mean that the recording must actually have been read by someone at the receiving authority. Even a "dormant" recording is an official document if routine measures can make it deliver its information.

According to the registration provision in section 15:1 of the Secrecy Act, official documents, including recordings, should be registered without delay after they have been received or drawn up. In a computer system, registration by manual means would be awkward and would result in various types and combinations of computerized index files. Such files must, according to section 15:2 of the Secrecy Act, provide such information as the date when the recording was

received, its index number or other form of identification, the sender, the addressee, and its main contents. The last item is particularly essential for the effectiveness of the right of access; keywords, classification systems, references, and so forth should be designed to make it easy for the public to find relevant materials. Such aids should also take into account the interests of various branches of the social sciences including history and law. Today's indexing systems are weak in this respect and are only intended to serve the immediate needs of the authorities themselves. It remains to be seen whether section 3 of the DLC proposal can lead to any improvements, such as the requirement that EDP systems be designed with due concern for the principle of public access.

To a certain extent, it is easy to decide what constitutes a recording and how a recording ought to be registered. An example of that is a "letter" in a teledoc system intended for an individual official. As things become more complex, computer systems provide excellent means of registration. An illustration of this is an intervention in a "conference" and the various messages associated with it in the form of corrections, commentaries, and additions. In this respect the new technology offers many advantages over manual registration and serves to strengthen the right of access. Difficulties arise since, in principle, any meaningful combination of data constitutes a recording.

It appears necessary to distinguish between "basic" recordings and "generated" recordings, although it should be emphasized that the dividing line between the two categories is not clear. The registration requirements in the Secrecy Act concern the basic recordings category. A text message from the outside that is made available in a teledoc conference in which a public authority participates would belong in that category. The second category consists of all possible combinations on data that may be requested according to the rules on the right of access and that are official documents according to the terminology of the law. One cannot realistically require that all such "generated" recordings be "registered." Their nature and number change constantly, and it is difficult to say when each recording has been received or drawn up. Consequently, in dealing with computer systems and data bases, attention will be focused on data structures and retrieval possibilities rather than on recordings as such. The Secrecy Act permits registration to be replaced by "arranging documents" so that it can easily be established whether a document/recording has been received or drawn up. It is therefore possible to design data bases without thinking in the narrow categories of conventional "registration." Conversely, the requirement imposes obligations on the authorities with respect to the

retrieval and classification facilities of their computer systems. The DLC proposal does not deal with these difficulties in detail, but it does contain a new requirement that "search keys" be documented, as will be discussed below. It should be noted that the Secrecy Act makes an exception for documents/recordings that are to be kept secret. These recordings must always be registered as soon as they have been received or drawn up unless the Government decides otherwise. This registration requirement, therefore, will be particularly difficult to apply to "generated" recordings because advance knowledge about all combinations of data that may be requested and their possible threats to various secrecy requirements is not always available.

A discussion of the general problem of the point of time when recordings should be considered to have been drawn up should begin with the reasoning of the Data Inspection Board and the Administrative Court of Appeals in the KOM 79 case. According to this reasoning, messages are considered to be dispatched and thereby drawn up as soon as they have been made available to external users of the teledoc system. Messages that are not made available to external users are considered to be drawn up when the related matter has been concluded or, if they are not related to any matter, when the messages have been stored in the teledoc system.

A schematic solution of this sort should not be heavily relied upon. Teledoc systems may be used for many different purposes and at different stages of work on a particular task.[71] They may serve both as a "scratch pad" for preliminary notes and as a means of communicating completed texts expressing decisions, reports, and opinions. Schematic legal reasoning is likely to prevent the full use of the potentials of teledoc systems, an undesirable effect from the point of view of the right of access. Moreover, public authorities that use teledoc systems may define "matters" so as to avoid access to recordings. The statutory language indicates that it should be possible to treat EDP systems in a flexible way which leaves room for exemptions involving recordings of an "intermediary" nature.[72]

It may be questioned whether it is necessary to create completely new rules for teledoc systems which take into account their special character as a novel means of communication. The FOA's suggestion that some messages be treated as contributions to a "symposium" may serve to illustrate this approach. Although novel

71. The FOA emphasizes this aspect by detailed language in its application for a prolonged license. *See* decision of the Data Inspection Board March 10, 1981, DN 4203-80, at 19.

