10

Electronic Document Exchange in Sweden — the legal aspects

Per Furberg
Associate Judge of Appeal
Pl. 9205
S-444 97 Svenshögen, SWEDEN
Phone/Fax +46 303 77 55 54
Mobile tel +46 10 206 25 32
E-mail per.furberg@mailbox.swipnet.se

Abstract

The legal issues which have arisen due to computer based handling of documents may be addressed by following the examples provided by the international standardisation of digital signatures and related services. A generally accepted definition of a digital document should be elaborated, founded upon the underlying legal principles and basic technical routines of electronic information handling. By these means questions concerning legal obstacles may be replaced by the creation of a legally unified regulation of traditional routines and IT-routines, with security maintained.

Keywords

Electronic record, digital document, legal aspects, public administration, electronic commerce.

1 INTRODUCTION

Swedish public administration and businesslife are extensively computerised. The main body of legislation in this area comes however from the 70's, when for example the Swedish Data Act and provisions in the Swedish constitution concerning public electronic records were introduced.

The Swedish Administrative Procedure Act has in the 80's been designed to provide legal principles applicable to both paper-based and electronic handling of cases.

However, the legislation reflects a view of computers and databases originating from a different technical culture. The many special cases, with different technical solutions

for different sectors of public administration, has led to extensive laws and regulations that are inconsistent with the general approach.

2 DIGITAL DOCUMENTS

2.1 Documents in the public administration

2.1.1 The Swedish approach

In 1989 the Swedish work in the area of *electronic records with digital signatures* began with the establishing of a committee whose task it was to suggest new regulations for customs procedures.[1] They then observed the possibility of:

— linking the legal efforts to the principles behind the international standardisation of digital signatures and related services,

— creating a base for the legally *unified regulation* of paper-based and electronic routines.[2]

These questions have been further analysed in other areas such as criminal law (document forgery), taxation law (electronic tax returns), electronic mortgages, and eventually the totally electronic handling of cases and proceedings.

In the following I will introduce the Swedish approach, by giving a short presentation of the substantive problems from a legal point of view, created by computer based handling of documents. Then I will describe Swedish laws and bills concerning documents with digital signatures. In conclusion, a description will be provided of the task of *seeking general legal concepts* for digital documents and electronic files, a subject that contains EDI as well as E-mail and transfer of electronic files.

2.1.2 Substantive problems

The use of documents in public administration is — from a legal perspective — mainly constructed on the same notion of "document" as the protection in criminal law against document forgery. The concept document, in administrative as well as criminal law, is built on presumptions that a traditional document obviously possesses certain qualities. These qualities makes it needless to discuss some security aspects, that legal demands are built on. However, these qualities are partly missing in digital documents.

The *paper document* consists of three aspects:

— the carrier (the sheet of paper)

— text and pictures (the physical representation of the information)

— information about the originator (usually a written signature).

The connections among carrier, text and signature are self-evident. The carrier gives border-lines and structure to one finalised representation of the content. However, these qualities are partly missing in an digital document, where all information is broken down to a pattern of digital signals. It is important to address the legal problems that these new objects confer to the notion "document".

I will briefly mention the following aspects:

It is an implicit qualification within the document that it shall give *self-dependent existence* to the information, and via its physical bounds provide a clear distinction from other objects. Data representing a particular digital document, however, is stored together with data representing other information.

One additional demand is the *durability* of a document. The transportation of data via the telecommunication infrastructure or transitory text upon a computer screen will hardly fulfil these demands.

The need for *trust in the authenticity* of a document is central. The document shall give the reader reason to believe that the text originates from the individual who, according to the record, is seen to be the originator. Therefore a traditional document, as carrier of the information, is often furnished with stamps, printed logotypes, attestation of signatures etc., enabling the *examination* of a paper document to find out *if it has been manipulated.*

Until recently most methods used to produce the equivalent functionalities in electronic handling of documents relied on the system being regarded as a secure domain. The users were identified during some log-in procedure. From a legal perspective, however, this provides an unacceptable level of security, leading to the development of new methods for creating digital documents with digital signatures.

However, the function of a paper document to transmit authority as a physical example — an original — can not be recreated digitally in a simple way. Certain applications, such as shipping documents, demand some form of registration in the IT-environment (confer the functionalities within the EU-project Bolero).

The discussed "document problem" leads to the delineation of the term "data". The word data, by concentrating on the representation, has — according to international standardisation — been given a concrete meaning while information is seen as something abstract, namely knowledge.

The difficulty in understanding the nature of data depends on the fact that we are moving in the borderland between concrete and abstract objects, where some of the self-evident presumptions that a traditional viewpoint is built upon do not exist. This confers to the "document problem" new dimensions.[3]

There may be different methods available to solve the legal problems in this area. The Swedish approach, however, has in principle been to follow the example from the international standardisation of digital signatures and related services. The legal system should in this way be capable of supporting adjustments towards a more secure IT-milieu.

