Le droit de la preuve dans la télématique professionnelle

Amory, Bernard

Published in:
Informatique et télécommunications : y a-t-il un juriste dans la salle ?

Publication date:
1989

Document Version
le PDF de l'éditeur

LE DROIT DE LA PREUVE DANS LA TELEMATIQUE PROFESSIONNELLE*

par Bernard Amory**

Introduction

1. Le sujet dont vient de nous entretenir brillamment mon collègue, M. Martin, est très différent quant à son contenu de celui que je vais examiner (la preuve). Mais s'ils sont différents, ces sujets sont néanmoins très intimement liés l'un à l'autre. Ce n'est d'ailleurs pas par hasard que les organisateurs de ce colloque ont prévu de se faire suivre ces deux exposés. En effet, en matière télématique, l'attribution de la charge de la preuve ou la détermination des modes de preuve admissibles ont des conséquences directes sur le fonds du droit et particulièrement sur les responsabilités.

2. Permettez-moi de vous donner un exemple pour concrétiser cette affirmation: si une entreprise signe avec une banque un contrat de services financiers par télématique et que ce contrat contient une clause relative à la preuve stipulant que les "loggings" produits et conservés par la banque font preuve des opérations, il est évident que le client qui veut contester le montant ou l'existence d'une opération que la banque lui attribue risque de rencontrer quelques difficultés et donc finalement d'encourir une responsabilité. Dire que la matière de la preuve est liée à celle de la responsabilité c'est déjà souligner toute son importance. Importance exprimée par l'adage bien connu: "Idem est non esse aut non probare".

---

* Exposé présenté au cours du Colloque intitulé "Informatique et télécommunications: y a-t-il un juriste dans la salle", à Bruxelles du 9 au 11 décembre 1987.

** Assistant à la Faculté de Droit de Namur et membre du cabinet Dechert Price & Rhoads (Bruxelles).

3. Les juristes qui se sont intéressés au droit de l'informatique ont très vite été conscients que l'informatique puis la télématique posaient des défis à notre droit de la preuve. On sait que les règles actuelles sont encore le reflet de l'Ordonnance de Moulins de 1566 adoptée lorsque l'écriture et la signature manuscrite étaient le "State of the Art" et naturellement le législateur de l'époque en a fait la pierre angulaire du droit de la preuve. Mais nous sommes maintenant à l'ère de la signature électronique et de la transmission télématique. La confrontation des vieilles règles avec les nouvelles techniques suscitent des interrogations.

4. Ce que je vais tenter de faire aujourd'hui c'est d'abord de faire le point sur ces interrogations (distinguer les faux des vrais problèmes de droit de la preuve), et ensuite d'examiner de manière la plus concrète possible quelles réponses le juriste peut y donner <u>en pratique</u>, c'est-à-dire, nous le verrons, par la voie contractuelle. Il n'entre pas dans mon intention d'envisager ici les éventuelles interventions législatives car même si on admet qu'elles sont nécessaires, nous savons qu'elles n'interviendront pas suffisamment tôt pour solutionner les problèmes qui peuvent se poser dès aujourd'hui dans les millions de transactions télématiques qui sont réalisées quotidiennement. Je voudrais encore préciser que conformément à la compétence qui a été attribuée à cette session, je me limiterai à ce qu'on appelle la <u>télématique professionnelle</u>, c'est-à-dire la télématique qui met en présence des commerçants au sens juridique du terme et non des "particuliers", aussi appelés "consommateurs", et à qui une autre session de ce colloque est consacrée. Cette distinction est très importante car dans notre droit, le régime de la preuve en droit civil est très différent du régime de la preuve en droit commercial.

Les faux problèmes

5. Les faux problèmes sont ceux qui sont soi-disant posés par les exigences légales strictes de notre code civil ou du droit anglo-saxon (1) : l'exigence de la preuve écrite pour les actes juridiques contenue dans l'Article 1341 du code civil, la "Hearsay Rule" (la règle de l'ouï-dire) et la "Best Evidence Rule" (règle de l'original) en droit anglo-saxon. Voyons pourquoi ce sont de faux problèmes.

6. L'Article 1341 des codes civils français et belge requiert un écrit signé pour prouver les actes juridiques d'une valeur supérieure à, respectivement, 5.000FF ou 3.000 FB. Le but de cette disposition était d'assurer la présence physique du signateur à l'acte. Cette exigence paraît donc incompatible avec l'objet même de la télématique à savoir, échanger des informations et conclure des contrats à distance de manière instantanée sans nécessiter la présence physique des personnes qui y sont parties.

7. En réalité, l'Article 1341 du code civil ne constitue pas un obstacle sérieux à la conclusion de contrats par télématique parce qu'il connaît de nombreuses exceptions parmi lesquelles sa non-application aux actes de commerce. Cet article précise dans son deuxième alinéa que "le tout (est) sans préjudice de ce qui est prescrit dans les lois relatives au commerce". Ces lois (les Articles 25 et 109 des codes de commerce français et belge) nous disent qu'en droit commercial la preuve est libre. Tous les modes de preuve sont admissibles sous le contrôle du juge dont

---

(1) Cette affirmation est un peu brutale. Le temps imparti à cet exposé ne permet pas de la nuancer. Le lecteur pourra se référer au texte ci-joint, "Le droit de la preuve face à l'informatique et à la télématique, Approche de droit comparé", par Y. Poullet et B. Amory.

il faudra emporter l'intime conviction. Et c'est là que les vrais problèmes commencent.