72. *Cf.* Government Bill 1975/76:160, at 91-92.

concepts may be needed, however, the following comments will be restricted to those relevant special rules in the FPA that are now in force.

According to the Data Act, the teledoc system of the FOA constitutes a single file even though the system consists of a number of files, such as the user file and the activity file. Some of these files contain subfiles. Moreover, the text of a particular message may sometimes be treated as a specific file. The file concept is hierarchical and subjective. The physical organization of data need not be decisive since different logical structures may all rely on the same physical storage organization. This description of data structures has many legal implications, the most important of which is that there is a need for better structured legal views on databases. It is important to determine the legal purposes of concepts such as "file," "recording," and "information from recordings" in the context of the right of access.

To understand the implications of this determination, consider section 2:7, subparagraph one, of the FPA. It states that "indexes of matters, journals, as well as files or other lists which are maintained continuously," should be considered to be drawn up when they have been prepared for entry or posting. The file concept of this provision should cover only certain types of files in a database: (1) files that provide user-oriented search aids and guide the information seeker to decisions, matters, parties, and activities, and (2) files that store information concerning objects of a particular type and that require regular updating to enable a specific kind of activity associated with these objects to take place. These activities may include supervision, inspection, investigation, regulation, and caretaking. Thus, section 2:7, subparagraph one, of the FPA may apply to certain files in a database, such as the KOM system, but not to the database as a whole. The files in KOM that come within this provision are the index file, the activity file, the user file, and the key word file.

Recordings that have been prepared exclusively to present a matter or that have been prepared for decision become official when they are dispatched. Storage in a teledoc system through which external parties may gain access to the recording should, as the Data Inspection Board points out, be viewed as dispatching. It should not be necessary that an external party has actually read the recording. The fact that it is possible to read it should suffice. The effect of storage in the teledoc system on "memoranda recordings," which are only available internally within an authority, is also a crucial issue. Is storage to be regarded as placing a recording in an archive to be kept for the future? Only if such storage takes place will the "memorandum recording" be regarded as an official document. The

question has no simple answer. The important point is that the effects of storage in the system are made clear in advance. A system may have one sub-file that is used as an archive and another sub-file that is used for provisional storage of memoranda which may or may not be placed in the archive file. The provisional file should be viewed as a desk drawer in which recordings may be kept for temporary use. Such personal storage by individual officials is not presently regarded as equivalent to placing in an archive.[73]

Drafts and other intermediary recordings with or without connection to a matter are dealt with in section 2:9, paragraph two, of the FPA. Again, storage that makes recordings available to external parties must be viewed as dispatching. An exception exists, however, where an authority allows an external party to study drafts for the purpose of providing advice without the recording being considered dispatched. Thus, consultations and similar activities can take place in a teledoc system, and the recordings may still be regarded as internal working documents.[74]

"Draft recordings," which can only be accessed internally within the authority, should not be considered to be stored merely by placing them in an archive. The solution in this case should be the same as for "memoranda recordings." The Data Inspection Board concludes that storage in a teledoc system means that a recording has been made ready. This principle is too general. The deciding factors must be the nature and contents of the recording. The fact that a teledoc system is used for storage and communication is not conclusive.

The Data Act presently contains a rule that simplifies the decision as to whether or not recordings are official documents. Thus, if a recording is used for deciding a matter or if it influences the handling of a matter, then the recording should be printed out and added to the documents that constitute the file of this matter, in accordance with section 13 of the Data Act. This rule is closely related to section 2:9, paragraph one, of the FPA which states that documents/recordings cannot be excluded from the right of access as "memoranda" to the extent that they add factual information to a matter. The Data Legislation Committee has included this provision as section 5 of their proposal.[75]

The registration of recordings is associated with the need for rules concerning the documentation of automatic data processing

73. *Id.* at 168.

