TRANSNATIONAL DATA FLOWS AND THE SCANDINAVIAN DATA PROTECTION LEGISLATION

BY

JON BING

1. INTRODUCTION

The Scandinavian countries have a long tradition of cooperation. The similarity of the languages facilitates common cultural and economic action, and the political cooperation has encouraged business ventures of an inter-Nordic nature.

A new feature of this inter-Scandinavian activity has developed with the advent of automatic data processing. Owing to the rapid growth of teleprocessing, and the modest size of the Scandinavian societies, computer facilities are often shared between enterprises belonging to two or several Scandinavian countries. Two typical situations may be mentioned.

One is the back-up situation. A computer service bureau or an enterprise with an in-house facility makes an agreement with an enterprise having a similar facility. In the event of exceptional peak traffic, or a failure of its own computer, jobs may be piped through telecommunication lines to the other site for processing there. In this way, a higher level of computer security is achieved. Often a firm gets to know of a suitable computer in another Scandinavian country, and makes arrangements to use this for back-up purposes. It is, for instance, rather typical that a big computer service bureau in Oslo uses back-up facilities in Stockholm or Denmark.

Another situation arises where an enterprise with branches in several Scandinavian countries has a common computer system. This may be just a matter of designing an effective system, thus obviating the need to have parallel systems in all the countries. A similar situation would be a service bureau marketing its services in several Scandinavian countries through teleprocessing. This is quite common—a curious example is Norwegian State Railways, which uses a Danish system for its own ticket reservation service. The international market place of computer-bureau services is, however, larger than the Scandinavian countries, and the impact of big companies—often American-based—is being felt in the Scandinavian market also.

After the preparation of this paper in the autumn 1979, a regulatory statute concerning the Data Surveillance Service has been passed. In the text, at p. 70, it will be mentioned as a draft of September 13, 1979. In substance the statute is in conformity with the draft.

The Data Surveillance Service has later amended its English name to "Data Inspectorate". In this paper, however, the former translation is retained.

This illustrates the facts that traditionally the Scandinavian countries are heavily involved in cooperative business ventures and that these ventures are today dependent upon computer systems. Lately, Denmark, Norway and Sweden have adopted data protection[1] legislation, which regulates the use of personal data[2] in computerized and—to a certain extent—conventional form. This legislation has been designed within the framework of an international debate, and the Scandinavian countries have taken additional steps to harmonize their different Acts at the preparatory stage.[3] The result is, however, three Acts with rather different fields of application, and rather different systems of control. The norms of these Acts are then projected down onto the interwoven fabrics of the Scandinavian cultural and business life. This, of course, is bound to create problems.

This paper will discuss a few of the areas in which problems are created in this way. It will compare the clauses governing transnational data traffic in the three Acts, and it will outline some of the problems involved in the determination of jurisdiction and choice of law.

It should be appreciated that the problems within the Scandinavian area are only exponents of the problems encountered in the international field. So far, four European countries apart from the three Scandinavian ones have enacted data protection legislation (Austria, France, Germany and Luxembourg). The United States and Canada both have national legislation which applies to the public and federal systems. International organizations like the Council of Europe and the OECD are currently preparing draft treaties or recommendations on data protection legislation.

This paper, however, will not try to cope with the problems on an international level, but will rather discuss in some detail the problems in the Scandinavian legislation which apply to a geographical area with intensive transnational data traffic.

The comparative perspective of this paper is difficult to establish. The data protection legislation cannot be understood apart from its legal context in national law. In Sweden, the Data Act can only be appreciated in the context of the liberal public access to governmental files which has so long been a tradition in that country. In Norway, the Personal Registers Act is closely related to the legislation on procedure within public administration.

[1] The term "data protection" (from the German *Datenschutz*) is used in preference to the more traditional term "privacy", which is so closely associated with the United States constitutional "right to be let alone". Though considered to be a synonym of "privacy", it signalizes the rather more mundane legal context of administrative law (cf. Bing 1979*b*).

[2] Throughout this paper "data" will not be used as a technical term distinct from "information", but rather as a synonym for both "data" and "information".

[3] Cf. for instance, *Ot.prp.* no. 2 1977–78, pp. 8–10, *SOU* 1978:39.

Though there are great similarities between the national legal systems of Denmark, Norway and Sweden, the differences still create pitfalls for the incautious student of comparative law.

2. THE SCANDINAVIAN DATA PROTECTION LEGISLATION

As a background for the discussion below in sections 3 and 4, the data protection acts in three Scandinavian countries will be briefly outlined.

Sweden was the first of these countries to adopt a Data Act (1973:289). The Act applies to computerized systems only. These are made subject to licence. Any person for whose activities processing is carried out, and who has control over the system (in the Act such a person is termed the "responsible keeper"[4]) has to apply to the Data Inspection Board for a licence. The Data Inspection Board is an administrative agency created by and given powers under the Act. The Swedish system of control hinges on the Data Inspection Board, which grants licences, checks that the provisions in the licence are actually followed, investigates appeals from the public, etc.

The Swedish legislation was intended to be experimental. It was fairly successful, at any rate measured by its influence on the development in other countries. It was, however, subsequently reviewed, according to plan, by a committee established in 1976. This body reported in 1978.[5] The report resulted in amendments of the Data Act in July 1979.[6]

Denmark, which enacted its data protection legislation in 1978, chose a rather original approach. Computer systems within the public and the private sectors are regulated in two separate Acts (nos. 293 and 294 of 1978). For the purposes of the present paper, the Private Registers Act which deals with the private sector is the one which possesses the greater interest, as the transnational data flows from the public sector are rather modest.

The Act applies to computerized systems as well as to most manual systems containing personal data. Both systems are mainly regulated by substantive clauses in the Act itself, but there are provisions for licensing of certain systems or activities. The licence is then granted by the Data Surveillance Authority, a public agency created by the Public Authorities' Registers Act.[7]

[4] Cf. sec. 1(5).
[5] Cf. *SOU* 1978:54.
[6] Cf. *prop.* 1978/79:109.
[7] Cf. ch. 7.

The Danish Acts entered into force at the beginning of 1979, and the Authority was also established at that time.

The Norwegian Act relating to Personal Data Registers (Act of June 9, 1978) applies to manual as well as computerized systems within the private and the public sectors. It makes computerized systems and systems containing sensitive personal data subject to licence, while other systems are governed by a set of basic, substantive norms. A special public agency, the Data Surveillance Service, is to be established, and this will be given power to grant licences, etc., in much the same way as the Swedish Data Inspection Board.

The Norwegian Act has not yet come into force. It constitutes a framework to be completed by more specific regulatory law, which at present only exists in the form of a draft of September 13, 1979. The Act will enter into force at the beginning of 1980.

This introduction does not, of course, do full justice to the Acts themselves. Its only aim is to indicate the fields of application and the system of control established in the three countries. Even this brief introduction, however, reveals major differences—the Swedish Act applies only to computerized systems, while the Danish and Norwegian Acts both, albeit to different degrees, apply to manual systems too. Denmark relies within the private sector mainly on substantive norms set out in the Act itself, while Norway and Sweden utilize as the major tool of control provisions spelled out in the licence issued to the specific system. These differences are only examples of those which exist between the Acts. Some will be discussed below, but most of them cannot, of course, be dealt with in this paper.

