International Journal of Communications Law and Policy
Issue 2, Winter 1998/99

THE "ANONYMISATION" OF THE TRANSACTION AND ITS IMPACT ON LEGAL PROBLEMS

A THEORY AS TO WHY THE USE OF ICT ENGENDERS LEGAL PROBLEMS*

by

Joachim Benno *

A. Introduction

The need for adaptability of legal consequences forms a consistent theme in the changes attending the dynamic development and use of technology. Most traditional areas of the law are affected, often by common and at the same time overarching problems which can disturb basic structures of the legal system. Critics are often heard to say that the legislator is not keeping up with developments and that current law stands in the way of efficient utilisation of the potentialities of technology. Others point to the need for reflection and to the dangers of a development in which the legislator under pressure takes precipitated action on the basis of inadequate supportive documentation. There are also those who maintain that the legislator ought as far as possible to remain passive and instead allow the players in the market to solve, through self-regulation, the problems arising.

The emergence of the information society confronts the legislator with challenges of apparently unprecedented extent and complexity. At the centre of it all we have the Information and Communication Technology (ICT), not only as the motive force of development and of the possibilities which the information society affords, but also as a factor generating the legal problems which have to be dealt with. In most cases this is a matter, not of new, unregulated legal phenomena but of existing ones where current law is becoming incapable of serving its intended purpose when ICT is used.

The purpose of this article is to discuss *why* the use of ICT engenders legal problems. It demonstrates the possibility of pointing to common factors in this respect and of describing these factors as "anonymising" the transaction, or in other words making it more difficult both for the

---

* This article is an updated and slightly changed version of the IT Law Observatory report 6/98. This and other reports can be ordered from The IT Law Observatory, The Swedish IT Commission, SE-103 33 Stockholm, Sweden (http://www.itkommissionen.se/observ/engel.htm).

* Member of the IT Law Observatory (a working group under the Swedish IT Commission) and Principal Secretary to the Swedish Committee on Media Convergence (http://www.konvergensutredningen.org). E-mail: joachim.benno@culture.ministry.se.

parties themselves and for legislators and judicial practice to understand and deal with the transaction and its environment. Concrete and more general examples are given, and ways are discussed in which the phenomenon of "anonymisation" can be coped with.

> In the present account, the term "transaction" is used in the broad sense, so as also to include unilateral acts and activities, such as criminal acts and situations where somebody uses a freely accessible database in order to transmit or collect information, without necessarily entering into a contractual relationship with the provider of the database. Concerning the use of the term "anonymisation" in this context, see the following section.

B. The difference between "traditional" and "new" ways of conducting various transactions

One fundamental reason why existing law is to such a great extent losing its capacity for dealing with situations where ICT is used, is that ICT is creating new ways of performing transactions of different kinds and at the same time is transforming the environment in which those transactions take place:

The contours of the transaction are being dissolved and the difference between different types of transaction is becoming blurred. In addition, transaction time inputs are diminishing and geographical distance is ceasing to matter. Ordering goods and services, carrying out banking transactions, making travel and other ticket reservations, collecting and passing on information - all these things, and much else besides, can now be done through one and the same medium, from one and the same position, without the parties involved needing to move from A to B or meet face to face.

Another way of describing this is by saying that ICT is transforming the characteristics of the transaction, and entities such as *time* and *space*, as determinants of the perception and performance of different types of transaction.[1] Because these changes are making ICT-assisted transactions more difficult to trace, identify and distinguish, compared with "traditional" ways of performing transactions of different kinds, I have chosen to describe this phenomenon as "anonymising" the transaction.

> As with the term "transaction" (see the preceding section), this article employs the term "anonymisation" in a broader sense than is commonly the case. "Anonymisation" is used to describe, not only effects making the identification and description of a subject more difficult but a whole phenomenon as such, in which the difficulty of identifying and describing the subjects involved is one of several elements which have to be taken into consideration. The conjugated forms "anonym-isation" and "anonym-ise" of the word "anonymous" describe a change in relation to what has gone before, meaning, in the present context, the change which the use of ICT entails in relation to "traditional" ways of conducting transactions of various kinds. Even if this use of the term does not fully accord with its true meaning and common usage, I feel that it

---

1 Cf. Burkert, H.: "Which Law for the European Information Society?" (text of a presentation given at the EC Information Day for senior executives of IEPRC, ICRT and EPC Brussels, 31st January 1996), http://www.gmd.de/People/Herbert.Burkert/Brussels.html (as of 16th March 1998 at 10:47 am). Burkert describes these aspects in the way that ICT invites – by its basic characteristics – uses that seek to overcome the limitations of time, complexity, quantity, space and physical representation, and that it does so in a manner that makes the process appear to the user as intangible, invisible and variable.

serves an important purpose by enabling us to summarise a complex reasoning in a word which, in these declensions, is not often used, is easy to remember and, as used in this context, not alter the description but only *enlarges* the matter of description. (The characteristics of anonymisation are the same but, instead of being confined to the description of subjects include an entire phenomenon as such.)

C. Anonymisation and its consequences in a legal perspective[2]

To appreciate the import of anonymisation for the legal problems arising when ICT is used, one has to consider its consequences for the users, legislators and judicial practice, in relation to the framing and intended purpose of a legal rule.

I. Consequences for the users, legislators and judicial practice

The consequences of the transaction being anonymised for the users are manifested through less knowledge of the transaction as such and of its various elements. These effects are accentuated by the problems of knowledge and understanding already entailed by the technology underlying the transaction.

In more concrete terms, use of ICT can make it more difficult to distinguish between different types of transaction which, previously, demanded more distinct and distinguishable measures. That which, in reality, would seem a manifest impropriety to the individual becomes more difficult to distinguish in an electronic environment. The connection between act and consequence becomes less clear and the borderline of the impermissible therefore becomes easier to transgress, both deliberately and inadvertently. Appropriating other people's banking assets through the Internet by cracking their PIN codes, for example, is probably a lower moral threshold to cross than the physical act of breaking into or robbing a bank. Then again, it is probably impossible for the uninitiated web surfer to perceive the borderline between proper and improper use of copyright material available through the Internet. Perhaps he or she does not even realise that an act entails the copying of copyright material, comparable to the manifest act of copying a book from end to end and producing, with a copying machine, a certain number of copies for further distribution.

Anonymisation can also make it more difficult to tell what is required in order for an act to be completed, and thus legally binding. This can apply both to commercial transactions, for example when entering into a contractual relationship, and to the relationship between public authorities and private individuals, for example concerning the date when a document is deemed to have been received. Even though legal rules, case law and custom indicate certain elements as determinant in these respects, it can be unclear to the parties concerned *when* these elements occur in an electronic environment and, moreover, how evidence of their occurrence can be secured and presented.

---

[2] The theory of the transaction being "anonymised" is based on the analysis in Benno, J.: Consumer Purchases through Telecommunications in Europe - Application of Private International Law to Cross-Border Contractual Disputes, CompLex 4/93 (Oslo: Tano, 1993), see especially pp. 117-122. See also ibid.: Burkert is here discussing the relation between ICT's properties and its impact on the individual person's perception of different processes and the structure of current law.