74. *Id.* at 170.

75. *Cf.* SOU 1972:47, Data och integritet, at 90; SOU 1980:31, Offentlighetsprincipen och ADB, at 48.

systems. Section 6 of the DLC proposal suggests that public authorities that use EDP maintain a catalogue of the uses that should be available to the public together with a copy of the proposed statute. The catalogue should provide information regarding the purposes of the various uses and the names of existing files and systems. Public authorities that are responsible for the operation and maintenance of EDP systems should, in addition, prepare system documentation providing more detailed information on the types and sources of data, the users of data, the concepts used for retrieval of data, the rules that apply to the keeping and erasure of data, the particular measures that have been taken to ensure the right of access, and the relevant secrecy provisions. This enumeration has been subject to criticism in that the Data Legislation Committee has overlooked the fact that EDP systems to which public authorities have access via on-line communication may be operated by private organizations. For such systems the DLC proposal contains no requirement that system documentation be prepared and made available by the authorities that use the systems.

D. Archives

Section 8 of the DLC proposal deals with archives and erasure of recordings. It contains references to various laws and decrees and, in addition, suggests that special consideration be devoted to the purpose of the usage of EDP, the right of access, the rule of law, and scientific information needs. This section contains no new provisions, and the explanatory report of the committee does not delve into the many problems of maintaining machine-readable data for the future, an area that is presently quite uncertain. The volume of machine-readable materials is rapidly growing since more and more activities of the public authorities rely on the use of computers. The National Swedish Records Office has only recently begun to experience and investigate these problems. Presently the authority stores approximately 1,000 magnetic tapes, and its main problem seems to be an inability to obtain explanatory documentation of sufficiently high quality. The Central Bureau of Statistics, which stores about 10,000 magnetic tapes, is experiencing similar difficulties.

Experts in the field say that there is a need for a new theory of storing computer-readable materials for the future. One of the questions under Swedish law concerns the extent to which the right of access ought to apply to historic materials; today there is no time limit. As for teledoc systems, the questions concern not only the possible storing of individual messages, but also the future interest

in statistical and similar information concerning the use of the systems.

E. Anonymity

The Data Legislation Committee describes the right to anonymity as "one of the most important elements of the right of access."[76] The right to anonymity consists of both a right to not be compelled to reveal one's identity and a right to not reveal the purpose of a request for information. The latter right may, in fact, be the most important one. The right to anonymity is not explicitly stated in the FPA and only recently has it been included in lower level legislation. Section 9 of the DLC proposal expresses this principle by stating that there should be a right to anonymity in so far as it is unnecessary for an authority to learn the identity and the purpose of a requester in order to decide whether secrecy must be maintained. The proposal also requires that security measures be designed in order to preserve anonymity.

F. Information Services

The Data Legislation Committee considers it particularly important that persons who request information in computer systems obtain guidance and advice from the authorities. Section 10, paragraph one of the DLC proposal concerns "information from a recording" and refers to a provision in the Secrecy Act that prescribes that public authorities provide information from official documents so long as this does not require secrecy or interfere with the ordinary work of the authorities. This obligation is clearer in the context of ordinary documents than in the context of recordings. The problem, again, is that a recording is not a set of data that is delimited and determined at one time. Consequently, it is not always easy to decide what constitutes "information from a recording" and what constitutes a recording in its own right. The concept of "information from a recording," however, is meaningful at least with regard to information that is derived intellectually from recordings.

The second paragraph of section 10 requires the authorities to assist the public in exercising the right of access. The committee considers such assistance particularly important when the information is retrieved from computer systems.

G. Access on the Premises of an Authority

Sections 11 through 14 of the DLC proposal describe the manner

76. SOU 1980:31, Offentlighetsprincipen och ADB, at 72.

in which recordings should be made available on the premises of an authority. An authority may choose how to make a recording available. The primary alternatives are an already existing printed list, a specially made print-out, or text on a CRT terminal. This freedom to decide the manner of presentation is not without problems. An authority may delay the release of a recording by choosing a particular way of presentation. Moreover, some forms of presentation are easier to understand than others. The Data Legislation Committee, however, has not investigated such issues.