> In citing the acts, the English translations made available through the OECD Compilation of Privacy Legislation in OECD Member Countries will be used. The Swedish Act will, however, be cited in an approved English version made available after the amendments of July 1979. Since the translations are approved by the respective national authorities, the phrases in each translation are rather idiosyncratic. Where not actually citing the acts, I shall therefore employ those terms which seem to have emerged through the international debate on data protection. Where thought necessary, these terms are explained in footnotes.

3. EXPORT OF REGISTERS CONTAINING PERSONAL DATA

3.1. *What is a "Register"?*

The data protection legislation has created its own terminology. In order to qualify the field of application, the acts use some basic concepts. One of

these is "system" or "register". It is used to define what forms of personal data processing fall within the scope of the law.

The data protection legislation does not, as a rule, apply to the processing or use of single elements of personal data, but rather to that use which is organized in connection with a system of personal data. The common core of the system concept is the computerized base of personal data, where, for instance, data on income, criminal history or education may be retrieved by name or personal identification number. When used in defining the scope of an act, however, this concept is refined and specified.

In the definition of a "system", three main categories of criteria are in use: (1) qualification of the *content*, (2) the *technology*, and (3) the *organization* of the system. In this paper, a detailed discussion of the system concept in Scandinavian legislation cannot be justified, but the major characteristics to be found within the three acts will be given. A more detailed discussion will be found in a study by the present author.[8]

The Swedish system concept is, perhaps, the simplest. According to the Data Act, sec. 1, a "personal register" is any register which is computerized and which includes data on an individual. The term "register" is also taken to imply that some sort of structure must be imposed on the system—if, for instance, personal data are imbedded in the text entered into a word processor, this does not make the text a "personal register".

The Danish concept in the private sector Act,[9] is a composite concept, made up of two definitions. First, all computerized systems containing personal data fall within the scope of the Act. Secondly, all manual *or* computerized systems containing "private" data on physical or legal persons fall within the scope of the Act. The phrase "private" is given the same interpretation as in the Danish penal code sec. 264 d, and is a qualification of "personal" data. Examples are data on family life, sexual relations, certain private conflicts, and health.[10] Furthermore, in the Danish Act, the term "register" implies a certain organization, though the phrase is given a wider interpretation than in everyday language.

As to the Norwegian Act, "personal data registers" are constituted by any system containing data on physical or legal persons. This is qualified, however, so as to include only those systems in which the data:

> ... is systematically stored in such a way that information concerning an individual person can be retrieved.[11]

[8] Bing (1979*b*).
[9] Cf. sec. 1(1).
[10] Cf. Jensen 1978, p. 4436.
[11] Cf. sec. 1.

This criterion of retrievability is stronger than the simple criterion of organization implied by the term "register" in the Swedish and Danish Acts. The system must allow identifying data—e.g. name, personal identification number or fingerprint—to be used as a search request.

This bird's eye view of the system concepts basic to the three Acts shows that, though the core is common, the shell is different. The core is the computerized systems containing information on individuals. The Danish and Norwegian Acts also include computerized systems containing data on *legal* persons, but the Danish Act qualifies this further by excluding those systems in which the data is not "private". Both the Danish and Norwegian Acts apply to *manual* systems, but the Norwegian Act demands that personal data shall be retrievable by identifying criteria.

The system concepts in all three Acts are characterized by the term "register", which indeed is used in all of them. Though this expression is given an interpretation which deviates from the everyday notion of a "register", and has no counterpart in computer terms, it is well suited for use as a common denominator for the Scandinavian system concept. But, when discussing the clauses, one should bear in mind the underlying differences in the way "register" is defined.

> Several problems of the system concept have not been discussed here. There is the problem of how strong the link between a person and data should be before that data is qualified as "personal". It is the problem of what really is the distinction between "computerized" and "non-computerized" systems. The Norwegian criterion of retrievability is also rather problematic; though well suited to manual systems, it is uncomfortably slippery in respect of computerized systems. For a somewhat more in-depth discussion of the system concept, see Bing 1979*b*.

3.2. *Export of Computerized Registers in General*

A computerized register may typically be exported in two different ways. It can be transmitted by telecommunication to a computer facility in another country; or it can be copied onto magnetic tape, discs or similar devices and physically transported to another country.

By both methods, the register becomes available outside the territory. Even if the national legislation on data protection still applies,[12] the practical problems of enforcing the law are rather evident. In order to grant the citizens the level of data protection determined by the law, there have been enacted special provisions in order to control the export of registers.

Again, the most clear-cut example is sec. 11 of the Swedish act. If there

[12] Cf. 5.3 below.

is "reason to believe" that the data of a register will be used in computerized systems abroad, a licence from the Data Inspection Board is required. It is laid down that the Board should give such a licence

> ... only if there is ground to believe that the issuance will not cause undue encroachment on privacy.

In applying this cause, the Data Inspection Board has adopted a rather restrictive approach.[13] Licences have been granted for client registers in respect of activities concerning cars, television sets, and gramophone records. Also, public agencies have been given temporary licences for the testing out of new computer equipment abroad with real-life data.[14]

On at least two occasions the Board has refused licences for the export of data to the United Kingdom. In both cases, it was a matter of exporting registers containing data on a rather large section of the population. The stated purpose of the exportation was in both cases the existence of better facilities for processing the data in the United Kingdom than in Sweden—in the first case, plastic health cards were to be embossed, in the second case a printed catalogue of the names with certain key data was to be produced. In its statement of reasons for the first decision,[15] the Board maintains that the presence of registers containing information on a large section of the Swedish population abroad creates a risk of establishing total population registers outside Swedish jurisdiction through the cooperation between a number of foreign computer service bureaus.

This is one way of interpreting these decisions. It should, however, also be noted that the United Kingdom still does not have any data protection legislation, and consequently cannot offer the registers within its territory protection corresponding to that provided within Sweden. The "level of protection" has been pointed out as the most important single factor in the German statute on data protection,[16] which allows the export of simple personal data if

> ... *kein Grund zu der Annahme besteht, dass dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden.*

The Swedish decisions seem also to have been interpreted in this way in the United Kingdom itself. The Lindop Committee argues as follows in favour

[13] Cf. *SOU* 1978: 54, p. 277.
[14] For a review of the Data Inspection Board's licensing practice in respect of sec. 11 of the Act, see *TDR* 3/1978, pp. 4, 6.
[15] Of August 12, 1974.
[16] *Bundesdatenschutzgesetz*, sec. 32(1).

of regulating registers containing data on non-nationals or non-residents:[17]

> ... data protection authorities in other countries might impose restrictions on the export to the UK of personal data about their own citizens if the processing of such data were excluded from the protection in the UK Act. Indeed, we understand that UK computer service companies, competing for Swedish data processing contracts, have already suffered from restrictions imposed by the Swedish Data Inspection Board, because of the absence of data protection legislation in the UK.

At the moment, only Sweden can show examples of how the export of registers has been regulated in practice. And it is interesting to find two central arguments relevant to such export associated with the early major decisions of the Data Inspection Board—the risk that undesired registers will be set up abroad, as well as the risk to the data subjects[18] that is created by the lack of data protection legislation in that country. These arguments are, of course, related to one another, as a data protection act might create the requisite control to eliminate the risk of unauthorized registers being created while the data is outside Swedish territory.

The Norwegian Act also has the same general rule as the Swedish on exportation of computerized registers:[19] export of a register is subject to the issuance of a licence by the Data Surveillance Service.