8. Mais avant d'aborder ces vrais problèmes, laissez-moi encore tenter de démystifier les faux problèmes en droit anglo-saxon. En droit anglo-saxon de la preuve, il y a deux règles anciennes et fondamentales connues sous le nom de la "Hearsay Rule" (règle de l'ouï-dire) et de la "Best Evidence Rule" (règle de l'original). La règle de l'ouï-dire stipule qu'un document n'est pas admissible comme preuve si son auteur n'est pas présent pour témoigner de son contenu (et dès lors être soumis au "cross-examination"). La doctrine et la jurisprudence ont considéré qu'un document d'origine informatique était de l'ouï-dire parce que l'ordinateur contribuait à sa production et bien entendu l'ordinateur ne peut en témoigner. De même, la règle de l'original prévoit qu'un document n'est recevable à titre de preuve que s'il est produit en forme d'original. Or un document informatique n'est souvent que la transcription d'un autre document (facture, bon de commande, ...) et même si les données sont entrées directement dans l'ordinateur, l'original serait l'information contenue sur la disquette et non l'imprimé produit par l'imprimante.

9. Les règles de l'Hearsay et de la Best Evidence ne constituent pas plus que l'Article 1341 du code civil des obstacles sérieux à l'utilisation de la télématique dans la vie des affaires, étant donné qu'elles connaissent aussi des exceptions qui permettent d'en faire échapper les transactions télématiques professionnelles. Ainsi, en droit américain, il existe une exception à l'interdiction de l'ouï-dire: c'est la "Business Record Exception", qui dit que les données enregistrées régulièrement dans le cours normal des affaires sont recevables sans témoignage de leur auteur. Cette exception s'applique aux documents d'origine informatique et la Cour Suprême du Nebraska a dit à ce sujet qu' "elle était destinée à faire entrer dans les salles d'audience les réalités du monde des affaires". De même, pour écarter l'application de la Best Evidence Rule, il

suffit d'établir que l'original est indisponible ou a été détruit. Cette exception a aussi été interprétée très largement et s'applique sans difficultés aux documents informatiques.

10. Donc ni l'exigence de l'écrit signé contenue dans l'Article 1341 du code civil, ni les principes du droit anglo-saxon interdisant la recevabilité de l'ouï-dire et des documents non-originaux ne constituent de véritables obstacles à l'usage de la télématique pour les transactions commerciales.

Les vrais problèmes

11. Les vrais problèmes sont ailleurs. Un document produit par un système télématique peut être présenté à un juge, en droit continental, en vertu du régime de la preuve libre en droit commercial, et en droit anglo-saxon en vertu des exceptions aux règles rigides de l'ouï-dire et de l'original. Mais il faut encore convaincre le juge de la valeur probante et de la fiabilité du système informatique. Et c'est à ce moment que les vraies difficultés surviennent.

12. Cela m'amène à aborder une notion qui n'est pas à proprement parler une notion juridique (on ne la trouve pas reprise dans les index des traités), mais qui revêt une importance fondamentale pour le droit de la preuve. C'est l'authentification. On pourrait en donner la définition fonctionnelle suivante: l'authentification d'un texte (télématique ou autre) a deux fonctions:

1. identifier la personne qui est l'auteur du message;
2. indiquer sa volonté de s'approprier le contenu du message, de le faire sien.

En cas de conflit, on se réfèrera à cette authentification pour prouver qui s'est engagé à quoi. L'authentification pourra donc servir à apporter la preuve d'une transaction commerciale, c'est-à-dire démontrer vis-à-vis des personnes qui en sont partie et des tiers que la transaction a bien eu lieu entre ces parties et quel en est le contenu.

13. Traditionnellement, la signature manuscrite servait à authentifier. On a admis aussi dans certains cas l'apposition de la signature au moyen d'un cachet, d'un fac-similé, de la perforation, etc. Mais dans une transaction télématique, ni l'apposition de la signature manuscrite, ni celle d'un cachet n'est possible, puisque par définition les parties sont éloignées l'une de l'autre et l'opération est quasi-instantanée. Il existe des techniques d'authentification adaptées à la télématique. Il s'agit de codes secrets, appelés aussi PIN ou PIC (utilisés par exemple pour les cartes de paiement), de la cryptographie (utilisée dans le système SWIFT) et de la reconnaissance de caractéristiques physiques (par exemple les empreintes digitales). Ces techniques modernes d'authentification sont en général très fiables. Ainsi, avec un code de 4 chiffres dans un système ne permettant que trois essais, un fraudeur n'a que 0,03% de chances de découvrir le code secret. Ces systèmes d'authentification procèdent par comparaison: ils comparent l'information saisie avec une référence. On peut donc les comparer à la signature manuscrite, puisque l'on peut aussi la confronter éventuellement à un spécimen pour vérification. Mais avec les systèmes modernes d'authentification, la vérification se fait automatiquement, systématiquement tandis que la signature manuscrite n'est vérifiée qu'occasionnellement. Je crois, bien que je ne sois pas technicien, qu'on peut affirmer qu'il existe aujourd'hui des systèmes d'authentification télématiques très fiables (par exemple, le système bancaire belge TRASEC).