Section 14 deals with the right to use the computer terminals of the authorities. The Committee assumes that the right of access does not include a right to use a terminal. This assumption is consistent with decisions of the Government and of the Supreme Administrative Court.[77] It reflects the current interpretation of the FPA, but it may be challenged for a number of reasons. The latest Government Bill revising the rules on the right of access states that an information seeker has a right to retrieve recordings with his own program if such retrieval can be accomplished routinely and without violating any of the provisions in the Secrecy Act.[78] It may be argued, then, that an information seeker has a right to retrieve information by formulating queries at a computer terminal. Moreover, the right of access unquestionably allows a requester to look through a docket, journal, or similar collection of information. Thus, at least those files in a data base which are similar to traditional materials that are open to browsing should, in principle, be available for inspection and retrieval from terminals.

The Data Legislation Committee has adhered to the predominant interpretation of the FPA. The suggested right to use a terminal in the DLC proposal is intended to be a complementary right, one not guaranteed by the constitution. The right is also subject to conditions. There must be no risk of changing or destroying data, and ordinary work must not be interfered with. Provisions in the Secrecy Act can also bar the public from using terminals. In practice, the value of the right to use computer terminals will depend on how public EDP systems are designed and the willingness of the authorities to abide by the principle of adapting EDP systems to the right of access (section 3 of the DLC proposal). Ideally, databases should be organized and computer facilities made available so that interested parties can inspect large collections of data in order to find items and activities of interest.

77. Decision of the Government, April 10, 1980 (Ministry of Justice, dnr 2177-79); Judgments of the Supreme Administrative Court cited *supra* notes 14 & 60.

78. Government Bill 1975/76:160, at 91.

On-line searches open new vistas for the right of access. Among other things, a requester may discover during a search and with the aid of the computer which information is of interest. Computerized on-line searches usually permit the use of more flexible retrieval strategies, and its speed can compensate for lack of precise knowledge about the recordings that are of interest. The computer can, through "dialogue," narrow the request. There are also numerous difficulties associated with the character of data and retrieval languages, and the lack of knowledge about retrieval methods. While some of these difficulties will remain, others will disappear as computer systems improve and as the public becomes more educated in computerized means of retrieval.

H. Print-outs and Copies of Machine-Readable Data

Section 15 of the DLC proposal contains nothing new. It merely mentions the right to get a print-out of recordings at a preestablished fee which is further regulated in section 18. According to this provision, fees should be low enough to permit the exercise of the right of access. The concluding part of section 15 states that public authorities may hand out copies of machine-readable data unless the Data Act or other restrictions prevent this.

I. The Principle of Equal Access

The public should have access to recordings that are available to the authorities. Recordings that can be generated by routine measures (simple work, insignificant extra costs) are considered to be available. Section 16 states this principle in a confused way which creates uncertainty and confuses constitutional rights with less important obligations of the authorities to provide service and information.

J. Other Issues

The concluding sections 17 through 19 of the DLC proposal deal with time limits for supplying information, fees for obtaining print-outs, and appeals. Existing rules are brought together and in some respects clarified.

VIII. ACTIVE DISSEMINATION OF INFORMATION

The Data Legislation Committee devoted one chapter of their report to "active dissemination of information." The discussion concerns the possible ways to complement the right of access to official documents with information systems that serve particular needs.

EDP technology would play an important part in such information systems. Their purpose would be to serve as bases for public debate, political programs, research, educational efforts, and activities of interest organizations. Areas of interest to which the committee devotes particular attention are statistical data bases and legal data bases. It would probably be desirable to create specialized information centers that coordinate activities and develop contacts with different groups of "information consumers." Teledoc systems can probably play an important role in such activities. They offer, among other things, selective dissemination of information to particular interest groups and communication between interest groups as well as between such groups and the authorities. They can provide early information about plans, decisions, investigations, and other activities of the authorities. Teledoc systems may even constitute subsystems of teledata systems, computer utility systems with widespread participation and a broad spectrum of data and activities. This is still at least one or two decades away.