Another consequence is that it becomes more difficult to identify the other party and to decide in what capacity and with what authority he or she is acting - for example, whether the opposite number is the person he or she professes to be, is acting in a consumer capacity, has due authorisation (e.g. power of attorney), is over a certain age, and so on.

Another aspect is that, in connection with "traditionally" performed transactions, the individual can normally be expected to be in reasonably good control of the information which he or she provides, whether directly or indirectly, and reasonably able to decide who receives that information and in what way. The opposite applies to electronic transactions, the individual often being entirely unaware of the "electronic track" which he or she leaves behind him and, consequently, of the person or persons to whom these tracks become accessible.[3]

To this are added the changes, already mentioned, of *time* and *space* as determinants of the performance and perception of the transaction. Everything happens faster, the margins for reflection and consideration are diminishing, with a growing risk of rights being lost. Geographical distances are losing their practical relevance, and it is becoming less and less easy to ascertain the location from which a party trades or carries on his business, or the geographical source of information.

The problems which anonymisation creates for legislators and judicial practice are to a great extent matched by the problems described above in relation to the individual, but of course in terms of the perspectives and tasks of these institutions: the transaction and its parties are growing more difficult to trace, identify, define, classify and characterise, which poses problems both in the development of new legal rules and in the modification and implementation of existing law. Allowance also has to be made for the fact that, since the design of the regulatory structure and its implementation are to a great extent based on the possibilities of the individual understanding the transaction and its environment, the legislator and judicial practice must also relate to the problems which anonymisation presents to the individual.

The difficulties of understanding the underlying technology and its impact on time and space also accentuate the effects of anonymisation at this level. In addition, the legislator and judicial practice must also relate to the insensitivity of technology to political boundaries, the very boundaries which impose restrictions on their possibilities of action.

II. The framing and purpose of a legal rule

In order, however, to understand the legal problems entailed by the use of ICT, it is not sufficient to view anonymisation and its consequences for users, legislators and judicial practice in isolation. These effects also have to be related to the design and purpose of the legal rules applicable to the situations concerned.

Here, on closer analysis, one finds that the purposes to be served, the interest or interests to be protected or reconciled, are very often represented by the very criteria which are hard hit by anonymisation: criteria based on the possibilities of the parties understanding and foreseeing the

---

3 Further to the subject of "electronic tracks", see Bing, J.: *Personvern i faresonen* (Oslo: Cappelen, 1991), pp. 64-76.

transaction, its scope and consequences, as well as its positioning in time and space, and so on. Consequently, the criteria laid down in a legal rule lose their relevance for the accomplishment of that rule's purpose.

In the light of the above discussion and of the examples given in the sections which follow, we find that anonymisation impacts above all on knowledge and perception of:

- **Who** (which person or persons) are involved in the transaction or commit a criminal act, and in what capacity that person or persons act.
- **What** constitutes the object of the transaction/protection and how this is to be classified, defined and delimited, e.g. in relation to various types of exclusive rights and to data collections of importance for personal privacy.
- **Where** the transaction/criminal act takes place, where the effect occurs, where the party/culprit acts from, where the information originates and is supplied from, where a party can be deemed to be established, and so on.
- **When** an activity has legal consequences: when a legal commitment occurs, when a document is to be deemed to have been received, and so on.
- **How** the transaction and its various stages are performed, how evidence is presented and evaluated in these respects.

The following section contains a number of concrete examples of bodies of rules, actual or proposed, where the use of ICT, because of the transaction being anonymised, raises a variety of questions and problems. More generalised examples are also given from various legal fields and contexts.

D. SOME CONCRETE EXAMPLES

I. The Rome, Brussels and Lugano conventions - applicable law and jurisdiction4

The 1980 Rome Convention deals with the question of the law applicable to contractual obligations.[5] The fact of this often being referred to as an EC convention must not be misunderstood. It is not a legislative act passed by the law-making bodies of the EC, but a convention to which each of the Member States is a contracting party. The same applies to the Brussels Convention (1968) on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters.[6] Both the Rome Convention and the Brussels Convention, however, are regarded as important instruments in the process of European integration and are to be viewed in this light. Accession to these

4 The legal problems generated in these connections are further analysed in Benno. J.: *supra* n. 2, see especially pp. 78-113.

5 *OJ* 1980, L 266/1, The Rome Convention on the Law Applicable to Contractual Obligations.

6 *OJ* 1978, L 304/77, the Brussels Convention on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters.

conventions, accordingly, is stipulated for new Member States. The Lugano Convention is the counterpart of the Brussels Convention, extending its scope to include the EFTA countries.[7]

The following example focuses on Article 5 of the Rome Convention concerning the law applicable to consumer contracts. The content of this article corresponds in all essentials to Article 13 of the Brussels and Lugano Conventions, to which, accordingly, the same argument applies.

Article 5 is prompted by the need to protect weaker parties in contractual relations, which in this connection is manifested by the consumer being assured of the implementation of the consumer legislation of the country where he or she resides. This provision is relatively complex, but basically it lays down the following criteria for the consumer to be able to plead the consumer protection rules of "his own" country: [8]

- That the contract is to be regarded as a consumer contract, i.e. refers to the supply of goods or services to a person (the consumer) for a purpose which can be regarded as being outside his trade or profession.
- That the invitation/advertising took place *in* the country where the consumer resides, and that he took, *in* that country, the steps necessary for the conclusion of the contract, *or*
- that the other party, or his agent, received the consumer's order *in* that country.

It follows that this provision does not apply to all consumer agreements but is restricted to situations where activities vital to the contractual relationship took place in the country where the consumer has his "habitual residence".

Neither the text of the convention nor the report by Giuliano/Lagarde[9], normally used for interpreting the provisions of the convention, explains the choice of this criterion for limiting the applicability of the article. Some guidance is offered, however, by Jenard's report on the Brussels Convention[10], which states that the provision concerning jurisdiction over consumer contracts is intended to include transactions having a sufficiently strong connection with the country where the consumer has his habitual residence. This does not fully answer the question, but it seems reasonable to assume, on this basis, that the connection criterion is partly intended to represent what is seen by the parties as a strong connection and can thus be justified by the parties' expectations and their demands of predictability.

---

7 *OJ* 1988, L 319/9, the Lugano Convention on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters

8 For the full text of Article 5, see App. 1.

9 *OJ* 1980, C 282/1, Report on the [Rome] Convention on the Law Applicable to Con-tractual Obligations (Giuliano, M., and Lagarde, P.).

10 *OJ* 1979, C 59/1, Report on the [Brussels] Convention on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters (Jenard, P.).

Allowing the choice of applicable law in relation to "traditional" modes of transaction to hinge on the territory in which each party has acted may seem a natural balance between the interests of the seller and the consumer: as long as the consumer acts in the home market, he or she must be able to rely on the rules applying there, at the same time as it must be clear that the opposite applies, for example, to purchases where the consumer is abroad, and conversely in the seller's case.