14. Mais il ne suffit pas d'affirmer qu'un système est fiable pour emporter l'intime conviction du juge. Il n'existe quasiment pas de jurisprudence relative à la force probante des nouvelles techniques d'authentification (a fortiori puisque ces techniques sont récentes). Il y a bien une décision du Tribunal d'Instance de Sètes, qui a rejeté le code secret comme mode de

signature dans un système de paiement électronique. La Cour d'Appel de Montpellier a infirmé cette décision. Il y a aussi une jurisprudence plus ancienne relative à une technique qui fut nouvelle: le télex. On constate, en général, que la jurisprudence accorde aujourd'hui un haut degré de fiabilité au télex, étant donné la pratique devenue courante dans les affaires de conclure des contrats par télex.

15. Il reste néanmoins que les parties à une transaction risquent toujours de voir leurs systèmes d'authentification considérés comme non fiables.

Solutions pratiques

16. Pour éviter ce risque, il y a une solution. Elle est de nature contractuelle. Il est en effet généralement admis que les dispositions relatives à la preuve dans les codes civils et de commerce ne sont pas des dispositions impératives. La jurisprudence dominante et la doctrine unanime sont d'avis que la preuve est une matière d'ordre privé et non d'ordre public, comme le dit le Professeur Lucas de Leyssac dans un récent article intitulé "Plaidoyer pour une droit conventionnel de la preuve en matière informatique" (2) : "Lorsque la convention sur la preuve porte sur un droit dont on peut disposer, un droit à recevoir une somme d'argent par exemple, il n'y a pas de raison de ne pas admettre la convention sur le preuve puisqu'au pire, elle conduit à la disparition du droit. Si l'on peut disposer du droit directement, on peut en disposer indirectement par le biais d'une convention sur la preuve". Les conventions relatives à la preuve sont donc possibles. Il y a cependant certaines limites à leur validité: une partie ne peut pas par une convention s'interdire de faire primer la vérité. Il faut toujours laisser la possibilité de contester, de faire la preuve contraire. Sinon la clause reviendrait à dénier à une partie le droit d'agir en justice.

---

(2) Voir Expertises, 1987, p. 260 et seq.

17. Ne serait à notre avis pas valable la clause par laquelle, dans le cadre de services financiers électroniques, une entreprise cliente d'une banque "reconnaîtrait comme correctes, conformes, exactes et contraignantes les données reçues et enregistrées par la banque". Par contre, si la clause prévoit que des données sont réputées exactes jusqu'à preuve du contraire, c'est-à-dire que la clause n'établit en fait qu'une présomption, alors qu'elle serait parfaitement valable.

18. Un autre aspect sur lequel je voudrais attirer l'attention est l'utilité de distinguer dans une clause relative à la preuve, d'une part l'aspect "authentification", et d'autre part l'aspect "contenu". En effet, il s'agit de deux choses quelque peu différentes. Il se peut que l'on conteste radicalement avoir envoyé un message par télématique ou bien que l'on conteste seulement le contenu de ce message (par exemple le montant). C'est pourquoi une clause qui peut être intitulée "signature" ou "signature électronique" est conseillée et peut être rédigée de la manière suivante:

> "Il est convenu entre les parties que la technique d'authentification décrite à l'Annexe X sera considérée par les parties comme preuve de l'identité et de l'accord des parties pour les messages envoyés sous le couvert de cette procédure d'authentification."

De nouveau, cette clause n'est valable que dans la mesure où elle ne constitue qu'une présomption et laisse donc la possibilité d'apporter la preuve contraire (que le message a été envoyé par un fraudeur par exemple).

19. Il existe encore un véritable problème auquel je ne peux apporter de solution. Ces conventions relatives à la preuve ne sont concevables qu'entre parties en relations d'affaires régulières, par exemple dans la convention de base entre une

entreprise et une banque dans le cadre des services financiers électroniques, ou dans le cadre d'une convention relative à la remise d'instructions par téléfax. Une telle clause peut également se trouver dans un "règlement" auquel adhèrent tous les membres d'un réseau télématique, par exemple: SWIFT, ODETTE. Mais conclure une telle convention écrite préalable n'est pas possible si les parties n'ont qu'un rapport occasionnel, et que leur contact est exclusivement et dès le départ télématique. Or ce genre d'opération est susceptible de devenir de plus en plus fréquente avec le développement du courrier électronique et des réseaux en général.

Dans ce cas, la convention préalable relative à la preuve est impossible. Cela est un vrai problème. Il faudra convaincre le juge de la fiabilité du système. Toutefois, on peut espérer que si une technique d'authentification est largement utilisée, adoptée par un ensemble d'entreprises, par exemple la communauté bancaire, et si elle fonctionne convenablement, un tribunal y accorderait, même en l'absence de convention préalable, une force probante privilégiée.

COMPUTERS IN THE LAW OF EVIDENCE - A COMPARATIVE APPROACH IN CIVIL AND COMMON LAW SYSTEMS

by

Bernard E. Amory* and Yves Poullet**

Annex to presentation by B. Amory at conference entitled "Computers and Telecommunications : Is there a lawyer in this room ?" Brussels 9-11 December 1987.

---

* Bernard E. AMORY is an associate with the law offices of Dechert Price & Rhoads and a lecturer at the Computer and Law Research Centre, University of Namur (Belgium).