The Committee does not make specific proposals for the creation of active information systems. It discusses possibilities, aims, difficulties, and strategies, and concludes that the development of such systems should occur independently of the right of access. The discussion concludes with a proposal for a broader study in which groups such as political parties, trade unions, the mass media, the scientific and educational community, and private business should be involved.

IX. STRUCTURING TELEDOC SYSTEMS TO SUPPORT THE RIGHT OF ACCESS

A. Some Axioms

Teledoc systems will continue to grow in number. The FOA's application for an indefinite license has been granted (March 10, 1981), signaling an open door policy on the part of the Data Inspection Board. Other public authorities and, of course, private organizations will organize similar systems. Within the next five to ten years there will be a growth of teledoc networks in which many types of institutions and organs will participate. As the KOM system now demonstrates, teledoc networks will be used for such diverse purposes as administrative work, journaling of matters, decision-making, private communication of messages, preparation of decisions, and inquiries. The trend will be toward integration with other types of systems, and the teledoc facility will be increasingly viewed as one of many closely interrelated functions of data networks. From computerized terminals people will be able to solve

whole series of tasks with the aid of such interrelated functions that include, for example, the retrieval of information from libraries, the maintenance of administrative files, the use of automated controls and checklists, the filling out of forms, the editing and printing of texts, and selective dissemination of information. Thus, in the future the teledoc function will be a natural part of computer networks for legislation, jurisdiction, and public administration.

The software used for teledoc systems will probably become even more flexible and versatile than it is now. There are many dimensions for continued improvements: user friendliness, retrieval facilities, routing and linking of messages, interfaces with other functions, to name but a few.

There is little doubt that today's problems of administrative openness will change quite radically. The present mixture of manual, computer-assisted, and automated routines leave much room for a new mixture. The discussion will now turn to the consequences for the rules on the right of access. The focus will be on teledoc systems; however, many conclusions and viewpoints will concern applications of EDP in general.

B. Narrow and Broad Issues

A number of loosely interrelated detailed problems as well as general structural problems, caused by EDP and, in particular, by teledoc systems can be found to exist. There is the question of whether those who seek information should have a right to use terminals. There are questions of the meaning of concepts such as "routine measures" and "information from a recording." A final problem concerns the point in time from which to count time limits for secrecy for "generated" recordings. Problems like this are important, but there are many reasons to devote attention to broader structural issues first. A better understanding of these issues is required in order to design rules that are well-suited to teledoc systems and other applications of EDP. Existing particular problems may best be solved by a thorough revision of the present rules on the right of access.

C. Focus on the Design of Information Systems

It has traditionally been assumed that the principle of openness can be applied effectively to the procedures and routines for administration, decision-making, consulting, and handling of matters which each authority develops. In other words, it is taken for granted that relevant information is generated and preserved in the form of documents that interested parties can find. The rules on the

right of access provide only minimal guarantees that the authorities will organize their information collections and their procedures for handling information in ways which further a policy of openness. It is assumed that the self-interests of the authorities and their decisions on how paperwork should be organized are, at least, consistent with the purposes of the right of access.

Among the consequences, the following two deserve particular attention. One, facilities for requesters to survey, retrieve, combine, identify, and locate information receive little, if any, attention. A requester may decide which official documents he wishes to inspect, but the rules on the right of access provide no advice on making this decision. The right of access is presently a "passive" instrument for obtaining information. Its orientation is "ex post," not "ex ante." Requested documents should be made available—that is the core obligation of the authorities. Two, the main rule for deciding which units of information constitute official documents and their possible withholding under particular secrecy provisions, is that action is taken when requests are received. This is reflected, for example, in section 14:9 of the Secrecy Act, which states that an authority may impose restrictions or conditions to prevent damage when information is made available to a requester. Furthermore, notices of secrecy on documents are not final and binding but should be reexamined and re-evaluated each time a document is requested.