The proposed regulatory statute, however, modifies this rule. Under its rules an explicit export licence would not be necessary. It would be sufficient to notify the Service of the exportation of the register.[20] This declaration is to be made as far in advance as possible, and the Service may on the basis of the notification decide to refuse export. This, however, presupposes an active intervention on the part of the Service. The proposed regulation is even more lenient with regard to registers which are explicitly excluded, by regulatory law, as being subject to licence under sec. 9 of the Act. This exception includes ten categories of registers, which in practice are rather important.[21]

- an association's list of members,
- a trading company's list of customers and suppliers,
- a newspaper's or journal's list of subscribers,
- a library's catalogue of books or list of borrowers,
- a record keeper's register of personnel or employees,

[17] *Report* 1978, p. 246.
[18] "Data subject" denotes an individual, data on whom is included in a register.
[19] Cf. sec. 36(1).
[20] Cf. ch. III, sec. 8–3.
[21] Cf. ch. III, secs. 2 and 3.

- a bank's register of customers,
- a lawyer's register of clients,
- the register of patients of physicians, dentists, psychologists or other authorized health personnel,
- newspapers' and weeklies' registers of persons,
- any register only containing name, address and occupation.

Each of these categories is defined by content as specified in the proposed regulatory law under sec. 9 of the Act, and these registers may be exported without notification being made to the Data Surveillance Service. However, according to a provision in the regulatory statute the exception only applies where the data is not communicated to a third party.[22] Consequently, if the export implies communication to a third party, the record keeper must notify the Service of the exportation.

Though the Acts are similar in their general mode of regulating the exportation of computerized registers, the Norwegian Act differs from its Swedish counterpart in reducing the licence to a notification in the Norwegian proposed regulatory law, and in excepting a set of seemingly trivial, but actually important registers.

The Danish Act on the private sector does not include any general provisions on the exportation of registers. Computerized registers may, consequently, be exported without the necessity of obtaining a licence from the Data Surveillance Authority or notifying that agency. The Danish Act, however, contains special provisions on, for instance, registers containing sensitive data; these will be discussed below.

In my opinion, this exposé of the regulation of exportation of registers discloses a fascinating stratification of variations: from the general clause in the Swedish Act, which has been enforced rather strictly in practice; through the rather diversified regulation in the Norwegian Act, where by the proposed regulatory law the requirement of a licence has been eliminated or reduced to a notification; to the very liberal regulation in the Danish Act, where as a general rule registers may be exported without any restrictions.

3.3. *Export of Registers Containing Sensitive Data*

In the international debate on privacy and data regulation, the need to protect "sensitive" data has emerged as a controversial issue. The term "sensitive" is used to denote data of a very "private" nature, data for which there are special reasons for ensuring that they shall be given extra protec-

[22] Cf. ch. III, secs. 2–7(3) and 3–5(4).

tion. The issue is controversial, not because anybody has denied such a need, but because it seems to be difficult to arrive at any kind of international agreement as to what types of data are "sensitive".[23]

> Actually, there have been attempts to specify a "general sensitivity grading" of personal data. Though of some interest as illustrating the difficulties involved, the result is certainly not "general" in an international context, cf. Bing 1972.

In the Scandinavian legislation, on the other hand, a basically identical qualification of sensitive data has emerged. This qualification may be found in the Swedish Act sec. 4, the Danish Act on the private sector sec. 3(2), and the Norwegian Act sec. 6 (repeated in secs, 9, 16 and 26).

The Danish Act on the private sector gives the following definition of sensitive data:[24]

> Data on race, religious belief, colour of skin; on political, sexual, or criminal matters; on health, excessive use of intoxicants and the like ...

The definitions in the Swedish and Norwegian Acts are similar, though they differ in detail—for instance, the Danish definition is open-ended, while the two others are definite.[25]

In the Danish and Norwegian Acts this definition of "sensitive data" is relevant to the export of registers.

> Though not explicitly mentioned in the Swedish Act sec. 11, which regulates transnational data flows, it is evident that sensitivity of data will be an important factor in assessing the risk of infringement of privacy that is likely to arise if a licence to export a register is granted. In this way, the sensitivity of data also contributes to the decision reached under Swedish law.

In the Danish Act, export of registers containing sensitive data is subject to the obtaining of a licence from the Data Surveillance Authority.[26] This applies to manual as well as computerized registers, but only when the purpose of the exportation is to process the data by computer abroad.

In the Norwegian Act, all computerized registers are subject to export regulation as discussed above in 3.2. Manual registers containing sensitive data are, for the purposes of export regulation, treated as computerized registers.[27] According to the general rule laid down in the proposed regu-

[23] Cf. Bing 1979*a*, pp. 174–5.
[24] Sec. 3(2).
[25] Cf. Bing 1979*b*.
[26] Sec. 21(2).
[27] Cf. secs. 36 and 9.

latory statute, such exportation must be notified to the Data Surveillance Service prior to actual transmission, and the Service may prohibit the exportation.

> In relation to the computerized systems, notification was not necessary in respect of the registers excepted from the licensing system under the Norwegian Act, sec. 9. The proposed regulatory statute defines what elements may be contained in such registers, and this definition excludes registers containing sensitive data. Therefore, manual registers containing sensitive data will not profit from the more lenient regulation of "trivial" registers. It should, however, be pointed out that there is a loophole. The register of an association or a journal must not include any sensitive data, but the *nature* of the association or the journal may, of course, indicate political attitudes or other data of a sensitive nature. Such registers may be exported without notification being made to the Data Surveillance Service. There are not, however, many loopholes of this kind. In the case of the registers of a library, for instance, the inclusion in the register of borrowers of the titles of books lent to a certain borrower brings that register out of the "trivial" category, and makes it subject to ordinary licence under sec. 9, and notification if exported according to sec. 36.

The Danish Act on the private sector also makes an interesting exception in sec. 21(2). There it is provided that a licence to export a register containing sensitive data is not necessary with respect

> ... to a register which is found in Denmark solely for the purpose of undergoing electronic data processing.

This exception is designed to meet the special situation when a register is imported into Denmark only for the purpose of processing the data in that register. Such a situation would typically arise because of a desire to use Danish back-up facilities, but it could also arise where, for instance, the foreign enterprise wishes to use a Danish computer service bureau for commercial reasons.

As mentioned in the introduction to this paper, the use of back-up facilities in another Scandinavian country is rather common. This is also the assessment of the Swedish committee on data legislation,[28] which states that the lack of a licence to use foreign facilities for back-up may cause problems for the enterprise concerned.

> In one case, the Swedish Data Inspection Board granted a bank in the south of Sweden a licence to use back-up facilities in Denmark for its personnel register. This also includes a licence to test the back-up routines on the Danish

[28] Cf. *SOU* 1978: 54, p. 278.

facility regularly.[29] In this case, the licence from the Swedish Board was necessary for the export of the register, whereas a licence from the Danish Data Surveillance Authority is not necessary for exporting a register which is temporarily created for back-up purposes in Denmark, even if this register should contain sensitive data. The problem of registers established for a brief period for back-up purposes may be seen as a special case of problems caused by the "temporary registers".[30]

3.4. *Export within an Organization*

A rather common situation is expert of data from a company in a Scandinavian country to the parent or sister company in another country. This constitutes data export within the same organization, and—in general—according to the Scandinavian Acts the same rules apply as to other reasons for export. By way of contrast, reference may be made to the German legislation, where as a general rule export is permitted if based on a contractual relationship.[31] This would normally include export within an organization.