** Yves POULLET is a professor at the Law Faculty and Director of the Computer and Law Research Centre in Namur (Belgium)

This paper is a summary of an article published (in French) in the Revue Internationale de Droit Comparé No. 2, 1985, p. 331 à 352.

Introduction

I. The Common Law approach
   A. The hearsay rule
      1. English law
      2. American law
   B. The best evidence rule
      1. English law
      2. American law

II. The approach in French and Belgian law
   A. The problem
   B. The legal requirements
      1. The distinction between legal acts and legal facts
      2. The principle
      3. The exceptions to the principle and their application to telematic contracts

Conclusion

INTRODUCTION

The amount of information which companies have to keep, often for long periods, whether for legal reasons or in the interests of good business management, can in some cases cause serious storage problems, thereby affecting overhead costs (1).

One of the advantages of the use of computers in business is the ability to reduce the volume of documents kept in archives and to facilitate their processing. There is no longer any doubt that companies need to be able to keep computerised records (2).

The combined use of computers and telecommunications, known as "telematics", offers further possibilities, such as long-distance operations, which include transferring funds, ordering consumer goods, accessing data banks and numerous other types of information exchange.

This technology, immediately raises some rather complex legal questions, notably in relation to the law of evidence.

Does the processing and storage of information in the form of computer documents (computer listings, magnetic tapes, discs, computer microfilms) constitute the basis of valid evidence for the purpose of legal proceedings? Do transactions which can nowadays be carried out by computer (so-called telematic transactions) satisfy the legal requirements relating to evidence of legal acts?

The answers to these questions are considered in turn in relation to two legal systems: the Common Law (more particularly English law and American law) and the Civil Law (more particularly French law and Belgian law).

I. THE COMMON LAW APPROACH

The law of evidence under the Common Law system, which is characterised by the wealth, the precision and the technicality of its rules, contains two fundamental principles which appear to constitute major obstacles to the admissiblility of computer and telematic documents as evidence of the information which they contain. These rules are the hearsay rule and the best evidence rule.

By virtue of the hearsay rule, oral evidence, which is a privileged form of evidence under the Common Law, is only admissible if it is given by the person who has personal knowledge of the facts which he is asserting. He is in fact the only person who can validly be cross-examined on those facts. Applied to written evidence, this rule means that a document is not admissible unless its author is present to testify before the court on its contents. So when data, eg. bills, is fed into a computer and then presented in the form of a computer document, the original information has passed through several "hands": those of the author of the original document (in our example the bill), those of the coder, who is not necessarily the same person or even answerable to him (eg. in the case of a service agency) and finally those of the computer, since in processing and storing the information, it is capable of altering it. Since by their nature computers cannot be cross-examined, legal writers (3) and the case law (4) have always considered computer documents to be hearsay evidence.

By virtue of the best evidence rule, a document is in principle only admissible if it is produced in its original version. Computer documents are often only transcriptions of "traditional" documents (bills, order forms, etc.), which constitute the originals; these are often destroyed after being recorded on computer. Even when there is no written document which could serve as the basis of a computer document, for example in the case of direct recording, the original is considered to be the data contained in the computer in magnetic or electronic form and the machine printout on which the data appears in readable form is only a transcription of that data and, as such, is not admissible before a court.

Fortunately, in both American and English law there are numerous exceptions to the best evidence and hearsay rules and their application to computer documents will now be examined (5).

A. The hearsay rule

1. English law

In the absence of jurisprudential exceptions to the hearsay rule granting the admissibility of computer documents as evidence of the facts which they contain and given the fact that it is impossible for the courts to create new exceptions to this rule (6), the legislature intervened in 1968 (7) and introduced, along with new general provisions relating to hearsay evidence, provisions relating specifically to computer documents.

In its provisions of general applications, the Civil Evidence Act 1968 allows the admissibility of "first-hand" hearsay (8). Applied to computers, this rule means that a computer document is admissible if the person who loaded the data had a personal knowledge of it, or, acting in the exercise of his duty, received it from a person who had such knowledge (9). These provisions do not apply when a computer document does not have as its original a document of which a person has direct and personal knowledge. Such is the case with a transaction performed at an automatic teller machine or a recording by optical reading. In these circumstances, Section 5 of the Civil Evidence Act lays down specific conditions relating exclusively to the admissibility of evidence in the form of computer documents.

By virtue of these conditions, a computer document will be admissible as evidence if:

- it was produced by a computer which is regularly used for the normal activities of its user;

- the computer is regularly supplied with information of the kind contained in the document put forward as evidence;

- the computer was operating properly at the moment of the recording of the information;

- the information contained in the document reproduces or is derived from information supplied to the computer.

By virtue of section 5(4) of the Act, a certificate identifying the document, describing the manner in which it was produced and any device involved in its production as well as any other useful information relating to the conditions contained in subsection (2) must be submitted to the court signed by a person occupying a responsible position in relation to the operation of the relevant process or the management of the relevant activities.

If the document satisfies these conditions, it is declared admissible and it is then for the court to weigh up its probative value taking into account all the circumstances, notably the degree of simultaneity between the occurrence of a fact and its recording on computer as well as any interest that any person who is implicated might have in altering the data (10).

These provisions have been much criticised (11) for the definitions which they contain and the conditions of admissibility which they lay down. For example, the definition of computer is limited to hardware and makes no mention of software. The result is that the requirement of proper operation does not extend to programmes, which can, however, be the source of errors.