When ICT is used, however, this criterion loses its relevance as a determinant factor for maintaining a balance of interests between seller and consumer. Where the invitation/advertisement takes place, technically speaking, is irrelevant to the ability of the parties to go through with the transaction. It can even be less worry and, moreover, cheaper for the consumer to order a product on the Internet than to go to the shopping centre "round the corner" in search of the same commodity - regardless of whether the consumer replied to an invitation which he or she downloaded from a database somewhere in Europe, the USA or Asia. There need not even have been anything to show the technically uninitiated consumer where the invitation/advertisement "took place" or from where the goods are going to be delivered. A Swede ordering a product from a web site where the language options include Swedish and the price is stated in kronor would thus be unable, the database posting the home page being located, say, in Ireland, to count on Swedish consumer law being applicable.

Thus the implementation of Article 5 may lead to results which are arbitrary, are difficult for the consumer to understand and thus can hardly be said to reflect the intended balance of interests between the parties. One way of solving the problem might be instead to make the decisive factor the country to which the invitation/advertisement was, or can be deemed to have been *directed.* It would then be possible to take into consideration various elements of the concrete situation which, with consumer interests in mind, indicate the place with which the contract has its closest connection.[11]

> As the Rome Convention is now incorporated with Swedish law,[12] and as Swedish marketing law applies to all marketing *directed* at a Swedish public,[13] the result may be that Swedish law is applied to the content of the invitation/advertisement but not to the consumer contract, based on the same advertisement.

Another problem arising in this connection concerns the prerequisites for the transaction being classed as a consumer transaction in the first place. Although the wording of the article does not show as much, it follows from the Giuliano/Lagarde report that the Convention protects the

---

11 Benno, J.: *supra* n. 2, pp. 124-126.

12 The Act incorporating the Rome Convention with Swedish law, "lag (1998:167) om tillämplig lag för avtalsförpliktelser", entered into force on 1st July 1998. The problems discussed in this section are not remarked on in the *travaux préparatoires* to this Act: See prop. 1997/98:14, *Romkonventionen – tillämplig lag för avtalsförpliktelser*, pp. 43-45, and the ministerial memorandum discussing the incorporation of the Rome Convention with Swedish law: Ds 1996:7, *Romkonventionen - införlivande med svensk rätt av EG-konventionen om tillämplig lag för avtalsförpliktelser*, pp. 42-44 and 80-84.

13 Cf. MD 1989:6 (the Swedish Market Court), see also Lindberg, A.: "Vilka regler gäller för marknadsföring på Internet?" in *Dagens IT*, 8th April 1997, p. 14.

good faith of the seller.[14] This means that Article 5 is only to apply if the seller knew or, having due regard to all the circumstances, should have known, that the other party was acting in a consumer capacity.

Since, in open electronic systems with their extensively automated routines, there can seldom be any question of the seller having acquired a genuine knowledge of the other party before entering into the contract, it is more a question here of deciding, from the concrete situation, whether the seller should have been aware of this fact. One's first impulse here is to consider whether the object of the transaction is a typical consumer product or not. Several situations are, however, imaginable in which the type of product affords no reliable guidance - e.g. computer hardware and software used both privately and professionally - and so other factors also have to be taken into consideration, such as how and through what channels the product was marketed.[15]

The examples given in this section illustrate how concepts, workable in the context of "traditional" transactions, either fail to serve their purpose or demand a new understanding of the same transactions, when performed with ICT.

II. The EC Data Protection Directive

Whereas the main purpose of national data legislation is the protection of personal privacy, the main purpose of the EC Data Protection Directive[16] (the directive) is to abolish existing impediments to a free flow of personal data between the Member States. This is to be achieved by harmonising the national rules of the Member States as far as is possible. Thus the existing national regulatory structures are to be adapted or replaced in accordance with the directive. After this has been done, the Member States will no longer be able to plead considerations of individual privacy as an impediment to the transfer of personal data from one Member State to another.

According to the preamble to the directive, this process must not have the effect of weakening the original national protection of personal data, and this too must be the natural point of departure when assessing whether the safeguards of individual privacy will be affected by the directive being implemented.[17] In order for this aim to be achieved, the individual must be able to assert his rights to the same extent at international, EC level as at national level.

In this respect it may first be noted that the directive *de facto* provides scope for national differences in levels of protection when implementing its provisions. It is therefore possible, indeed likely, that, within the framework of the directive, the strength of safeguards for individual privacy

---

14 *OJ* 1980, C 282/1, *supra* n. 9, p. 23.

15 The problem is further analysed in Benno, J.: *supra* n. 2, pp. 78-84.

16 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

17 Cf. *ibid.*, recital (10) of the preamble: "Whereas the object of national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy...; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community."

will be seen to vary from one legal system to another. The main purpose of the directive being a free flow of personal data between the Member States, questions concerning applicable law and jurisdiction have a critical bearing on the way in which safeguards for individual privacy are affected by the implementation of the directive.

Article 4 of the directive contains provisions concerning the law to be applied to data processing coming under the directive.[18] These provisions also affect the questions of competent court and damages (Arts. 23-24) and, indirectly, the mandate of the supervisory authority (Art. 28). Under the main rule, the applicable law is that of the country where "the controller" is established.[19] The consequences for the individual can be illustrated by means of the following, hypothetical example (references to foreign law are also hypothetical):

> A Swedish person (A) is faced with a situation where he (or she) is refused credit by his Swedish opposite number (B) due to a credit report which (A) claims is incorrect. The company supplying the credit report is a credit assessment firm (C) established in France. This means that (A), in order to get the incorrect information put right, must comply with French law and petition a French court in any action for damages.
>
> This is hard for (A) to understand, for after all, he is in Sweden and is being refused credit by a Swedish company. What does France have to do with it? It makes absolutely no difference to (A) where (C) is established - be it in Sweden, France or anywhere else - the effect is the same. (B) for his part could equally well have obtained the credit information from a Swedish company, but chose (C) because their services are cheaper, which in turn is due to French fiscal law being more lenient. In fact (B) does not even know that (C) was a company established in France, because the credit information service is part of a whole package of corporate services provided by a German business service company.
>
> (A) is referred to the French company. Following obvious language difficulties, (A) finally manages to make himself understood. The French company, while regretting what has happened, state that they obtained their information from the highly respected British credit information company (X), and that French law requires (A) to prove that the information is incorrect. (A) sends an excerpt from a Swedish register, translated and attested by a French friend. The French company, however, does not accept the excerpt, on the grounds that its relevance to an amendment of the information cannot be deemed verified, and until this has happened, French law being what it is, no changes can be made which are liable to impair the quality of the data. Time passes and (A) is confronted over and over again with the incorrect information in situations requiring a credit assessment.
>
> (A) has now finally realised that some support is obtainable from the Swedish Data Inspection Board (DI). DI has no mandate in relation to the French company, has no procedural capacity for representing (A) in French legal proceedings, is not, at first, acquainted with the details of French law, but is able, under the directive, to ask the French supervisory authority for assistance (Article 28 (6), second paragraph). Despite good contacts between the authorities, however, this takes time, partly because the French legislation, within the framework of the directive, differs in certain respects from Sweden's. Eventually, though, after still further problems due to the incorrect information being circulated, the data entry is corrected by (C). It now only remains for (A) to

---

18 The full text of Article 4 is to be found in App. 2.

19 Cf. Article 4 and recital (18) of the preamble: "Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State..."

> try to find out whether, and if so how, he can obtain compensation in France for the damage he has suffered as a result of the incorrect information. We offer (A) our best wishes...