An important decision by the Swedish Data Inspection Board may illustrate this point. The German multinational company Siemens was not allowed to export data on employees at their Swedish company to a central personnel information system in Germany (the reason given for the export was to facilitate coordination of staff transfer, statistics, internal education schemes, etc.). The Board justified its decision by pointing to the risk that if consent was given such export would generally take place from Swedish subsidiaries. The Board maintained that this would create a possibility for unauthorized establishment of a register comprising a large number of Swedes in a foreign country. It also pointed to the lack of data protection legislation in foreign countries at the time of the decision.[32]

A similar policy is indicated in the Danish bill, where the Minister of Justice, in his remarks on the clause governing register export, explicitly states that this would also apply to the case where a computer service bureau exports a register for processing to a section of the bureau abroad, or where the register of an enterprise is processed by a section of the enterprise abroad.[33]

In general this also holds true for the Norwegian Act—export of a register from a subsidiary in Norway to a parent company abroad is subject

[29] Cf. *SOU* 1978: 54, p. 278; Freese 1979, p. 42.
[30] Cf. Freese 1976, pp. 250–51.
[31] Cf. the German Act, sec. 24.
[32] March 1975—the German Act on data protection was not enacted until 1977. Cf. *TDR* 3/1978, pp. 4, 6; Bogdan 1978, p. 12; Freese 1979, p. 63.
[33] Cf. L36 1977–78: 23.

to the regulation in sec. 36. But the proposed regulatory statute to be issued in pursuance of sec. 36 introduces an exception in respect of the "trivial" registers mentioned in 3.2 above. Such registers may be exported without any restraints so long as the record keeper[34] conforms to the rules laid down in the proposed regulatory statute under sec. 9 of the Act, according to which data from the register must not be disclosed to a third party, for instance "another company".[35] Whether export to a foreign subsidiary or parent company constitutes export to "another company" is rather doubtful. And certainly this is not the case if the register is exported to, for instance, a local representative of the national company residing abroad.

In general these registers contain—as discussed in 3.3 above—rather trivial data. But one of the types of registers classified as trivial is a personnel and salary register,[36] which includes educational data, job-related data, and other "neutral" data necessary for general administration. One would think that in the Siemens case referred above, the register to be exported was very close to being what in the proposed Norwegian regulatory statute is classified as "trivial", and that under the Norwegian data protection legislation Siemens would have been able to export the register to Munich without even notifying the Data Surveillance Service.

3.5. *Export of Subregisters from Registers*

Above it has been assumed that a whole register is exported. This is, of course, by no means an unusual situation, as the reported cases from the Swedish Data Inspection Board demonstrate. One should, however, be aware of the even more common situation where only part of the data contained in a register is exported.

The Swedish Act sec. 11 regulates the export of data from a register. If there is reason to assume that this data will be processed by a computer abroad, the export is subject to licence. It should be noted that this applies even to the transmission of a single data element contained in a register.[37]

Though manual registers are in general not covered by the Swedish Act, the Act regulates the export of any output from a register for computerized processing abroad.

[34] "Record keeper" denotes the person or organization responsible for the register's conformity to the data protection legislation. This responsibility will be defined by rules in the national legal system which may be deviating, and create problems additional to those discussed in the paper.

[35] Cf. the proposed regulatory statute ch. III, secs. 2–7(3) and 3–5(4).

[36] Cf. the proposed regulatory statute ch. III, sec. 3–2.

[37] Cf. 4.2 below.

> Obviously it is difficult to determine the reasons for an export, and there are certainly practical difficulties in applying this as the criterion for determining what exports are subject to licence. This criterion is, nevertheless, used by all three Scandinavian Acts with different functions. It will be discussed below in 4.2.

In the Swedish Act, only export from registers is regulated. This simplifies the situation somewhat, as generally there has to be a computerized register in Sweden which is already licensed under sec. 2 of the Act. A borderline case is that where data are collected in Sweden for export abroad and are to be included in or organized into a register there. This situation will be dealt with below (4.1).

In the Norwegian Act, export of registers as well as export of data is regulated. Computerized registers and registers containing sensitive data may generally not be exported without notification thereof being made to the Data Surveillance Service,[38] while data may generally be exported without restrictions.[39] There is, consequently, some legal justification for distinguishing registers from a mere collection of data.

This issue may be broken down into two questions. One is simply a variation of an age-old legal problem of construction: When does a copse become a forest? The modern version of this would be: When do a few names become a register? Obviously, data on one person is *not* a register. If, for instance, there exists access to a Norwegian register from abroad, and data on a single person is extracted from that register, this does not constitute export of a register. This access would then come under sec. 36(2), and would—with the exception discussed in 4.2 below—be unrestricted.

It is equally obvious that export of data even on a small number of persons would be regarded as export of a register. Where this threshold is located, may be revealed by practice, but will probably depend to a great extent on the overall situation and the nature of the data exported. As any export for the purpose of introducing data in a register abroad is subject to restrictions, one may find that the Data Surveillance Service will take a rather liberal view when data is exported *without* that purpose. This may make the Service inclined to accept lists on, for instance, six or seven persons as being export of data on several persons rather than export of a small register.

The other question is that of organization. The criterion of retrievability is essential. In Norway a register may be transformed into a collection of

[38] Cf. 3.2 and 3.3 above.
[39] Cf. 4.2 below.

data by making the personal data non-retrievable by identifying particulars. Also, a computerized register always falls within the scope of sec. 36(1), while a manual register must contain sensitive data to be subject to this provision. Consequently, one may remove a register from the area of sec. 36(1) by either reorganizing it as non-retrievable by identifying particulars, or—if it does not contain sensitive data—by printing a manual copy. Therefore, under the Norwegian Act, one may very well export products which contain the data of the register, but which are not subject to sec. 36(1) and the proposed regulatory statute under this provision. This is in contrast to the situation under Swedish law.

> Under Norwegian law, one must consider the nature of the product, and determine whether this qualifies as a "register" in its own right. This does not create any special problems, though it may be difficult both to determine whether data in a register is "retrievable" by identifying particulars, especially if the register is computerized,[40] and whether the register is "manual"[41] or "computerized", if, for instance, a printout is typed with a fount designed for optical character reading. The issue is, however, somewhat confused by comments in the government bill.[42] There it appears that a distinction is made between machine-readable copies of the register ("tapes, discs, files, etc.") and manual copies ("lists or publications"). This is, to my mind, not very clarificatory, and I would suggest that the product, in whatever form it may appear, should be regarded as subject to the provisions in sec. 36(1) and subsequent regulatory statute if it qualifies as a "register" under the Act.

As discussed above under 3.3, the Danish Act regulates only export of registers containing sensitive data, and does so only when these are exported for processing by computer abroad. Also in respect to the Danish Act, the qualification of a "register" consequently determines what clause in the Act will govern the export. However, export of sensitive data is in general rather strictly regulated in the Act,[43] and therefore the consequences of the distinction between a "collection of data" and a "register" are less important than in the case of the Norwegian Act. The more general "register" concept of the Danish Act will also make some of the borderline cases discussed in respect of the Norwegian Act rather impractical.

In this section, it has once more been demonstrated how the Scandinavian legislation differs in important details. The Swedish Act makes any export from a register subject to licence. In Norway, only the export of

[40] Cf. Bing 1979*b*.

[41] A "manual" register is a register which is not computerized. It may, however, be mechanized or be in micro-form—consequently the term is used in a rather specialized meaning.

[42] Cf. *Ot.prp.* nr. 2 1977–78, p. 96.