2.1.3 The Swedish customs act and succeeding legislation

A basic assumption for the Swedish legislator has been that the digital document needs to provide the same evidence as a paper document, and must be able to be linked to a specified originator. Therefore, the password method was not accepted. A document definition was constructed instead, which was centred on the need for verification of the documents themselves.

It was not appropriate to lay a detailed technical description as a foundation for the construction of the rules since new security methods in accordance with technical advances might arise. The legislation should instead be tied into the developmental work which is continuing for electronic authentication. Therefore the phrase "electronic document" was introduced in the Swedish Customs Act of 1990, and defined as *"a record, the content and originator of which, should be able to be verified by a certain technical procedure."*[4]

The same document definition has been adopted
— in 1993 in a law concerning the registration of mortgages,
— in 1995 in taxation law, and
— in 1995 in the regulations concerning recovery of debt by enforcement orders.[5]

2.1.4 Swedish bills

These problems have been analysed, also from criminal and procedural viewpoints, by *a Swedish governmental committee on computer related crime*. In a report from December 1992[6] the committee has suggested a unified regulation for traditional documents and digital documents with regards to document forgery, according to the Penal Code. The following definition has been suggested: *"By document in this chapter is meant [a written original record or] a defined set of data for automatic information processing, if it is possible to ascertain that the contents originate from the designated issuer."*[7]

This Bill is under consideration in the Ministry of Justice. The demand for authentication according to the definition implies that there shall be a technical procedure providing for the possibility of verification of both the text and the issuer.

The Swedish government established in 1994 *the IT-committee,* whose task was to consider suggestions for the legal redefinition's that are necessitated by the replacement of traditional and established routines of document transmittal and verification by digital documents and services. In March 1996 the committee presented its report Electronic Documents.[8] One of the main features of the committees' findings were the following definitions;

> *electronic record:* a defined set of data, which can be viewed, listened to or otherwise apprehended only by electronic means,
>
> *digital document:* an electronic record with a digital signature or a digital stamp,
>
> *digital signature:* the result of a transformation of an electronic record, by means of a unique key, making it possible to ascertain if the contents originate from the individual designated as issuer,
>
> *digital stamp:* the result of a transformation of an electronic record, by means of a unique key, making it possible to ascertain if the contents originate from the legal person or authority designated as issuer.[9]

2.1.5 Natural legal solutions

The aforementioned definitions of "document" are built on the same concept, and with this kind of definition it has been natural to solve the various legal questions that arise on the basis of the rules which are already established for paper documents. Questions concerning legal difficulties which arise from digital documents and signatures are thereby replaced by the possibility of creating a legally unified regulation of traditional routines and IT-routines. The functions of a paper document are then replicated within the framework of useful applications of a digital signature, with security maintained and without the general principles of legal procedure being affected.

The attainment of a sufficient level of security has been judged as being primarily a technical problem, with the presuppositions that both the contents and the originator should be possible to be verified, as when the demands of a digital signature according to international standards are fulfilled.

2.1.6 Requirements of hand-written signature or the like

The IT-committee also addresses certain practical questions arising from a legal viewpoint due to the rapid transition to electronic document handling. A relevant act, in a case involving legal procedures, may prescribe something which precludes the usage of electronic documents, such as the requirement of a hand-written signature. The committee recommends that the government be allowed to stipulate that digital documents (or, if that is deemed to be sufficient, electronic records without a digital signature or stamp) may be used.

Also recommended is the right of agencies to require confirmation by the originator when a message lacks the originator's hand-written signature, as well as to commission a third party — when needed — for the technical conversion of electronic messages so that they may be read or otherwise comprehended.

2.1.7 Incoming documents

Furthermore, the committee has suggested new provisions concerning the establishment of the point in time when incoming electronic records are deemed to have been received by an agency. In a traditional environment, a document is deemed to have been received by an agency the day upon which the document is delivered to the agency. This rule may also be applied when a diskette is mailed via the postal service to an agency.

In those cases where messages are transmitted via an electronic network, the principle applied is that the document is deemed to have been received by the agency when the data which represents the document have reached the agency's mail-receiving function. This is seen as being applicable whether this receiving function is physically located in the agency's information system or has been relegated to a mediating company which furnishes a service in which the "mailbox" is physically located on the mediating company's premises. These provisions are complemented by certain stipulated exceptions which primarily correspond to current legal practice.

> A document that is transmitted electronically is deemed to have arrived to an agency that day when the document
>
> 1. has arrived at the agencies electronic address,
> 2. has been received by a qualified employee, or
> 3. may be assumed to have arrived at the agencies electronic address, if it has come into the hands of a qualified employee on the following working day.

2.2 Documents in business life

2.2.1 New patterns of commerce

Similar questions occur within civil law concerning the creation of security in contract formulation, etc. However, IT has not been limited to the conversion of traditional routines to their electronic equivalents. Instead, the entire pattern of commerce is transformed, and the focus of change becomes automatic *processes*, rather than *products* such as bids, contracts, invoices, bills of lading, etc.