In many respects, EDP systems, computerized and computer-assisted procedures for decision-making and handling of data, are characterized by structuring in advance. The activities that rely on EDP must be understood as fully as possible in terms of information needs, information habits, information structures, types of decisions, rules of procedure, and frequency of cases. There is a shift from reliance on discretionary decisions in individual cases to analysis and description in advance of rules for decision-making. This challenges the traditional nature of the rules on the right of access. Perhaps the emphasis should be placed on the authorities' design of the information systems rather than on the concepts of "document" and "recording" in isolation. The Data Legislation Committee has partially observed this need, as is reflected, for example, in the provisions dealing with description and documentation of EDP systems. These provisions, however, do not require the authorities to develop particular types of solutions. In this respect, the requirements in the DLC proposal are vague, and their practical implications are uncertain.

If the rules on the right of access remain as they are, then a number of negative consequences will probably become increasingly apparent. To begin with, the greater flexibility of EDP systems

with regard to methods for posing questions and retrieving data will not be fully exploited to the benefit of the information seekers. Using terminals without the assistance and control of an intermediary represents a serious weakness. Efforts to increase the effectiveness of the rules on the right of access are hampered by their present orientation. Secondly, there is now a tendency to rely on paper documents and manual routines. For instance, recordings that have been used in preparing a matter should be printed out and kept in that form. This rule is probably practical, but it must remain consistent with the rules on the keeping of data in machine-readable form. Furthermore, the rules regarding journals of matters and similar lists are presently aimed at "paper-based" manual routines. Should they not be complemented and extended to exploit the power of automated data processing systems in order to organize data and keep track of measures and activities? If each authority is left to deal with the problems of access to data stored in computer systems when requests are made, access will probably often be denied simply because it would presuppose expensive improvisations.

Finally, the negative consequences of uncertainty should be mentioned. Uncertainty regarding the application of the rules on the right of access to EDP systems and regarding the nature and status of recordings in such systems will tend to conceal such knowledge from the general public. It is far easier to deny access on the ground that there are risks of, for example, violations of secrecy requirements than to try to eliminate such risks in an ad hoc fashion when requests are made. Simplified reasoning of the kind applied in the KOM 79 case (i.e., storage of a recording in a teledoc system signifies that the recording has been "made ready"), however, may discourage the authorities from using teledoc systems. Thus, a valuable tool for administrative and judicial activities may not be utilized as fully as it should be. Although they are not as practical, the desk drawer, notes on paper, and telephone calls may appear "safer."

The rules on the right of access should be oriented toward the design of EDP systems. Although precise and detailed solutions shall not be developed, the implications and issues shall be discussed.

D. Network Structure

Several issues concern the structure of computer networks with respect to participants, possibilities of access, and consequences of the sharing of information resources. One result of the growth of computer networks, public as well as private, is that the notion of

"theoretical availability of recordings" will be of greater interest. Technically, data can be accessed from the terminals of a particular authority in selections and combinations that do not interest the authority. This leads to a need for planning and investigation in advance, taking into account such problems as the safeguarding of secrecy between authorities and the "transfer" of secrecy when recordings and files are made available by one authority to another.

To what extent should the public be required to request information from the authority or the authorities that are responsible for a certain data base when a request could just as easily be addressed to another authority that has access to the same data base? How should responsibilities for the implementation of the right of access be distributed when several authorities are involved in the building up and maintenance of data bases? What is needed to design different retrieval procedures for different participants in a network from the point of view of the right of access? In this context, the concept of an "authority" may cause difficulties. More precisely, it may be uncertain whether to treat an organization as one or more separate authorities. In a teledoc network such difficulties are more likely to arise and require additional needs for structuring and planning.

Finally, when does the right of access motivate private network participants to attach terminals or to obtain access to official data bases by "dial up" procedures? The relationships between private and public sectors of future computer networks will require new ways of thinking. For one thing, authorities may be required to promise secrecy when they are allowed to access private data banks. Today such promises are exceptional, and their legal consequences are uncertain.