Another criticism of the Act is that it has no provision for verification of the accuracy of the original information which has subsequently been processed by computer. If this information is wrong, the computer document will likewise be wrong - garbage in, garbage out.

In parallel with this adaptation of the law by the Civil Evidence Act, the English legislature has also specifically recognised the value of computer documents in certain particular areas. Thus in the banking sector, the Banking Act 1979, amending the Bankers' Books Evidence Act 1879, expressly recognises that "bankers' books" includes records "kept on microfilm, magnetic tape or any other form of mechanical or electronic data retrieval mechanism". In the same way, the Stock Exchange Act 1976 allows commercial enterprises to keep the books which the Companies Acts oblige them to keep other than in directly readable form as long as they can be reproduced in readable form.

2. American law

There is a jurisprudential exception in the United States to the rule prohibiting hearsay evidence which is known as the business records exception; this was introduced into federal legislation (12) and adopted without major alteration by a majority of states. This exception provides that business records (13) are admissible as evidence without the requirement of oral evidence by their author if the transactions which they record were performed in the normal and regular course of business and recorded at the time or shortly after they were performed (14).

Since these conditions of admissibility are based on the circumstances surrounding the recording of the information and not its form, the jurisprudence has been able to resort to the business records exception to allow the admissibility of computer documents.

This usage of the exception can nevertheless be criticised: information is often stored only in electronic or magnetic form and only printed in legible (i.e. by man) form if this proves necessary (eg. when there is a dispute), which may be long after its recording. The result is that it could be claimed that in the strict legal sense neither the requirement of regularity nor that of simultaneity are satisfied. These arguments were rejected in an important decision of the Supreme Court of Nebraska (15), which gave rise to much case law (16) on the subject. The judgment of the Supreme Court confirms that the business records exception must be given a broad interpretation because its purpose is to "bring the realities of business and professional practice into the courtroom". The court added that the requirements of regularity and simutaneity must be satisfied at the moment of the introduction of the information into the computer and not at the moment of the printing of the computer document.

According to the business records exception, such documents are admissible without the need for evidence in person by their authors. They may be presented by the person responsible for the computer system or by any other employee of the company who is fully informed about the system of recording, processing and storage of information (17). This person explains to the court the procedures for detection and correction of errors and gives evidence on the reliability of the system, its proper functioning etc. There was formerly a requirement that the computer be of a standard type but this has now been abolished since it acted as a brake on technical development.

Because of the great flexibility of the business records exception, there was no need for the legislature to act to allow the admissibility of computer documents. The federal legislature nevertheless adopted a new formula for the Federal Rules of Evidence (18) and stated that the exception applies to information stored "in any form", which, according to official commentaries (19), includes information stored by computer.

Insofar as it confirms an already firmly established body of case law, this provision was not really necessary. However, it may prove to be useful when new data processing and storage techniques are discovered.

B. The best evidence rule

1. English law

The production of a copy as evidence of the contents of its original is permitted if the party exercising this right establishes that he was unable to obtain the original (20). Thanks to its very general terms, this exception allows the removal of the obstacles created by the best evidence rule to the admissibility before the courts of computer documents. To establish their non-availability, it is enough to show that the originals of such documents were destroyed in the normal course of business or never existed (eg. direct recording) (21). The argument that the original is the document in its magnetic or electronic form as it appears in the computer and not the computer printout seems untenable to us, for in reality only as a printout is the document legible by man and therefore able to be put before a court.

The requirement of proof of the non-availability of the original was abolished in 1982 for copies of films and audio recordings by a decision which held that they are by their nature reliable (22). According to certain writers, this decision could be applied to computer documents (23). We believe that such an interpretation should be qualified: an extension of this case law to computer documents containing information which has undergone fairly complex processing does not seem to us to be well-founded since in the circumstances the original information has been altered. It is therefore no longer a simple copy.

There are also legislative exceptions to the best evidence rule. Thus section 5 of the Civil Evidence Act 1968 provides that the copy of a computer document (eg. on microfilm) is admissible if its conformity with that document is sufficiently established in the eyes of the court. The criteria of conformity are not defined in the Act and to our knowledge the courts have not yet clarified this point.

2. American law

As in English law, the admissibility of a copy depends on proof of the non-availability of the original. This concept of non-availability has been interpreted very broadly in relation to computer documents (24).

Another exception which can be used is the voluminous writing exception, by virtue of which a summary (possibly in computer document form (25)) is admissible in the place of the original when this is too complex or lengthy to be put before the judge and where the opposing party has had the opportunity of examining the originals; this presupposes that they have not been destroyed.

II. THE APPROACH IN FRENCH AND BELGIAN LAW

Unlike the Common Law, the problem does not arise in French and Belgian law in relation to admissibility before the courts and tribunals but to satisfying legal requirements concerning on the one hand the storage of documents and on the other the conclusion of transactions.

A. The problem

The combination of computers and telecommunications, known by the term "telematics", enables the performance at long distance of certain transactions, such as the electronic transfer of funds, the ordering of consumer products and the consultation of data banks.

If the advantage of telematics is the increased speed at which contracts can be concluded, the disadvantage is the transience of the operations. Information appears and disappears on the screen, making it difficult to keep a record of an operation.