Thus the rules of the directive can mean the individual finding himself in situations where he (or she) has to plead foreign law and approach foreign authorities for the assertion of his rights. And this in spite of the effect of the data processing occurring in the Member State where he has his residence. In addition, it is not certain that the national rights of which the individual is assured under his own country's law agree with current law where the controller is established. It must be hard for the individual to understand these consequences, and especially why, when he himself is affected in his own country, his ability to assert his rights must depend on where the controller is established.

One relevant question here is whether the party making use of an item of information, such as the Sweden-established company (B) in the above example, can be liable as "controller". If so, (A) could plead Swedish law on these grounds in order to assert his rights. It follows, however, from the directive and from the new Swedish Personal Data Protection Act[20] that the "controller" is the person who, alone or together with others, *determines* the purposes and means of the processing of personal data.[21] The Swedish Governmental Data Act Committee (the Data Act Committee) pronounces as follows:

> "...The characteristic here is that somebody is entitled to gain access to the information and, for example, to search it, but not independently to alter, supplement or erase the data. There is, in our opinion, much to be said for the person who has only this limited access to the data not being deemed to have such a power of determination over the purposes and means of the processing that he or she can be deemed controller."[22]

This being so, (B) in the above example can hardly be regarded as controller, and this seems natural in view of the very fact that (B) would not be in a position to amend the incorrect information.

It is not apparent from the directive why the question of applicable law and jurisdiction has been made to hinge on the establishment criterion. Our example shows, however, that the criterion cannot be deemed to promote the aim stated in the preamble (at least not in relation to individuals domiciled in Sweden), namely that implementation of the directive must not lead to a weakening of the original national protection for personal information.

One alternative to the establishment criterion may be to focus on the place where the effect occurs, which would seem to be more in keeping with what the individual can expect in a particular situation. Considering, however, that anonymisation affects, not only the subject of the data but also the controller - his expectations and possibilities of understanding and predicting the situation - the effect criterion may possibly be considered to imply an unfair shift in the balance of interests in this respect as well. That, however, may be counteracted by combining the effect criterion with an objective assessment as to whether the effect occurring was a natural part of the controller's

---

20 Personuppgiftslag (1998:204); the new Act entered into force on 24th October 1998.

21 Article 2 of the directive and Article 3 of the new Personal Data Protection Act, *ibid.*.

22 SOU 1997:39, Integritet, offentlighet och informationsteknik, p. 334. (Freely translated)

activity or whether the controller at all events should have considered that there was a danger in that direction. Failing this, an alternative could be to fall back on the establishment criterion.

This example illustrates how the anonymisation of the transaction affects the knowledge and expectations of the parties and creates problems for the legislators in finding appropriate criteria for the achievement of a certain purpose, e.g. that of maintaining an intended balance of interests appropriate to this knowledge and these expectations.

> The Data Act Committee did not comment on these problems in its report (SOU 1997:39). It is, however, remarked in the *travaux préparatoires* to the new Swedish Personal Data Protection Act, that Article 4 of the directive is hard to construe and that any questions in this respect will have to be resolved within the committee set up under Article 31 of the directive.[23]

III. The report of the Swedish Governmental Committee on Electronic Document Management (the IT Committee)

The report raises several legal problems connected with the use of ICT.[24] As part of its remit, the IT Committee[25] (the Committee), was among other things required to solve legal problems arising in relation to bulletin board systems (BBS). Bulletin board systems, quite simply, are electronic notice boards where large groups of users can read each other's messages and add messages of their own. Out of consideration, however, for technical development and, accordingly, the necessity of not confining oneself to a single type of service, the Committee chose to treat these problems under the wider heading of "electronic mediation services", a general term for services whereby the user can receive information or transmit it to others.[26]

One problem that the Committee had to consider was that of balancing the interests of personal privacy against freedom of expression and information: electronic mediation services are an important medium for the free exchange of opinions, at the same time as current data protection legislation, for the sake of personal privacy, makes stipulations which can limit the use of these services (as does the new Swedish Personal Data Protection Act, which is based on the EC Data Protection Directive, see previous section). The legislation that was proposed by the Committee on electronic mediation services contained in this respect an exception to the former Data Protection Act[27], worded as follows:

> Section 2
>
> The provisions of Sections 1-20 and 22-25 of the Data Protection Act (1973:289) shall not apply to personal data files included in a service referred to in this Act, insofar as
>
> 1. the file only contains continuous text and particulars of messages and users, and

---

23 Prop. 1997/98:44, *Personuppgiftslag,* p. 55.

24 SOU 1996:40, Elektronisk dokumenthantering.

25 "IT-utredningen" not to be confused with the Swedish IT Commission ("IT-kommissionen").

26 SOU 1996:40, *supra* n. 24, pp. 143-147, 173-174 and 177-178.

27 Datalag (1973:289).

2. the file is kept so as to enable the users to transmit or collect information for a free exchange of opinion, free and multifaceted ("allsidig") information or free artistic creativity.

The term "continuous text" refers to information which has not been structured in such a way as to facilitate the searching of personal data.[28]

There are several themes of discussion, some of them concerned with legislative technique, where this proposed provision is concerned. For present purposes, however, we will concentrate on the choice of the term "continuous text" as one of several criteria for waiving the Data Protection Act. The Committee's argument for using the term "continuous text" was that text of this kind differs from a *file* (or register) in that it has not been structured to facilitate the searching of personal data. The investigator of the Committee wrote:

"Continuous text should thus be taken to mean ordinary free text not having a structure which makes it easy for many data about a particular person or a certain type of data about many persons to be automatically compiled and processed. Even if continuous text of this kind can be processed with a view to personal data, for example by using a name as a search concept, the text is not a register in the true sense, because it has not been structured in such a way as to facilitate the searching of personal data. The interpretation of such a text requires human beings...

"On the other hand, text which is prepared so as to be easily convertible to structured form or otherwise used as if it were structured should not come within the scope of the continuous text concept which I propose."[29]

The Committee's proposals are to be seen against the background of the former data protection legislation, which focused on the register concept. In order to exclude certain types of data collection from the scope of the Data Protection Act - which among other things meant the requirement of a license - the Swedish Data Inspection Board made a practice of using the term "continuous text". The problem, however, is that present-day technology is already making the distinction between continuous text and register less relevant. The possibility of variously compiling and processing personal data does not hinge any more on whether a text can be characterised as continuous or not, nor on whether or not a text has been structured so as to facilitate the searching of personal data.

The handling of personal data is not a new phenomenon, but the way in which it is done has changed with the passing of time. During the 1960s and 1970s, "data technology" developed into a powerful tool with which national authorities, among others, were able to process personal data more efficiently than before. This contributed towards the identification of a special need for the protection of personal privacy, manifested among other things by the passing of Sweden's Data Protection Act, at the beginning of the 1970s. The reference at that time was to clearly delimited and defined collections of information in the form of computer files, and so it was natural for the legislation to focus on these as an object of regulation; the processing of personal information, with the danger it implied to personal privacy, could be linked directly to a particular register as such.