E. Data Structure

There is a need to plan teledoc systems and other types of EDP systems so that those who use the systems can do so for different purposes and know the effects of their actions on data elements and files. Methods should be established for giving messages the status of memoranda, drafts, messages for purposes of consultation, private messages, etc. Methods should also be established for signaling that recordings have been "made ready." Library files, which are not open to the public, should be established and labeled as such, as should files used for archive purposes. It may be valuable to establish special standards for archive files since, in practice, it has proved very difficult for the central archive authorities to handle the many different forms and types of files that are now created by various authorities.

Of particular interest are the information structures that are directly intended to aid the public in locating and retrieving information. Here it may be of value to introduce a concept of "support files," such as indexes of various kinds, logs of users and activities, files used for selective dissemination of information concerning ongoing activities (notification files) and other types of files and procedures. Vague requirements to document activities must be replaced by detailed rules that can be implemented in the form of computer programs.

The general issue also exists of which collections of data should constitute "search units," i.e., units which may be gathered from terminals by the information seekers. In manual systems it is clear, for example, that a journal of matters consisting of a cover and sheets of paper is to be considered as one single document that should be made available for inspection. As section 2:7 of the FPA indicates, there are also other types of lists, journals, and files which should be treated in the same manner. Clear rules are needed for EDP systems. A special concept of a "search unit," designed specifically for EDP systems would probably aid efficiency.

The various aspects of the design of computer systems that have now been discussed indicate a general need for standardization aimed at implementing the rules and the goals of the right of access. Efforts in this direction will probably also draw attention to the problem of different levels of openness and preparedness to serve the general public. It is more urgent for some types of systems and activities than for others to safeguard the right of access. Standards, as well as costs, will be higher in urgent cases than in cases when access is not as urgent. The choices and decisions are sensitive. Although they have existed in manual systems, they have tended not to be discussed. The task of designing EDP systems brings issues to the surface and creates opportunities for analyses of various problems which, in manual systems, have tended to be hidden. It may also be noted that the dividing line between the "classical" right of access and the area of "active dissemination of information," which the Data Legislation Committee has devoted attention to, is not at all clear. It is largely a matter of taste and policies whether particular measures are regarded within the area of the right of access or within the area of information services provided by the authorities.

F. Secrecy

A third topic to which attention should be devoted concerns secrecy requirements. These are usually expressed as combinations

of some or all of the following four elements: type of fact (information), type of matter, type of activity, and type of authority. A secrecy requirement is rarely absolute. The most common situation is a conditional secrecy in which the presumption may be either for openness or for secrecy. The test focuses upon the damage that may possibly result by divulging information. In many situations, consent of the individual concerned may authorize the handing out of information. The protection afforded by the Secrecy Act is diverse and concerns the interests of the state, the interests of private enterprises, and the interests of individuals. This last category of protected interests in particular causes difficulties with regard to the need to examine the circumstances of each individual case.

The present rules on secrecy place emphasis on the point in time when information is requested, rather than on earlier occasions such as at the creation of a document or the inclusion of a recording in a particular file. Notices of secrecy can be used but are of a provisional nature ("warning signals"). Decisions regarding withholding of documents are made when documents are requested. Secret parts of documents should be excluded and restrictive conditions may be imposed when documents are made available. It is doubtful whether there is any room at all for planning and decision-making in advance concerning the "secrecy structure" of teledoc networks.

An assessment of obligations of secrecy at the stage of EDP systems design involves obvious difficulties. The task is, however, not impossible, nor is the need for advance evaluation completely unknown at present. Quite often only a rough estimate of the risk of damage associated with the handing out of documents is possible. It is the "typical" risk which is decisive.[79] This applies both to situations in which requests for information are received and to situations in which problems of secrecy are dealt with in connection with the registration of documents.[80] Consequently, support already exists for the notion of evaluation in advance of obligations. Of course, the practice of using notices of secrecy also illustrates this point. According to a decision of the Parliamentary Ombudsmen, such notices should state not only the applicable provision in the Secrecy Act, but also the parts of the document that the obligation refers to.[81] A general principle with similar effects states that the authorities should try to avoid treating secret and nonsecret circumstances

79. *See, e.g.*, Judgments of the Supreme Administrative Court concerning the risks associated with making information about foreigners available, RRK 1974 R74 2:26; RRK 1975 R75 2:33.