Furthermore, even if it is possible to establish the existence and the details of a contract, the identity of the parties is not thereby certain. Identification of the terminal does not automatically lead to identification of the person who performs the transaction. Even a password or security code only identifies the person who has access to the network and not the person who actually carries out the operation.

So evidence of the transaction raises three different questions:

1. Evidence of the existence of a contract: the most far-reaching argument on this point is that which claims that the whole principle of a contract being in question, it is for the party claiming the benefit of it to show that it was properly concluded;

2. evidence of the details of the contract : the existence of the contract is not disputed, only some of its provisions (eg. delivery date, method of payment etc.);

3. evidence of the identity of the parties to the contract.

These questions are examined below in relation to Belgian and French law together. Where a provision is particular to one jurisdiction alone, this fact is mentioned.

B. The legal requirements

1. The distinction between legal acts and legal facts

The Civil Law makes a clear distinction between evidence of legal acts and that of legal facts. The distinction between the two notions is not a simple one (26). "It is that the legal fact is a social fact, a fact of man. The "I think therefore I am" leads one to the view that legal facts are linked to the individual and are so of his own accord. However, and this is where the distinction with legal acts lies, the consequences in law of legal facts are independent of the will of the author of the facts (...) a characteristic of legal facts is to leave undetermined the exact scope of their effects" (27).

The distinction between legal acts and legal facts may not be straightforward but the consequences for the law of evidence are important.

Legal facts can be proved by any means the law allows : presumption, oral evidence, confession, etc. On the other hand, the Code requires in principle that legal acts be proved by a signed written document with probative value.

This requirement has been re-affirmed on numerous occasions (28). In particular, the judges have refused to consider as written documents exchanges of correspondence by teleprinter on the grounds that the originals, typed at a distance, are not signed and cannot therefore be considered as signed documents (29).

2. The principle

Article 1341 of the Code civil lays down the principle that a legal act must be evidenced by a written document (either authenticated or signed by the author).

The application of this principle to contracts concluded by telematics leads one to question the probative value of these contracts: agreements transmitted through telematics networks dematerialise the written signature, which is the expression of the personality of the individual and his act of agreement to the contents of a document disappears (30).

Any surviving magnetic or electronic traces of the transaction cannot therefore, or so it would appear, have probative value or assist in establishing the truth for legal purposes.

This rather bold assertion must be qualified.

3. The exceptions to the principle and their application to telematic contracts

There are numerous exceptions. For example:

- transactions involving small amounts of money (up to 5000 French Francs and 3000 Belgian Francs) may be proved by any legal means. This will often be the case for operations performed at automatic bank tills and points of sale (31) and consultations of data banks.

- article 1341 of the Code civil applies when the subject i.e. the act, comes under the civil law (art. 1341, para. 2); in commercial matters, evidence is not restricted and all forms of evidence are admissible at the discretion of the judge (32).

So the requirement of written evidence is felt less in the use of telematics in business than in its private use since the former often involves contact between traders, whereas the latter, in most cases, makes possible the conclusion at long distance of contracts between traders and non-traders. The act is therefore "mixed" and it is the quality of the defendant which is the determining factor for the purposes of the law of evidence.

Furthermore, according to many writers (33), article 1341 of the Code civil is neither a mandatory provision nor a public order provision. It would therefore be possible to derogate from the written document rule in an evidential clause stating that legal transactions performed on a telematics system may be proved by any means of law.

This clause could be in the form of a general regulation applicable to all telematic operations. This general regulation and in particular the evidential clause, coming from the person providing the information by computer, would have to be brought to the notice of the user.

The concept of an evidential clause is not unrealistic in the case of agreements concluded by written document and performed by telematics, as in the case of a subscription to financial information. In fact, the classification of this type of contract as a contract of hire and not as a succession of service contracts for the supply of information allows the

problem of evidence to be easily solved. The written agreement by which the database company undertakes to tansmit financial information to the user can be analysed in two ways : is it a framework agreement which at each separate request for information is followed by agreements applying that agreement, or is it a single agreement on which subsequent requests for information are based, the answers to these requests constituting the performance of this single agreement ?

If there is no evidential clause in the framework agreement and the first alternative is considered to be correct, there is a risk of evidential problems arising. On the other hand, if the second alternative is considered to be the correct one, the existence of an evidential clause does not significantly change the situation since the performance of an agreement would in any case be a legal fact (34), which may be proved by any means under the law.

Finally, another situation in which article 1341 of the Code civil does not apply is when it has not been possible for the person who is pleading the fact to gather documentary evidence of the contractual obligation made in his favour (article 1348 of the Code civil) or when there is written evidence which does not strictly satisfy the requirements of contract law (article 1347).

According to several writers, the use of computer systems or telematic networks, at least by private individuals, constitutes the exception contained in article 1348 and even the one in article 1347. This interpretaion is in line with the extensive jurisprudential theory of the impossibility of keeping written evidence to oneself (35).

The recent Law of 12 July 1980 in France confirmed this jurisprudential development by providing for the exemption from the requirement of written evidence in cases where there is a "material impossibility" of obtaining such evidence. As F. Chamoux remarks (36), "it will be relatively easy for a judge to consider that it has been impossible for a written document to be drawn up, every time he finds himself dealing with the transmission of information which never appears in material form".

It is clear from this analysis of the scope of article 1341 of the Code civil that the principle of the signed written document (instrumentum) which is required for the proof of a legal act is subject to broad exceptions which, in the final analysis, mean that it very rarely applies to telematic transactions (37).