Subsequent ICT developments have gradually resulted in more and more advanced ways of processing information. The transaction as such has become "anonymised" and the context of the

---

28 Freely translated.

29 SOU 1996:40, *supra* n. 24, p. 166. (Freely translated)

threat to personal privacy has thus changed: the risk of intrusive use of technology has grown, at the same time as it has become more difficult to foresee, trace, define and classify. It has gradually become obvious that the register concept is losing its importance as a *delimiting* concept to indicate when privacy-threatening processing of personal data may occur.

It is still relevant, of course, to focus attention on data files - they are still being used and developed for the processing of personal information - but now that the file structure is no longer a prerequisite of quickly retrieving and manipulating privacy-threatening information, it is no longer the quality of file (register) as such that calls for legislative attention, but rather a general vigilance against the privacy-threatening handling of personal information in any form.

It is in this perspective that the Committee's proposal of "continuous text" as a delimiting criterion in relation to registers shall be seen. By suggesting this exception to the former Data Protection Act, the Committee intended to eliminate obstacles to a free exchange of opinion.[30] It is unclear whether, to this end, an effort was made to sustain the balance of interests aimed at in the former data protection legislation, or whether the view was taken that development has necessitated an elucidation and/or a shift of the balance in favour of the freedoms of expression and information. Whatever the intention, however, the choice of the "continuous text" concept was questionable as it is technically limited and suggests a practical difference between continuous text and registers: a distinction which may still be relevant in certain situations but which technical progress has already made less important and will go on doing so, to such an extent that it is doubtful whether in future, any useful purpose can be served, in a legal perspective, by speaking in such terms.

This example highlights the problems which the anonymisation poses in the pursuit of appropriate concepts for the attainment of a certain purpose, in the present instance that of eliminating impediments to a free exchange of opinion, with due regard for considerations of personal privacy.

> Since the original report underlying this article was written, the Swedish Riksdag has passed a new Act on the responsibility for electronic bulletin board systems ("Lag (1998:112) om ansvar för elektroniska anslagstavlor"), effective from 1st May 1998. The new Act does not include the provision treated here, restricting the scope of the former Data Protection Act. The reason being, according to the *travaux préparatoires*, that an exception of such a kind will have to be analysed more closely in relation to the new Personal Data Protection Act and the underlying EC Directive.[31]

E. Overarching examples from different branches of the law and in various connections

Just as with the examples given in the previous sections, the anonymisation is a fundamental element of many of the ICT related legal problems occurring in other connections. These problems can be related both to special fields of the law and to the particular contexts in which they appear.

---

30 *Ibid.*, p. 164 ff.

31 Prop. 1997/98:15, Ansvar för elektroniska anslagstavlor, p. 22.

A number of more general examples of this are given below, showing among other things that there are clear connections between the problems occurring in traditionally different areas of the law.

I. Freedom of expression and information, copyright, penal law and protection of privacy

The problems occurring in the fields of copyright, penal law, personal data protection and freedom of expression and information are mainly concerned with the balancing of contrary interests and the way in which this balance is to be expressed in the text of the law. This includes, for example, the question of how certain actions are to be described and classified in order to be capable of having legal consequences which the individual can identify, understand and foresee - consequences, both for the person performing the action and for the party who is adversely affected and/or can assert rights and liberties by virtue of the statutory provision. To this are added the difficulties, when exacting liability, of identifying who has performed a certain action and the problem of where the action and its effect can be deemed to have occurred as determinant factors in matters of applicable law and jurisdiction. This latter point can be further related to the difficulties of producing evidence, concerning, for example, performer, act and place, due to the evidence consisting of electronic tracks which are evanescent and easy to manipulate.

On the subject of copyright, special attention can be drawn to the problems entailed by a copyright work being divorced from its materially distinguishable carrier in an electronic environment. The integration of sound, text and image in multimedia applications is causing the traditional work categories in copyright to amalgamate, making them hard to distinguish from each other, which further accentuates the problems already described above.[32]

II. Mercantile and taxation law - the distinction between "product" and "service" etc.

One problem in the field of mercantile law concerns the distinction between "product" and "service" in an electronic environment.[33] Does the Swedish Sale of Goods Act[34] apply to purchases of software when both the software and manuals are delivered electronically, on the Internet? If the object of the contract in this instance is to be regarded as a service, the transaction comes outside the scope of the named Act. At the same time, the corresponding purchase in a computer shop, with the software packaged and stored, say, on a diskette or CD-ROM and accompanied by a printed manual, would come within the scope of the law. A corresponding question arises, for example, concerning the electronic ordering and delivery of music or moving pictures (cf. video on demand), when the buyer also pays for the right to make his own copy of the work on a CD or videocassette. Is the Sale of Goods Act applicable to cases like these? If the customer were to buy a

---

32 See, for example, Seipel, P.: *Juristen och datorn* (Stockholm: Fritzes, 1994, 5th ed.), pp. 167-168, and Smith, G.J.H. (Ed.): *Internet Law and Regulation* (London, FT Law & Tax, 1996), pp. 20-21.

33 Cf. Smith, G.J.H. (Ed.): *ibid.*, pp. 139-140.

34 Köplag (1990:931).

CD or a videocassette ready-made with the same content in a shop, there would be no doubt as to the applicability of the Sale of Goods Act.

At this point we can ask ourselves whether it is reasonable to make the applicability of the Sale of Goods Act depend on whether it is the seller who supplies the information on a certain medium or whether the purchaser himself provides the storage on a medium of his own choosing. What is reasonable in view of the parties' expectations of the transaction, e.g. in relation to a consumer who, one week, buys game and word processing programs and an Internet subscription in a computer store and then, a fortnight later, orders an electronic reference work and an updated version of the word processing program, both of which are delivered over the Internet?

The distinction between "product" and "service" and the way in which these concepts are to be handled in an electronic environment can also have fiscal consequences, e.g. with regard to the levying of value added tax and import and export duties, and in the question of which country these taxes are to be imposed in.[35] Another problem area relating to tax law concerns imaginary or virtual organisations (see below) and the question of where, for taxation purposes, an activity can be deemed to be established.[36]

III. Contract law

In the field of contract law, the most prominent questions concern the contractual mechanism and concepts and principles connected with it, e.g. when an agreement which is binding upon the parties has come about, when and how invitation and acceptance respectively can be revoked, where an agreement can be deemed to have been entered into, how the various stages of the contractual mechanism can be produced as evidence. To this are added more overarching questions, such as that of how the theory of the contract as expressing a declaration of intent is to be handled with regard to automated processes, such as EDI systems and electronic agents, and also how the doctrine of contractual preconditions is affected by the transaction being anonymised.

IV. Imaginary/virtual organisations

Another field in which legal problems arise concerns the possibilities which ICT creates of organising both public and private operations and their activities. Reference is often made to "imaginary" or "virtual" organisations, distributed work forms, teleworking etc. In his article "Imaginära organisationer, reell juridik" (Imaginary organisations, real law), Seipel describes a problem area which corroborates the view of anonymisation as a central underlying factor in this connection.[37] Among other things, Seipel offers the following reflection:

> "The question is whether the overall verdict on IT and organisations must not be made to focus on IT's capacity for dissolving limits of many kinds, namely limits dictated by physical distance, physical presence, loca-

35 Smith, G.J.H. (Ed.): *supra* n. 32, pp. 139-144.

36 Cf. *ibid.*, p. 145.

37 Seipel, P: "Imaginära orgainsationer, reell juridik", in Brinnen, M. (Ed.): *Nordisk Årsbok i Rättsinformatik* 1996 (Stockholm: Norstedts Juridik, 1996), pp. 67-80.