[43] Cf. 4.2 below.

computerized non-trivial registers and manual registers containing sensitive data is regulated, and made subject to a duty of notification. In Denmark, only export of registers containing sensitive data is regulated, and then subject to licence. It would seem that the Norwegian and Danish Acts are more lenient, inasmuch as they do not regulate *any* export from a register, but allow, for instance, access from abroad for retrieval of single data elements without licence. The leniency, however, is only apparent, as these two acts contain specific provisions governing the export of personal data *not* organized in a register. In contrast, the Swedish Act only regulates export from a register. This second level of regulation in the Danish and Norwegian Acts creates a safety net which permits a more flexible regulation of the export of and from registers.

4. EXPORT OF DATA

4.1. *Collection of Data for Foreign Registers*

The situation discussed in this section may, once more, be introduced by an example from the Swedish Act, which as mentioned before applies only to computerized registers. The qualification of a system as being "computerized" is by no means trivial. Is a register "computerized" only at the moment of inclusion in the computer, or is it computerized at an earlier stage, when collected for such a purpose? Swedish law takes this latter, more inclusive view. The obvious consequence is that even the collection of data for establishing a computerized register triggers off the obligation to obtain a licence. Also, such collection for the inclusion in a *foreign* register would be subject to licence from the Data Inspection Board. Bogdan[44] argues in this sense, but states that in his view the Board has not in practice exploited the possibilities of control which are inherent in such an interpretation. Allusions have been made to unspecified examples where the Act has consciously been sidestepped by exporting primary data in conventional form and establishing registers abroad.[45]

More recently, however, this practice has been revised. The example usually cited (from September 1977) concerns a bank which was redesigning its computer systems and for a limited period wanted to process deposit transactions in Luxembourg. The data was transmitted by telex to its subsidiary, and the output was mailed back to Stockholm. No com-

[44] Bogdan 1978, p. 10.
[45] Cf. Freese 1976, p. 273.

puterized register was established in Sweden. The Data Inspection Board considered the case to come within the scope of the Act, but licensed the export for a period of three years. It may be argued that this case is not clear-cut, inasmuch as the export by telex can be construed as export of machine-readable data. The case is, however, cited as an example of a more strict practice.[46]

Under the Danish Act, collection of data for export to foreign registers is, in general, not regulated. There are, however, three exceptions. One, dealing with any type of export of sensitive data, will be discussed below in 4.2. The other two will be dealt with here. They concern collection of data to registers which would have been subject to licence if they had been within Danish jurisdiction,[47] and collection of sensitive data.[48] These two types of export are subject to licence of the Data Surveillance Authority. The provisions are designed to reduce the risk of establishing registers abroad of a type which are subject to licence or are considered highly controversial in Denmark.

The first category includes such systems as are subject to licence—and, within the private sector, is in fact a very small one. An example may be registers

> ... established for the purpose of warning others against doing business with or employing or serving any party registered.

These types of "blacklisting" registers are subject to licence.[409] As this is qualified by the *purpose* of the register, the category may include very diversified types of data.

The second category includes types of data which are qualified as "sensitive" according to sec. 3(2), and which in general may not be included in a register. The Act does, however, provide for a few exceptions to this rule. Obviously the establishment and use of sensitive registers may be controlled within Danish jurisdiction, while there will exist a need to control export in order to avoid evasion of the rather strict provisions concerning sensitive registers.

Reflecting the general differences between the Norwegian and Danish Acts, sec. 36(2) of the Norwegian Act includes *any* export of data collected for the purpose of computerized processing abroad. There are, however, some non-obvious exceptions to this provision. These will be discussed below (4.2).

[46] Cf. Freese 1979, p. 64.
[47] Sec. 21(1) (2).
[48] Sec. 21(2) (2), cf. sec. 3(2).
[49] Cf. sec. 3(3).

Export of data for computerized processing abroad is subject to licence from the Data Surveillance Service according to the general provisions of the Act. The proposed regulatory statute has, however, exploited the possibility of modifying the general provision.[50]

To a certain extent, the regulatory statute has turned the tables on the Act. If data are collected for use in registers qualified as "trivial" by the regulatory statute (and this includes the requirement that data shall not be communicated to a third party), such data may be exported without restrictions. Otherwise, notification to the Service must be made prior to the export. This will also include export of *sensitive* data or data to be processed in registers which would have been subject to licence within Norway. It would seem that there are fewer barriers in the Norwegian regulation against the establishment of undesired registers abroad than in, for instance, the Danish law. The difference between a licence and a notification should, however, not be exaggerated. The Service may act on the information given prior to the export, and actually restrict or prohibit such export. Therefore, the system set up cannot be justly assessed without some knowledge of the practice to be followed by the Service.

> The comments annexed to the proposed regulatory statute discuss the problems in relation to this situation. A special licensing system for data export was suggested, but the committee drafting the proposed regulatory statute thought a system of notification sufficient at the outset. With increased knowledge, through the notifications made, of the nature of the data export, it is possible to identify situations which will be made subject to licence.

4.2. *Export of Single Data Elements*

In this subsection, the point of view is shifted. Up to now, either registers or data collected to establish such registers abroad have been discussed. There has been an implied understanding of a systematic activity and typically a significant volume of data. The discussion in 4.1 above may be considered an extension of the discussion of export of registers—though a register is not established within the country, data is collected for establishing such a register outside the country.

In this subsection, we shall take a look at the situation where single elements of data are exported: a single name, a dossier on a particular person, etc. It is obvious that the data exported is not itself a register, and that it does not by itself create a register abroad.

[50] Cf. 3.2 above for the discussion of the regulatory statute in respect of the export of registers—the same clauses regulate the export of data collected in Norway for computerized processing abroad.

In the case of the Swedish Act, the situation subject to regulation is the exportation *from* a register in Sweden *to* a foreign country when "there is reason to assume that personal data will be used for automatic data processing". Consequently even the export of single data elements from a Swedish register for computerized processing abroad is subject to licence. If such systems need to communicate with foreign systems, the problem will be discussed in the context of the general licence, and may also be solved there. Only where this is not the case must a licence for export of single data elements be obtained.

> It is easy to see that a considerable control problem exists in connection with the export of single data elements. By accessing a Swedish system through a dial-up terminal, data may be retrieved if the user possesses sufficient knowledge concerning passwords, etc. In such cases the system cannot distinguish between a national and an international dial-up. Though this is also, of course, a general control problem respecting export of data, even in the form of registers, the control problems will be serious in the case of the single data element export.

Outside the situation discussed above, the Swedish Act does not regulate export of single data elements—for instance the export of a single data element collected and communicated in conventional form for computerized processing abroad.

The Danish Act, too, is very unadventurous on this matter. Most of the provisions in sec. 21 are only relevant to the export of registers or the "systematic collection of data". Export of single data elements is not subject to these provisions.

In addition, however, sec. 21(1) (1) prohibits the collection of sensitive data "for the purpose of registration outside Denmark". As mentioned before, sec. 3(2) of the Danish Act as a general rule prohibits the inclusion of sensitive data in registers. There are important exceptions to this general rule. But where such an exception does not apply, the Act also prohibits export of single data elements of a sensitive nature for inclusion in a foreign register. The reason for this provision is obviously, once more, to reduce the risk of evasion of the Act.

Such export is only prohibited if "the purpose" is inclusion in a foreign "register". The Danish Act does not, according to its general scheme, restrict its application to export for computerized processing abroad, but also embraces inclusion in any kind of foreign "register". It may be noted that owing to the rather specialized register concept, such a foreign register may very well fall outside the scope of a foreign national data protection act.