CONCLUSION

According to René David (38), it is primarily the rules of procedure which account for the very different approaches adopted on the one hand by the Civil Law and on the other by the Common Law. It is for this reason that it was decided that this article should deal separately with the admissibility of computerised documents as a form of evidence in one legal system and then the other.

There are striking similarities between the two systems, even though a wide gulf separates the reasoning behind them. The law is hard pressed to recognise the existence of computerisation. In the Common law, "the fundamental problem is the rule which prohibits hearsay evidence" (39). In the Civil Law system the obstacle is the requirement of a written document. The work of the courts is being succeeded by legislative action. There are

many technical questions which cannot be answered by judges and require special rules; so, for example, without mentioning more specialised fiscal and accounting regulations, the Civil Evidence Act 1968 and the French Law of 12 July 1980 lay down certain principles relating to the admissibility by the courts of "computer-produced evidence".

These legislative principles should be enacted in sufficiently general and flexible terms to allow for technical development. In applying these principles, the law prefers to act by means of "recommendations" or "norms" which can more easily be amended and are less binding. As far as possible the linking of legal definitions and concepts to a technical subject should be avoided and the job of translating the deliberately hazy concepts adopted by the legislation should be left to more specialised practitioners who are conscious of the needs and the constraints of the technology on the one hand and of business on the other.

Over and above these national rules and "quasi-rules", there is also a move towards some sort of international regulation since the information market is international by nature. In the words of the Secretary General of the United Nations Commission on International Trade Law, "it is therefore urgent that measures be taken at international level to establish rules relating to the legal acceptance of commercial data transmitted by telecommunications" (40). The rules relating to the admissibility of computerised documents and the rules relating to signatures cannot differ from one country to another in a domain where frontiers no longer exist and where data which is signed and transmitted electronically must be identifiable at any place at any time.

As the Secretary General of the UN Commission remarks, "faced

with the necessity of adapting to the widespread use of computers for commercial and administrative purposes, a number of countries have amended their relevant legislation in order to allow this usage and to accept as a form of evidence documents recorded by computer or data storage systems, provided that they satisfy certain criteria. The disparities between the criteria which are used to determine their legal value together with the refusal by other countries to accord them such value create serious problems when computerised records stored in one country are to be used as evidence in a legal action in another country" (41).

As traditional jurists, we started off from the assertion of the originality of each national law of evidence; it is clear that the existence of an international economy based on transborder data flow makes it necessary for us to consider the need for an international law of evidence in the computer field. It is for us, as jurists, to take up this challenge not by sacrificing ourselves to an ever-changing technology but by broadening our legal concepts : what is a signature ? What is the finality of evidence in law ? What is the essence of the distinction between a legal act and a legal fact ?

FOOTNOTES

(1) Cf. the striking figures quoted by F. Chamoux, "La Preuve dans les affaires", Paris, Litec, p. 103 et seq.

(2) Ibid.

(3) D. Bender, "Computer Law: Evidence and Procedure", M. Bender, Ed., 1978; W.A. Fenwick and G.K. Davidson, "Use of Computerized Records as Evidence", Jurimetrics Journal, 1975, 21; F.B. Lacey, "Scientific Evidence", Jurimetrics Journal, 1984, pp. 254 to 272; L.E. Mills, K.J. Lincoln and C.E. Laughead, "Computer Output, its Admissiblility into Evidence", Law and Computer Technology, 1970, pp. 14 to 21; R. Reese, "Admissibility of Computer Kept Business Records" Cornell Law Review, 1969-1970; J.J. Roberts, "A Practitioner's Primer on Computer Generated Evidence", University of Chic Law Rev., 1974, pp. 254 to 280; N.E. Smith, "Evidence Admissibility of Computer Business Records, an Exception to the Hearsay Rule", North Carolina Law Rev., 1969-1970, pp. 687 to 697; C. Tapper, "Evidence from Computer", Georgia Law Review, 1974, pp. 562 to 613; R.P. Wallace, "Computer Printouts of Business Records and their Admissiblitity in New York", Alabany Law Rev., 1967, pp. 61 to 73; Note "Appropriate Foundation Requirements for Admitting Computer Printouts into Evidence", Wash. Univ. Law Quart., 1977, pp. 59 to 93.

(4) Cf. Notably in American law, Transport Indemnity Co v. Seib, 178 Neb. 253, 132, N.W. 2d 871 (1965); United States v. De Georgia, 420 F. 2d 889 (9th Cir. 1969); King v. State ex rel. Murdock Acceptance Corp. 222, SO 2d, 393 Miss 1969; and in English law: Meyers v. Director of Public Prosecutions, [1965] AC 1001; Regina v. Pettigrew, [1980] 71 G. App. R., p. 39 and Regina v. Ewing, [1983] 3 WLR 1.

(5) We are not going to examine here the situation in other Common Law jurisdictions.

(6) The House of Lords decided in Myers v. Director of Public Prosecutions [1965] AC 1001 that no new jurisprudential exceptions to the hearsay rule could be created.

(7) Civil Evidence Act 1968, Halsbury's Statutes of England, Annual Volume 1968, 1211.

(8) Civil Evidence Act 1968, section 2.

(9) Or even other persons also acting in the excercise of their duties as long as at the end of the chain is someone with a personal knowledge of the information (see Section 4 of the Civil Evidence Act 1968).