> tion etc., and also limits to accessible and manageable information (volume, frequency and nature), limits of possible follow-up, verification and control. At the same time, IT is imposing new limits and moving old ones. Competence in handling the new possibilities is required of the participants, thereby setting limits to their capacity - there are information haves and have-nots, not only in the world of individuals but in that of the organisations as well." [38]

The questions raised in this connection are complex and many-sided, and they span several traditional areas of the law, such as the law of association, public law, administrative law, labour law, insurance law and tax law. They concern, for example, what constitutes a legal person, its liabilities and outer limits, where an operation can be deemed to be established/registered, the line of demarcation between employee and contractor, the line of demarcation between public and private operations, the management of publicity and secrecy, the apportionment of responsibilities between employer and employee, the identification of tax objects and what is to be taxed.

V. The convergence between the data, tele-communications and media markets

As we have already seen, the digitalisation of information has blurred the boundaries between what used to be clearly distinguishable types of service. What is more, the services themselves can be conveyed "sideways", through infrastructures which used to be technically reserved for a particular kind of service. This has the effect of making it increasingly difficult to distinguish between what used to be the clearly separated IT, telecommunications and media markets. This is creating problems for the legislator, as these different markets have different codes of rules with different points of departure and different underlying motives: the unregulated IT market, which, on the basis of business and consumer policy incentives, is governed by market legislation; the telecommunications market, which is being liberalised in order to achieve effective competition for the achievement of particular aims of telecommunications policy; the media market, which is governed by democratic and cultural policy aims, and in which the State has taken upon itself a special public service responsibility in radio and television broadcasting.

The problems posed by convergence are apparent both at the detailed level of legislation, e.g. as regards the definition of and the distinction between different types of service (such as in relation to what is to be considered as private and public communication and specific regulation of the content of services and responsibility for that content), and on the more general plane, as regards the effects on the underlying political aims and their realisation, e.g. as regards public service, allocation of frequencies for private and public radio communications and the promotion of effective competition.

Typical questions on the detailed level are what shall be regarded as covered by the definitions of sound radio and television programmes, whether regulation of the content of radio and television services can be applied to services on the Internet, who in that case is to be regarded as the legally responsible publisher, whether it is at all possible and reasonable in the first place for this responsibility to be extended to the Internet environment and, if so, how it is to be defined. In this connection, the use of ICT has made it unclear what and who shall be included in the regulation

---

38 *Ibid.*, p. 72. (Freely translated)

and in what way these regulations are to be constructed for the achievement of one or more purposes (the subject and object to be regulated in relation to the underlying purpose).

> The Swedish Government has appointed a special investigator ("The Committee on Media Convergence") to study, among other things, the necessity, feasibility and implications for a co-ordination of the law relating to radio and television broadcasting and telecommunications activities. A report on the remit is to be presented on 28th February 1999.[39]

F. Measures to counteract and handle the anonymisation of the transaction

To cope with the effects of the transaction being anonymised, we first have to identify their impact in relation to the legal rule or the legal structure concerned and the purposes which that rule or structure is meant to achieve. This may, for example, lead to the conclusion that the intended balance of interests is not being maintained in the use of ICT. In certain situations this can also provide an incentive for discussing whether the balance of interests aimed for is still desirable, or whether there may be cause for a revaluation of earlier standpoints, e.g. in view of the changes entailed by the development of the information society. Whatever answer one arrives at, the next step will be to ascertain what measures are needed for the achievement of this purpose.

In many cases, the primary measure is to change/modify the design of a legal rule or a legal structure so that it will be able to meet the demands posed by the use of ICT. Among other things this means finding concepts and criteria which more appropriately manifest and build on the legal subject's justified expectations and knowledge regarding the transaction concerned; compare this, for example, with the discussion above concerning the use of alternative criteria in relation to the Rome Convention on the Law Applicable to Contractual Obligations and the EC Data Protection Directive.[40]

Measures of other kinds may be to reapportion and/or extend liability, e.g. when there are problems in identifying offenders (cf. the new Swedish Act concerning the responsibility for electronic bulletin board systems, discussed above), and to make stipulations concerning the actions of the parties, e.g. the seller's duty of information in connection with electronic trading.

Imposition of a duty of information is one example of a preventive measure which can augment subjective understanding of the transaction, and which at a later stage can also be an important aspect of interpretation when applying other legal rules. As an example we can take the EC Directive on consumer protection in connection with distance contracts.[41] Among other things this directive contains rules stipulating that the consumer shall be given prior information well in advance of a distance contract being entered into, and that, at an early stage of the completion of the contract, he or she shall receive written confirmation of that information.[42] This duty of information includes, among other things, the supplier's identity, the essential characteristics of the product or service and its price (including all taxes), right of cancellation etc.[43] Stipulations of this kind, and the way in which they are handled in the individual case, can serve as interpretative elements - re-

---

39 See http://www.konvergensutredningen.org

40 See *supra* 4.1 and 4.2.

garding, for example, the applicable law and jurisdiction - in deciding the legal system with which a transaction has its closest connection, e.g. to which geographical market an invitation is directed and what expectations the framing of the invitation may have given the consumer/other party concerned.

The duty of information can also be a prerequisite for the individual realising in the first place that a situation exists where he (or she) has rights to assert.[44] Thus it is relevant, from the viewpoint of personal privacy, to insist on the individual being informed when information about him is processed in various ways. This can relate, for example, to the possibility of recording the individual person's action on the Internet for marketing or other purposes. Often it is impossible for the individual to know when such recording takes place, and in the majority of cases the individual is doubtless unaware that, when surfing on the web, he leaves a host of "electronic tracks"[45] behind him which can be recorded and used for various purposes.[46] There is also the matter of an employer recording the employees' use of the firm's data communication system, partly in order to find out about any abuse or accessing of databases which, from the viewpoint of the employer (or the general public) are to be considered less suitable.[47] Accordingly, it is impossible, without knowing that recording takes place, to assert one's rights in relation to any abuses under existing data protection legislation.

However, part from what is discussed above, necessary measures also concern issues of a wider and more overarching scope, such as in the context of convergence between the data, telecommunications and media sectors. Here it is not just a question of the applicability of specific legal rules, but of basic legal structures which are disturbed by technological developments and consequently in need to be taken under consideration and possibly revaluated from the perspecitve of their underlying motives.

Furthermore, as already remarked, one central and overarching problem area concerns the international perspective. Especially notable are the difficulties of identifying applicable law and jurisdiction; these include the difficulties of finding criteria to indicate the legal system with which the transaction has its closest connection and which represents a reasonable balance between the interests of the parties and between other conflicting interests. To this is added the fact of ICT making it possible for enterprises and individuals, easily and at little expense, to act internationally

---

41 Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts.

42 Articles 4 and 5 respectively.

43 If, however, no advance payment is required, it is only in the written confirmation that the geographical address of the supplier's enterprise has to be stated.