> A fictitious example may illustrate this and indicate the strictness of the Danish regulation. For instance, health data may not as a general rule be included in a register. Inclusion of health data in a letter ("my wife had a headache, and could not attend . . .") is generally not permitted if that letter is filed either as a copy in the sender's register, or in the receiver's subject-indexed file of correspondence.

There is, however, a further qualification: the export must have the "purpose" of including the single data element in a foreign register. (This qualification may actually exclude the example given above from the scope of the provision.) One may contrast this criterion of "purpose" with the more open criterion in the Swedish act: "reason to assume that personal data will be used for automatic data processing" abroad.

The Norwegian Act likewise bases its provisions on the criterion of "purpose". It also has the most general regulation of export of single data elements: the same provisions as discussed above for collection of data apply to the export of single elements of data.

Through the proposed regulatory statute ch. III sec. 8–1, this is transformed as discussed above in 3.2 and 4.1: export to "trivial" registers is not restricted (provided data from such registers is not communicated to third parties), and export to a register which would have been subject to licence in Norway is made subject to prior notification to the Data Surveillance Service.

The problem of "purpose", however, exists. This is discussed in the bill.[51] In this discussion a distinction is made between a case where the reason for the export is the use of data for solving a problem abroad, and a case where the reason is inclusion in a register. In the first category—where utilization is the reason—the export falls outside the scope of sec. 36 of the Act. As examples, the bill mentions the use of credit data in a business transaction, or medical data exported from a Norwegian hospital for use in a foreign health institution where a Norwegian patient is being treated.

The bill distinguishes between a "primary" and a "secondary" reason for the export. If the primary reason is utilization, the foreign hospital may store the medical records submitted to them from Norway without further ado.

The discussion of "purpose", which is a major criterion in both the Danish and the Norwegian regulation, illustrates the problems created. It must be rather difficult to ascertain—when a request for information to a foreign source is received—whether the information is to be used or

[51] *Ot.prp.* no. 2 1977–78 p. 96.

whether it is just to be registered. If the request comes from a hospital actually giving treatment to a Norwegian patient, it may be exported without involving the data protection authorities. But if it comes from a hospital which is not actually treating a patient, for instance when the potential patient takes up residence in the district, the export is subject to notification.

There may also be cases in which there are difficulties in distinguishing between utilization and storage in a register—for instance, when subscribing to a magazine, is the purpose of the export of a person's name and address utilization (to have the magazine mailed to his address) or is it inclusion in a register of the subscribers for addressing purposes?

> This criterion of "purpose" is also used for collection of data for export. A sale of, for instance, a telephone directory to a foreign direct mail service is, in principle, subject to notification under the proposed regulatory statute if the primary reason for the export is inclusion in a register. The bill admits that there will be problems of control,[52] and states that the registration of official publications, like the telephone directory, income-and-tax listings, etc., cannot be avoided. The author submits that there is reason to be sceptical about a provision that introduces such an evasive criterion as "purpose", which admittedly cannot be construed in a satisfactory way.

When outlining the difficulties associated with the use of the term "purpose" in the Danish and Norwegian legislation, it is today only possible to speculate on the adequacy (or, perhaps more to the point, inadequacy) of such a criterion. Only when the provisions have stood the test of actual use will it be possible to judge them fairly.

> In concluding this section, one more point in relation to the Norwegian Act may be mentioned. The Act is, within the private sector, restricted to "private enterprise, societies or foundations". It is easy to give examples of private activities which have no business purpose (not an "enterprise" in the meaning of the Act), and which are not part of activities within a society, an association or any such organization. For instance, two people may be swapping stories about mutual friends, a person may do research for his own amusement, etc. If a person subscribes to a journal or purchases some other kind of service for his personal use, then the provider of that service will have a business purpose—and consequently the activity will fall within the scope of the Act. But if the provider of the service resides outside Norway, does the Act apply then?
>
> This is a rather general problem, but it is especially acute in the case of export of single data elements. Is, for instance, the export of my name to a foreign journal subject to prior notification to the Data Surveillance Service? As the Act would have applied to such an activity if the provider of the service

[52] *Ot.prp.* no. 2 1977–78, pp. 96–97.

was residing within Norway, I should be inclined to answer in the affirmative. The question whether something is a "business transaction" cannot be determined by looking at only one of the parties to the transaction. Also, it should be noted that the regulatory statute has reduced this problem. The register of a journal of its subscribers would be a "trivial" register according to ch. III sec. 2–3, and sec. 36 does not apply to such a register.[53] This, however, presupposes that the provider in question does not communicate the data obtained from the register to a third party—and this is perhaps an assumption which a few subscribers to international journals may be inclined not to make.

The details discussed above may illustrate the problems which arise when trying to regulate export of data not associated with a register in Norway, and where there consequently does not exist a prior responsibility for a Norwegian record keeper. The Swedish solution, which regulates only export of single data elements from registers, is certainly simpler.

5. DATA PROTECTION AND THE CHOICE OF LAW

5.1. *Introduction*

The discussion above has implied that data protection has an international aspect. This is obviously true—teleprocessing, facilitated by the use of telephone networks and, increasingly, by networks dedicated to the sole purpose of transmitting data, has reduced the geographical distance between the user and his terminal and the computer and data to be accessed, to a rather trivial factor. Numerous reasons can cause a user to choose a foreign rather than a national computer service: the price, the range of service offered, or the existence of more permissive foreign data protection legislation.

One difficult problem, which so far only has been touched upon, is that of jurisdiction in respect of computerized systems. Associated with this problem is, of course, the problem of conflict of laws: if a problem is of an international nature, which law will be applied to the problem by the court?

In the work of the Council of Europe and the OECD, attempts have been made to design a conflict-of-laws clause which may be applied to data protection law. So far these attempts have been unsuccessful, in the sense that none of the proposed clauses has been incorporated in a draft treaty or recommendation.

Obviously, these problems cannot be discussed in this paper in any detail. I shall, however, look into three problem areas—the problem of

[53] Cf. the proposed regulatory statute ch. III, sec. 8–1.

qualification, the problem of territorial features of the data protection legislation, and the problem of the proper law of data protection. The discussion should be regarded as a tentative specification of the problems to be solved rather than as an attempt to solve those problems.

5.2. *The Problem of Qualification*

So far, the term "data protection legislation" has been used in a somewhat vague sense. This legislation is, however, an integral part of each country's national legal system. The Scandinavian Acts are most certainly best assessed in the context created by other statutes which regulate the procedure and decisions of public and (to a lesser degree) private administration. Within the Norwegian private sector, special general collective agreements between the top organizations of employers and employees specify and regulate the same issues as the data protection legislation.

Thus data protection legislation is not limited to those central statutes that have been enacted and named as "data protection acts". But also, in a similar way, the acts themselves are heterogeneous. They contain elements of administrative law, tort law, criminal law, etc.

The conflict of laws is traditionally solved by a set of rules, often formulated as maxims. By qualifying the area of law in which the problem is located, the rule to be applied for the choice of law is determined. In the case of administrative law, the territorial principle is usually applied. But where the law of torts is concerned, another rule will be applied—for instance, the *lex loco delicti commissi* (the law of the country in which the harmful act was committed) or the more flexible "closest connection" doctrine.

It is fairly obvious that different substantive rules may follow from different rules for the choice of law, and that it may be rather problematic to qualify a certain clause in respect of such rules governing the choice of law.