An example of this is the concept "Business Process Reengineering", where even such demands that have been perceived as obvious from a legal point of view may be questioned. Striving to utilise the entire potential for rationalisation that IT offers has led

to a balancing between effectivity and security that, in some cases, may need to be re-evaluated.

2.2.2 EDI-agreements

The private sector has attempted to solve the legal questions that arise by constructing model contracts on how contracts should be entered into, such as the so-called EDI agreements. Among other things, these contracts deal with questions that arise when involved parties enter into agreements automatically, i.e. when computers generate and transmit messages that result in a binding agreement.

Electronic commerce will most likely, at least in certain areas, attain such dimensions that it will hardly be possible to initiate and preserve written EDI agreements with every business associate. Therefore, there is a need for a functioning legal structure even within civil law concerning the creation of predictable and secure information in electronic contract formulations.

2.2.3 The IT-committees' findings[10]

The committee has nevertheless found that most of the questions that arise may be answered within the framework of current contractual law. Not every detailed question can be answered in advance, but contract law is formulated at a general level and is limited to basic principles which are appropriate for agreements of varying type. Questions that do not directly fit under any of the prevailing regulations should still be able to be dealt with in close relation to the principles upon which contract law is based.

Regarding the question of whether or not electronic manifestations of a party's "will", generated automatically without direct human involvement, can result in binding contracts, a parallel can be drawn with such traditional "mass" transactions that occur frequently and in large volume in daily practice. Typical contracts that fall into this group are such things as small, simple purchases in stores or a bus trip paid in cash. It may also be cited from Swedish jurisprudence that a contract regarding parking is deemed to be entered into by simply placing the car in a parking place.

In a similar manner, the individual that electronically and automatically makes an offer or an acceptance is bound by the offer or reply. The purpose of the entire procedure is to create binding agreements when certain exterior circumstances combined with one another function as the direct establishment of a contract. The legal text is sufficiently accommodating to allow a non-prejudicial application of contract law, while at the same time avoiding a new construction that departs from traditional civil law.

However, certain provisions in contract law lose their purpose when contracts are entered into completely automatically. These are the provisions that presuppose human behaviour patterns, such as those dealing with coercion, deceit and usury. A computer, for example, cannot threaten another computer. However, this does not necessitate any amendments in contract law since irrational results may be corrected through the so-called general clause, which is completely free from subjectivity.

Also in other areas current contract law should be applicable to the IT area. For example, this is true concerning provisions regarding liability because a transmitted message is delayed or never received, as well as provisions dealing with "written" and "oral" communication.

The committee suggests, however, an amendment in contract law concerning the question of who is liable when an electronic message has been corrupted during transmission. A complementary addition to the current provisions concerning assignment of risk due to the delay or disappearance of a message is recommended. This provision should also be applicable when a message is corrupted during transmission to the receiver (Section 40 of the Contract Law). The Contract Law will then correspond to the present Law of Contract of Sale of Goods, which came into force in 1990.

3 CLOSING LINES

The legal problems concerning computerbased documents are of a general kind and exist in all countries. The character of these objects needs to be examined and legal definitions expanded to include the new dimensions in the field of IT. To preserve a traditional point of view that is partly antiquated will lead to differences in praxis between traditional and digital documents that are hard to understand. It would also most likely hinder an effective regulation.

Primarily, a discussion of whether or not a uniform definition is possible should be considered. A generally accepted document definition, founded in the basic principles of electronic handling of information, would most likely facilitate international harmonisation in this area. Secondly, the possibility of finding a uniform view on the category of objects needs addressing.

As a starting point, the same principle point of view could be adopted concerning paper documents and computer data. Further analysis of the new infrastructure will however probably show a need for adjustments to IT. In this area it is important to address the connection between digital signatures and general improvements of information security as well as consistency with the legal system.

---

[1] The governmental committee with the task to consider the need for legislation in customs computerisation (TDL-utredningen).
[2] See also the aforementioned committees report SOU 1989:20 (SOU is Statens offentliga utredningar; the Governmental Committee Reports).
[3] This Swedish description may be found in the Green Book of Information Security and in the Council of Europe Recommendation Concerning Problems of Criminal Procedure Law Connected with Information Technology, adopted by the Committee of Ministers on September 11, 1995.
[4] Proposition 1989/90:40 p. 4, 27 f. and 50 (proposition means in this instance the governmental bill containing the motivation for the legislation).
[5] Prop. 1993/94:197, prop. 1994/95:93 and prop. 1994/95:168.
[6] SOU 1992:110.
[7] SOU 1992:110 p. 22.
[8] SOU 1996:40.
[9] SOU 1996:40 p. 39.
[10] SOU 1996:40 p. 117-138. These report has also been discussed on the 34:th Nordic Assembly of Lawyers, Stockholm, August 21-23, 1996.