44 Cf. SOU 1995:69, *Betaltjänster*, p. 64.

45 Cf. see Bing, J: *supra* n. 3, pp. 64-76.

46 See, for example, Smith, G.J.H. (Ed.): *supra* n. 32, p. 66.

47 Cf. Anita Sjöblom's articles "Regeringens surfande övervakas" in *Dagens Nyheter* (1997-04-08, Inrikes A 5) and "Nätsurfare kan granskas" in *Dagens Nyheter* (1997-04-14, Inrikes A 7).

without any previous experience of doing so. At the same time, the actual performance of the transaction seldom affords any guidance concerning its international character and can even be directly misleading in this respect. Consider, for example, electronic market places and web hotels, where links between different web pages can "toss" the user between databases in different parts of the world without this in any way being made clear to him.

Both here and in other connections, one of several possible measures may be to insist on "boundary markers" which clearly show the user when he or she is being linked between different databases. This can also make a difference to the liability which can be imposed on the provider of the service, e.g. in relation to web pages which he or she has links to but no control over.[48]

The difficulty of overcoming "the international problem" is not to be underrated. International co-operation and harmonisation of both national substantive law and national rules of appropriate law and jurisdiction is necessary, but often hard to achieve. As regards the framing of determinant criteria, these must be made less dependent on spatial elements which can lead to arbitrary and, in relation to the balance of interests aimed for, perplexing results. Examples already quoted concerning consumer contracts and protection of personal data show that in these connections and with regard to the purpose of regulation it may be more relevant to consider to which country an invitation/advertisement is directed and where the effects of data processing occur than where the invitation/advertisement took place and where the controller is established.

G. Conclusion and concluding reflections

I. The "anonymisation" of the transaction - a common denominator

The analysis in the preceding sections contains concrete examples of existing and proposed legal rules, the construction of which does not measure up to the demands which ICT is making on the legal system, e.g. as regards the framing of a legal rule or structure in relation to its purpose and individual opportunities of transactional insight and understanding. More general examples are also given of similar problems in various fields of the law. The analysis above shows that the root of the legal problems arising is to a great extent to be found in what I have chosen to describe as the transaction being "anonymised".

"Anonymisation" serves here to denote the element which is added by ICT in relation to traditional ways of performing various transactions and which also constitutes a common denominator of the legal problems arising. The possibility of pointing to a common denominator in this connection not only provides opportunities for better understanding the nature of the problems but also creates opportunities of problem-solving in a wider perspective, in which the solution in one area can also furnish guidance for solutions in other areas.

From this viewpoint we can go on to note that, in all the problems arising, in order to counteract and cope with the effects of anonymisation, attention has to be focused on the following questions:

---

48 Cf. Smith, G.J.H. (Ed): *supra* n. 32, p. 56.

- Who (party, culprit, subject for protection)?
- What (object of, respectively, transaction and protection)?
- Where (direction, effect, establishment, origin)?
- When (legal obligation)?
- How (the various stages of implementation, pleading and evaluation of evidence)?

and that these have to be viewed in relation to the end or ends in view - e.g. the balancing of opposite interests - and that awareness is needed of the international perspective, with a variety of legal systems involved.

II. Legislative technique

There are various legal techniques for tackling the problems posed by the anonymisation of the transaction. The examples and proposals discussed in this article suggest that in certain respects greater flexibility is needed in legislation, which among other things could mean less distinction and predictability. Not infrequently, however, such legislation is criticised as providing scope for arbitrary decision-making, reducing predictability and creating uncertainty about the legal position. In an article entitled "Rättsfrågor kring tjänster i nät" (Legal questions concerning services provided through networks), Wahlgren discusses, among other things, the rapid legislative changes necessitated by developments:

> "...Meeting such demands is not without its problems, and there are a number of qualitative aspects to be taken into consideration. A different working approach should not, for example, result in generally worded declarations of objectives or inexact general clauses - the development of a deeper perspective means more than just the development of a regulatory system based on more general concepts..." [49]

Basically I endorse this reflection. Generally worded statements of objectives and general clauses must not be a "cop out" in situations where the legislator is working against the clock and with inadequate supportive documentation. This does not augur for the quality of the result. The same goes for excessive reliance on the analogical method of interpretation as sufficient means of solving ICT related problems within the scope of current legislation.

On the other hand, I do not feel that this rules out the need for greater flexibility of legislation. I believe this to be a matter of necessity in many situations, at all events during the initial stages, in order to cope with the problems posed by the use of ICT (such as the transaction being anonymised). In time, as we come to understand and know more about ways of coping with legal problems related to ICT , the rules can in all probability be given a sharper focus. But until then it is important to have solutions which leave us free to consider special circumstances in the concrete case and which at the same time afford scope for the development of more exact principles in the process of interaction between legislator, judicial practice and market. In this way the codified law can become more dynamic and can grow within given frames which at the same time ensure stabil-

---

[49] Wahlgren, P: "Rättsfrågor kring tjänster i nät", in Brinnen, M. (Ed.): *Nordisk Årsbok i Rättsinformatik* 1996 (Stockholm, Norstedts Juridik, 1996), pp. 49-58, 53-54. (Freely translated)

ity: the continuity of legislation will be promoted, at the same time as the problem of rapidly obsolescent norms out of tune with technical progress can be counteracted. It is immensely important, however, that more flexible legislation should provide clear and steady frames within which the freer assessment is to take place and which are based on the interests which the current legal rule is meant to balance or safeguard. For greater predictability and as a form of guidance, these frames can very well be supplemented by non-exhaustive examples and presumptions.

This, in my opinion, is where the great challenge lies at present: the finding of appropriate and clear frames, possibly combined with presumptions. If this is achieved, the legal rules can contribute towards stability and sufficient predictability, while at the same time affording necessary scope for continuity in harmony with development. Having said this, however, I wish to underline the need, even within the framework of more flexible solutions, of developing clear concepts, definitions and distinctions and, of course, where possible against the background of qualitative input data, more closely defined legal rules.

In this process I believe that the theory of the transaction being "anonymised" can make an important contribution to the deeper understanding which Wahlgren calls for in order to meet the demands made by ICT on legislation:

> "...The purpose of a deeper perspective is above all to provide opportunities for more initiated discussions and more soundly based proposed solutions. In many fields, therefore, this can be just as much a question of looking up and perceiving the connection between different activities and different types of legal solution. This is something which can require far greater analytical inputs, because the material will be more extensive, but it is at the same time a method which can lead to far more uniform and appropriate solutions." [50]

III. The wider perspective - the anonymisation of development and events

The ongoing development of the information society is above all in the hands of the legislator and the market and the interaction between them. At the same time it is hard to see the manner in which this is happening and the underlying forces and currents which are at work. Some maintain that we are going through a process whereby real decision-making is being transferred from the politically elected assemblies to the multinational corporations and capital investors, for one thing because ICT gives the players in the market such opportunities for swift action and decision-making at global level that the political process has no alternative but to comply with their agenda. In his article "Software Procurement and International Trade in the 1990s", Johnson offers the following reflection, among others:

> "By default, we are witnessing a historic shift in the center of gravity of global economic decision-making away from national governments and toward international enterprises. Ironically, the 1980s legacy of deregulation and government preferences for market-oriented policies have helped speed that process.
>
> "This trend is further fuelled by the accelerating pace of technological change which continues to compress time. The time to innovate, to market, to deliver, to gather and use information have all been compressed dramatically. Businesses have been forced to adapt to the compression of time and other consequences of rapid technological change in order to remain competitive in world markets.