In legal writing,[54] a distinction has been made between the problem of extraterritorial application of the Swedish Data Act, and the problems of conflicts of laws in the two areas of criminal law and torts. Further distinction may probably be made.

In this respect, it may be of interest to note that the method chosen to regulate registers may be of major importance. In Sweden all computerized registers are subject to licence. No really substantive rules on data protection are actually expressed; they are implemented through the

[54] Bogdan 1978.

licence awarded by the Data Inspection Board. In contrast, Denmark relies heavily upon substantive regulation in the statute itself, making interventions from the Data Surveillance Authority an exception rather than a rule. The Norwegian approach combines these two solutions, having a set of substantive rules applied generally, and qualifying a sub-set of registers as subject to licence.

In terms of private international law, the Swedish approach is based on intervention by a public agency. The law governing public agencies constitutes a part of administrative law. In relation to the choice of law, the authority of public agencies is traditionally limited to the territory.[55] The Danish Act has another approach. Within the private sector, the substantive rules obviously cannot be qualified as "administrative law"; one has to decide what is the "proper law of data protection".[56] The substantive law does not in principe create the same sort of tendency to territorial application as does the Swedish solution.

Some of these questions will be pursued below. First, the problem of extraterritorial application of data protection legislation will be discussed. Secondly, the "proper law of data protection" will be briefly considered.

5.3. *Territorial Features of Data Protection Legislation*

As mentioned above, the Swedish Act is based on the intervention of a public agency, the Data Inspection Board. This brings the Act within the realm of administrative law, and creates the presumption of its limited application to registers within the territory.[57] Freese[58] likewise presumes that the Act may be evaded by computerized processing outside the country, though he is less precise than Bogdan. Seipel[59] is rather more cautious; he states that the "territorial validity" of the Act "is somewhat uncertain".

In the Danish bill,[60] it is stated rather clearly that the Act does not apply to registers established abroad, even if such registers contain data on persons in Denmark. This statement is repeated by Jensen[61] in his commentary on the Act. Its importance should not, however, be exaggerated. The comment is rather brief, and certainly was not designed to make, for instance, "foreign establishment" a decisive criterion respecting "national

[55] Cf. Bogdan 1978, p. 5.
[56] Cf. 5.4 below.
[57] Cf. the arguments of Bogdan 1978, pp. 5–7.
[58] Freese 1976, p. 224.
[59] Seipel 1974, p. 46, and 1975, p. 184.
[60] L36 1977–78: 23.
[61] Jensen 1978, p. 4438.

access". Also, the bill containing this comment does not include sec. 7, which seems to indicate a certain extraterritorial application of the Act:

> The provisions of section 6 shall also apply where the register is subject to electronic data processing outside Denmark.

The provisions of sec. 6 briefly state a few main principles of updating, relevance, correctness and data security commonly found in data protection legislation. If a Danish company processes a register abroad, it has a duty to ensure that the foreign computer establishment conforms to these principles. This also implies that the Danish Data Surveillance Authority may take action against the company if such principles are not observed.

To my mind, this indicates that there may certainly be registers outside Denmark containing data on Danish subjects which are not subject to the Act, but that sec. 7 of the Act also clearly assumes that the location abroad is not, in itself, sufficient to remove the register completely from the scope of the Act (and certainly not from the scope of sec. 6). Consequently, it may still be argued that the criterion for the extraterritorial application of the Act is to be sought in other facts than the mere geographical location of the register.

In the Norwegian committee report on the public sector, it was stated rather briefly that it would be desirable to offer Norwegian data subjects equal protection regardless of the place where the register is located, but that the enforcement would in practice be limited to the territory.[62] Elsewhere I have claimed that this may indicate that the Norwegian Act will be applied to foreign registers,[63] though there is no reason to disagree with Bogdan in his criticism of this conclusion as somewhat premature.[64] In the bill,[65] it is stated that by mere export of data, the national control will not in practice be enforced: the legislation of the importing country will then determine how the data may be used. This may indicate an interpretation of the Act which restricts its field of application to registers located within the territory. The use of the phrase "in practice" may, however, also be taken to indicate that the bill only stresses that though the Norwegian Act is in principle applicable, it would—of course—in practice be difficult to apply it to activities within the jurisdiction of another country. Thereby the bill justifies the severe regulation of data export which was the theme of discussion in the cited section of the bill.

[62] Cf. *NOU* 1975: 10, p. 72.
[63] Bing 1977, p. 108.
[64] Cf. Bogdan 1978, p. 6.
[65] *Ot.prp.* no. 2 1977–78, p. 8.

This examination of the Scandinavian Acts and their *travaux préparatoires* as well as of legal writing leaves us with few conclusions. It seems rather obvious that the Swedish Act has the strongest arguments in favour of a limitation of the field of application to the territory. The Danish sec. 7 at least assumes a certain extraterritorial application, and I am still inclined to think that the Norwegian Act may be interpreted in such a way that at least ch. III, which contains general provisions of a substantial nature, is applicable to systems established abroad if the relation to Norway is strong enough.

Rather than pursue this line of argument, one may try to determine what the territorial limitation really represents in relation to computerized registers. The register does not necessarily have a fixed geographical location. Above, examples have been given of back-up procedures whereby registers are piped through telecommunication lines into a computer situated in another country. By modifying the example, by introducing advanced networks for computer communication, it would be shown that it may indeed be difficult to determine whether a register is at any one place at any time. Consequently, the location of the register may not be sufficient to determine whether the legislation applies to this register or not.

It may be easier to mark the location from where the register is used than to settle where it is located. This is the line of reasoning taken by Bogdan[66] in respect of the Swedish Act: A foreign register is considered to be within the territory if there exists a terminal within the territory which accesses that register. This may be termed the criterion of "the location of the user" in contrast to the above-mentioned criterion of "the location of the register".

> Bogdan[67] actually suggests that the presence of a terminal within the territory which *may* access the register is sufficient to bring that register within the scope of the law. Obviously, with increasingly standardized communication protocols, most foreign registers can be reached by Swedish terminals through dial-up connections. In addition, one might require that the Swedish user shall know the necessary passwords and have established an account with the foreign record keeper. To my mind, however, it would be impractical to rely on anything but *actual* use by someone within the country.

This is in effect an admission of the insufficiency of the territory to determine the application of the national legislation. The use of a foreign register may be completely innocent in relation to data protection. But it will bring the national legislation to bear down on that register, and create

[66] Bogdan 1978, p. 8.
[67] *Loc.cit.*

a positive conflict of jurisdiction—as, of course, the country where the register is located will also apply its national legislation to that register. The law-abiding operator of registers will then want to screen users in order to avoid such tangled situations. Of course, the practical possibilities of applying the national law to foreign registers are very limited (as stated in the Danish and Norwegian bills). And we have the situation in which a national user, through his use, brings the register within the scope of his national law, and thereby invokes the sanctions. This may be desirable in some respects, since thereby misuse through foreign registers is reduced. But if the use is completely innocent, and the foreign country has an adequate, though different, data protection law, it would seem to be a rather unnecessary consequence which may have adverse effects on international commerce and communication.

Using "the location of the user" as a decisive criterion would in practice seem to result in massive application of the national law to registers which are obviously located abroad and have little real connection with the country. If a Norwegian firm accessed a register situated in the United States, containing lists of directors of shipping companies, why should the Norwegian Act apply to that register?