80. H. STRÖMBERG, *supra* note 21, at 31-32; Government Bill 79/80:2, A, at 357.

81. JO (The Parliamentary Ombudsmen) 1971 report at 333.

in the same document.[82]

Decisions of a schematic nature regarding obligations of secrecy are practiced and, to some extent, accepted today. These practices need further development and detailing for application to teledoc systems. These difficulties are large, but not insurmountable. For many categories of data and retrieval procedures, it is possible to clarify in advance the risks from the point of view of the Secrecy Act and how these risks can be dealt with to allow the broadest possible access.

It is beyond the scope of this article to explore the detailed consequences of measures involving "secrecy design" for various types of information retrieval, text processing, and data base management systems; however, three key notions exist: secret, sensitive, and innocent (or open) information. The second and third categories together are more extensive than the first category. Sensitive information may be described as information that should potentially be kept secret and for which it is not possible to promulgate rules in advance which specify the form, context, and uses. The information may be made available without violating the rules in the Secrecy Act. The relative sizes of the second and the third categories are not fixed but are to some extent an outcome of a subjective choice. Thus, improved design tools for the improvement of teledoc systems and the ambition and preparedness to accept costs are of obvious significance. The decisions and design tasks will be of varying complexity, concerning data elements and aggregates of data. They will, of course, also concern many procedural elements, including programmed restrictions, monitoring and alert functions, and procedures for de-identification and encryption.

The three design elements which have been discussed, network structure, data structure, and secrecy requirements, form an integrated whole. The purposes of these three elements are (1) to clarify for the information holders, as well as for the information seekers, the nature of the systems from the right of access point of view; (2) to diminish the risk that lack of planning weakens the right of access as far as teledoc and other EDP systems are concerned; (3) to improve the possibilities of finding and bringing together information that is considered relevant and important by the information seekers and, in particular, to enable the information seekers themselves to use the computer as a tool for such purposes; and (4) to strengthen the right of access and open new dimensions for it with the aid of computer technology.

82. S. RYMAN & E. HOLMBERG, OFFENTLIGHETSPRINCIPEN OCH MYNDIGHETERNA 13 (Lund: H. Ohlsson 1980).

X. CONCLUSION

The preceding discussion emphasizes the need to shift attention from the application of the rules on the right of access to documents in individual cases to the design of whole information systems. Such a shift would probably benefit both manual and computerized data processing systems. Planning and structuring in advance are the key words. They mark the need for new control and enforcement mechanisms. Thus, the creation of a new function at each authority has been proposed, the "right of access supervisor."[83] One important task of these supervisors would be to assure that EDP systems are designed and used with due concern for the right of access. The supervisors would also be engaged in the organization of educational and advisory activities at the authorities. At a higher level, the responsibilities of the Data Inspection Board should be broadened, rather than restricted, to matters of protection of personal privacy. Assessment of the right of access to teledoc and other EDP systems can be viewed as one additional task of the Board.

The future of the rules on the right of access under Swedish law is uncertain. Undoubtedly, to some observers, the present rules probably seem both sufficient and satisfactory. The fact that the concepts and solutions have a long legal history does not create a favorable climate for radical restructuring. It is also uncertain whether the country is politically ready to accept the costs and troubles associated with a more active and efficient right of access.

I personally believe a revision is urgent. The proposals of the Data Legislation Committee should serve only as starting points and should not limit future proposals which may be made. The overall goal should be to create a regulation that is more detailed than the present one and that takes into consideration the characteristics of teledoc systems and other applications of EDP. I believe that this effort is necessary to maintain the principle of openness in an increasingly automated environment for administrative and judicial activities.

83. Working Party for EDP and Law (Stockholm University): Statements Concerning the Proposal of the Data Legislation Committee (ADBJ PM 1981:1).