---

50 Ibid., p. 54. (Freely translated)

> "Government and their time-sensitive institutions and processes have not adapted. Legislative and regulatory changes take time..." [51]

The developments described here reflect the socially transforming character of ICT. The changes are making themselves felt at both macro and micro levels and are affecting the foundations of established social structures. The extent and complexity of the process make it still more difficult to arrive at a concerted picture of this development and its consequences; perhaps here one can speak of an anonymisation of *development* or *events* and its effect on social structures.

When facing the problems which ICT entails in the legal system, it is important that one should also consider these questions against the background of the perspective which has now been described; in this fundamental, overarching perspective, a transformation is taking place of the whole of the society in which the legal system is one of the pillars on which the social order rests. In democratic states, the foremost task of the legal system is to manifest and maintain the democratic ideals, and legislation is framed in conformity with those ideals. One of the greatest risks here is that the complexity and rapidity characterising the development of the information society will result in prevailing ethical and moral values being undermined and changed without any standpoints being consciously adopted. This is not to say that there can be no reason for a revaluation of prevailing views, but this must be done on the basis of a deliberate standpoint concerning the consequences which this can have for both democracy and the individual. Among other things this has to take place within the democratic process and with an open, initiated debate in which everyone has an opportunity of taking part.

Here the problem of knowledge stands out as perhaps the biggest challenge to be overcome in the development of the information society, namely that of counteracting and managing the anonymisation of development and events, so as to facilitate active civic participation in the democratic process.

---

51 Johnson, Richard, A.: "Software Procurement and International Trade in the 1990s", in Mosesson, Erik (Ed.): *Nordic Yearbook of Law and Informatics* (Stockholm: Norstedts Juridik, 1992), pp. 167-175, 168.

Bibliography, etc.

- Benno, Joachim: Consumer Purchases through Telecommunications in Europe — Application of Private International Law to Cross-Border Contractual Disputes, CompLex 4/93 (Oslo: Tano, 1993).
- Bing, Jon: *Personvern i faresonen* (Oslo: Cappelen, 1991).
- Brinnen, Martin (red): *Nordisk Årsbok i Rättsinformatik 1996* (Stockholm: Norstedts Juridik, 1996).
- Burkert, H.: "Which Law for the European Information Society?" (text of a presentation given at the EC Information Day for senior executives of IEPRC, ICRT and EPC Brussels, 31st January 1996), http://www.gmd.de/People/Herbert.Burkert/Brussels.html (as of 16th March 1998 at 10:47 am).
- Johnson, Richard A: "Software Procurement and International Trade in the 1990´s", in Mosesson, Erik (ed.): *Nordic Yearbook of Law and Informatics 1992* (Stockholm: Norstedts Juridik, 1992), pp. 167-175.
- Lindberg, Agne: "Vilka regler gäller för marknadsföring på Internet?" in *Dagens IT*, 8th April 1997, p. 14.
- Mosesson, Erik (ed.): *Nordic Yearbook of Law and Informatics 1992* (Stockholm: Norstedts Juridik, 1992).
- Seipel, Peter: *Juristen och datorn* (Stockholm: Fritzes, 1994, 5 ed.).
- Seipel, Peter: "Imaginära organisationer, reell juridik" i Brinnen, Martin (red): *Nordisk Årsbok i Rättsinformatik 1996* (Stockholm: Norstedts Juridik, 1996), pp. 67-80.
- Sjöblom, Anita: "Regeringens surfande övervakas" i *Dagens Nyheter*, 1997-04-08, Inrikes A 5.
- Sjöblom, Anita: "Nätsurfare kan granskas" in *Dagens Nyheter*, 14.4.97, Inrikes A 7.
- Smith, Graham JH (ed.): *Internet Law and Regulation* (London: FT Law & Tax, 1996).
- Wahlgren, Peter: "Rättsfrågor kring tjänster i nät" in Brinnen, Martin (ed.): *Nordisk Årsbok i Rättsinformatik 1996* (Stockholm: Norstedts Juridik, 1996), pp. 49-58.
- Datalag (1973:289)
- Köplag (1990:931)
- Lag (1998:112) om ansvar för elektroniska anslagstavlor
- Lag (1998:167) om tillämplig lag för avtalsförpliktelser

- Personuppgiftslag (1998:204)
- Prop. 1997/98:14, Romkonventionen – tillämplig lag för vtalsförpliktelser
- Prop. 1997/98:15, Ansvar för elektroniska anslagstavlor
- Prop. 1997/98:44, Personuppgiftslag
- SOU 1995:69, *Betaltjänster* (Slutbetänkande av Betaltjänstutredningen).
- SOU 1996:40, *Elektronisk dokumenthantering* (Betänkande av IT-utredningen).
- SOU 1997:39, Integritet, offentlighet och informationsteknik (Betänkande av Datalagskommittén).
- Ds 1996:7, Romkonventionen — införlivande med svensk rätt av EG-konventionen om tillämplig lag för avtalsförpliktelser.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts.
- *OJ* 1978, L 304/77, the Brussels Convention on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters.
- *OJ* 1979, C 59/1, Report on the [Brussels] Convention on jurisdiction and the enforcement of judgements in civil and commercial matters (Jenard, P).
- *OJ* 1980, L 266/1, The Rome Convention on the law applicable to contractual obligations.
- *OJ* 1980, C 282/1, Report on the [Rome] Convention on the law applicable to contractual obligations (Giuliano, M, and Lagarde, P).
- *OJ* 1988, L 319/9, the Lugano Convention on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters.

Appendix 1 The (1980) Rome Convention, Art. 5 concerning certain consumer contracts

1. This Article applies to a contract the object of which i sthe supply of goods or serivices to a person ("the consumer") for a purpose which can be regarded as being outside his trade or profession, or a contract for the provision of credit for that object

2. Notwithstanding the provisions of Article 3, a choice of law made by the parties shall not have the result of depriving the consumer of the protection afforded to him by the mandatory rules of the law of the country in which he has his habitual residence:

- if in that country the conclusion of the contract was preceded by a specific invitation addressed to him or by advertising, and he had taken in that country all the steps necessary on his part for the conclusion of the contract, or if the other party or his agent received the consumer´s order in that country, or
- if the contract is for the sale of goods and the consumer travelled from that country to another country and there gave his order, provided that the consumer´s journey was arranged by the seller for the purpose of inducing the consumer to buy.

3. Notwithstanding the provisions of Article 4, a contract to which this Article applies shall, in the absence of choice in accordance with Article 3, be governed by the law of the country in which th econsumer has his habitual residence if it is entered into in the circumstances described in paragraph 2 of this Article.

4. This Article shall not apply to:

- (a) a contract of carriage;
- (b) a contract for the supply of services where the serivces are to be supplied to the consumer exclusively in a country other than that in which he has his habitual residence.

5. Notwithstanding the provisions of paragraph 4, this Article shall apply to a contract which, for an inclusive price, provides for a combination of travel and accommodation.

Appendix 2 The EC Data Protection Directive, Art. 4 concerning the applicable law

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.