There are, of course, several ways out of this undesirable expansion of the field of application. One may qualify the criterion of "the location of the user" by requiring that the use should be of a certain regularity or volume. Another possibility would be to look at criteria not associated with the territory.

An obvious alternative is the persons concerned. These are of two categories: the record keepers, and the data subjects. By using these to qualify the criterion of "the location of the user", one may arrive at a less inclusive field of application.

One possibility would be to make "the location of the user" a minimum requirement: the legislation is only applied when the register is actually used from the territory. Then the reference to the persons concerned is used to qualify this. One may say that such a register is subject to the Act either if the record keeper is national or if the data subjects are closely associated with the country. Again, the closeness of the association of the data subjects may be determined by the volume of, or the sensitivity of, the data on national data subjects that are included.

The result would then be that the field of application was determined by a discretionary decision, where the location of a user within the territory was the minimum requirement, but where the law was not applied in such cases unless a certain closeness in respect of the persons concerned was found to exist.

The argument stated above should clearly be understood as an argument to amend the law, though I am not aware of any conflict with provisions in the Scandinavian acts, or in the practice of the data protection authorities. It does not conflict with the principle of territorial application as presented by Bogdan, but rather restricts the field of application as compared with that principle. In spite of the fact that the suggested interpretation is not in open conflict with any accepted interpretation or opinion, it is nevertheless rather loosely founded in the Acts themselves or any other legal sources. It would, however, in my opinion reduce the possibility of positive conflicts of jurisdiction, and would not create too unpredictable a situation for the record keepers. To my mind, it also indicates a *probable* development of the law in the Scandinavian countries.

5.4. *The Proper Law of Data Protection*

The situation to be discussed in this subsection focuses on the data subject who maintains that his data protection has been violated. The situation is assumed to have an international aspect, which gives rise to the question of choice of law in respect of the violation.

As mentioned in 5.1 above, there have been attempts to design a clause in treaties or recommendations on how to solve this problem of choice of law. I will not try to recommend how this could best be solved in the future, but rather will restrict myself to a discussion of how this would be solved under existing Norwegian international private law.

> If the discussion in this subsection is confined to Norwegian private international law, this is because of my ignorance of the private international law of Denmark and Sweden. I doubt, however, whether the discussion would be very different if it had been extended to include these systems. Some basic differences in Scandinavian private international law are well known. For instance, Sweden applies the principle of nationality, while Denmark and Norway apply the principle of domicile in respect of personal law. This difference may be relevant to the problem under discussion.

Initially, one may take the situation in which the register is located outside the territory of the country of the forum, but where the *lex fori* also applies to that register. The data subject maintains that an infringement has taken place, and argues that the law of the country in which the register is located should be applied. His motives for doing this may simply be that the law of that country is more restrictive, which makes the infringement relatively more severe, and offers him more substantial sanctions.

In such a situation, one would not be inclined to choose another law than

the *lex fori*. A state offers a certain standard of data protection to its citizens or residents. That another state offers a higher or different standard will not by itself be sufficient to choose the law most favourable as the *lex causae*.

One should not, however, completely exclude the possibility of choosing the law of the country in which the register is located. It may be that the data subject who claims that an infringement has taken place also has strong ties with that country.

If a Dane resident in Norway sues a Norwegian company, but has suffered damages in respect of business activities in Denmark, and through an infringement associated with a register operated by the Norwegian firm in Denmark, the Norwegian court may apply Danish law as the *lex causae*.[68]

The situation may be modified to that where the *lex fori* is not applicable, according to the arguments put forward in 5.3 above. In such cases, the court would rarely consider itself to have jurisdiction, as the register and its use would have a rather remote connection with that country. But one may assume that the court of the forum has jurisdiction—the record keeper is, for instance, a national company which through the activities of a foreign subsidiary has encroached upon the data protection of a foreign national resident within the country.

In this situation, the court must choose between the alternative *leges causae*. In our example, the subsidiary may have the register located in country A, while the infringement took place in country B where the register was accessed by terminal. The data subject is also domiciled in one of the two countries.

Under Norwegian private international law, it seems probable that the court would choose the law with which the matter has the closest and most substantial connection. One would not, I think, try to solve the conflict by any strict rule like a version of the *lex loci* or the *lex situs*. In our example, the choice of law would, I think, depend largely upon the country in which the data subject was domiciled.

6. CONCLUSION

Though comparative studies are based on precarious foundations, they are exciting. Data protection is a matter of international discussion. The outline of an international "data protection law" may be seen emerging

[68] Cf. Bing 1979*c*, p. 47.

through the efforts of such bodies as the Council of Europe, the OECD and the European Research Foundation.

Conflict between legal systems and jurisdictions will certainly arise from the increased transnational data traffic. Even within the homogeneous societies of the Scandinavian countries, the legislation varies. As I have attempted to illustrate, these variations may have a common theme, but within that theme there are certainly characteristic and national chords. Unless explored and actively tackled by the national data protection authorities, these chords may indeed turn into dischords which will create undesired problems for Scandinavian—and international—commerce and communications.

REFERENCES

Bing, Jon (1972), "Classification of personal information with respect to the sensitivity aspect", *Data Banks and Society,* Norwegian University Press, Oslo, pp. 98–141.

Bing, Jon (1977), "Data over alle grenser", *Data og personvern,* Ragnar Dag Blekeli & Knut S. Selmer (ed.), Norwegian University Press, Oslo, pp. 95–114.

Bing, Jon (1979*a*), "A comparative outline of privacy legislation", *Comparative Law Yearbook,* Sijthoff and Noordhoff, Alphen aan den Rijn, pp. 149–81.

Bing, Jon (1979*b*), "Personal data systems—a comparative perspective of a basic concept in privacy legislation", in Jon Bing and Knut S. Selmer (ed.), *A Decade of Computers and Law,* Norwegian University Press, Oslo, pp. 72 ff.

Bing, Jon (1979*c*), "The computer in private international law", *Computers, Contrasts & Law,* Online, Uxbridge, pp. 39–49.

Bogdan, Michael (1978), "Dataflykt över gränserna och den svenska datalagstiftningen", *Förvaltningsrättslig Tidskrift,* pp. 1–26.

Freese, Jan (1976), *Data och livskvalitet,* Publica, Stockholm.

Freese, Jan (1979), *Data över gränserna,* Studentlitteratur, Lund.

Jensen, Asbjørn (1978), "Kommentar", *Karnovs lovsamling,* Karnov, Copenhagen, pp. 4436–42.

L36 (1977–78), "Forslag til Lov om private registre m.v.", Folketinget, Copenhagen, October 13, 1977.

NOU 1975: 10, *Offentlige persondatasystem og personvern,* Politi- og justisdepartementet, Oslo.

Ot. prp. no. 2 (1977–78), *Om lov om personregistre m. m.*, Justisdepartementet, Oslo.

Prop. 1978/79: 109, *Ändring i datalagen,* Justitiedepartementet, Stockholm.

Report (1978) *of the Committee on Data Protection,* HMSO, London.

Seipel, Peter (1974), "Legal controls of the storage and use of personal data", *Data* no. 5, pp. 43–6, reprinted in *Utvalgte emner i jus og EDB,* Tor Hafli (ed.), Norwegian Research Center for Computers and Law, Oslo 1976, pp. 51–65.

Seipel, Peter (1975), *ADB och juridik,* Finansdepartementet, Stockholm.

SOU 1978: 54, *Personregister – datorer – integritet,* Datalagstiftningskommittén, Stockholm.

Transnational Data Report, Washington, cited *TDR* (1978).