(10) It appears from American case law that parties rarely contest the probative value of computer documents once these have been declared admissible by the court (see D. Bender, op. cit. supra note (3), p. 82). There is insufficient English case law on this subject to allow conclusions to be drawn.

(11) A. Kelman and R. Sizer, "The Computer in Court", Aldershot, Gower, 1982, 21; C. Tapper,; op. cit. supra note (3) 604 to 612; R. Sizer, "Computer Generated Output as Admissible Evidence in Civil and Criminal Cases", A Report by the Professional Advisory committee of the British Computer Society, 1982, 831.

(12) The Uniform Business Records as Evidence Act and the Uniform Rules of Evidence, 9 A.U.L.A. (1965)

(13) The term "business" includes business, institution, association, profession, occupation and calling of every kind, whether or not conducted for profit.

(14) See in particular Article 63(13) of the Uniform Rules of Evidence.

(15) Transport Indemnity Co v. Seib, 178, Neb. 253, 132 N.W. 2d 271,11 ALR 3d 1368 (1965) with note by J. Evans.

(16) See in particular King v. ex. rel. Murdock Acceptance Corp. 222 SO 2d 393 (1969); Merrick v. U.S. Rubber Co., 7 Ariz. App. 433, 440 P 2d 314 (1968) and United States v. De Georgia, 420 F 2d 8879 (1969).

(17) See in particular United States v. Jones, 554 F. 2d 251, 7 C.L.S.R. 322 (5th Cir 1977) and United States v. Verlin, 466 F. supp. 155, 7 C.L.S.R. 323 (N.D. Tex 1979).

(18) Federal Rules of Evidence, Pub. L. No 93.595.88 Stat. 1926 (1975) Rule 803 (6) and (7)

(19) See "A Reconsideration of the Admissibility of Computer Generated Evidence", University of Pennsylvania Law Review, vol. 126, 1977, 432.

(20) Lucas v. William and Sons, [1892] 2 Q.B. 113, p. 116, C.A. per Lord Esher, M.R.

(21) See in American law King v. State ex. rel. Murdock Acceptance Corp, reference at note (4) supra.

(22) Kajala v. Noble, (1982).

(23) A. Kelman and R. Sizer, "The Computer in Court", Gower, 1982, p. 20 (a contrario).

(24) J.J. Roberts, op. cit. supra note (10) and King v. Murdock Acceptance Corp., supra.

(25) See Harned v. Credit Bureau, 513 2d, 650 (Wyo 1973).

(26) Cf. the thesis of Hauser, "Objectivisme et subjectivisme dans l'acte juridique, Paris, 1970.

(27) J.-L. Aubert, "Notions et rôle de l'offre et de l'acceptation dans la formation du contrat", (Thesis, Paris), 1970, 188.

(28) Notwithstanding Recommendation no R (81) 20 of the 11 December 1981 of the Committee of Ministers of the Council of Europe which requests the governments of those Member States whose legislation imposes evidence by written document "to examine the possibility of abolishing this requirement". On this requirement and the Recommendation, see X. Linant de Bellefonds, "L'informatique et le droit", P.U.F. 1981, 43.

(29) Cass. comm. fr. 19 Nov. 1973, Bull. civ., 1973, IV, no 333; G. Goubeaux, and D. Rihl, Preuve, Dalloz, Rép. dr. Comm.

(30) This argument is not conclusive since as F. Chamoux points out (op. cit. note (1)), a secret code is a much safer method of identification than a signature. It is also worth pointing out that a whole series of draft international conventions (on cheques, promissory notes, bills of exchange, commercial transport documents) accept mechanic or electronic means of identification (cf. "Aspects juridiques du traitement automatique des données", Report of the Secretary General, United Nations Commission on International Trade, A/CN 9/254 8 May 1984, 3 no 8).

(31) See D. Syx, "Aspects juridiques du mouvement électronique de fonds", Brussels, Kredietbank, 1982.

(32) On this point see in particular J. Van Ryn and J. Heenen, "Principes de droit commercial, vol. 1, 2nd ed., 1975, 484 on Article 109 of the French Commercial Code, implemented by the Law of 12 July 1980: "With regard to traders, commercial acts can be proved by any means".

(33) X. Malengraux, "Le droit de la preuve et la modernisation des techniques de rédaction, de reproduction et de conservation des documents", Annales de Droit de Louvain, 1982, 117 and the references cited at note 28. Cf. in the jurisprudence, recently Cass. française 7 January 1982, Bull. cass. 1982, III, 4: "The Court of Appeal did not comply with the terms of the new Article 202 of the Procedural Code by refecting written depositions on the grounds that their authors had not respected the conditions relating to form provided by the Article, whereas the penalty for non-compliance with these conditions is not nullity".

(34) According to N. Catala, "La nature juridique du paiement", Paris, L.D.G.J., 1961. In effect, it is the legislation which, de plane, attaches an extinctive effect to this factual situation which constitutes the satisfaction of the creditor.

(35) On this point see X. Malengraux, op. cit. supra note (33), 116; also J. Van Rijn and J. Heenen, "Traité de droit commercial", vol. 1, 481; P. Malinvaud, "L'impossibilité de la preuve écrite, J.C.P. 1972, I, 2468. In Belgian jurisprudence, Liège, 20 June 1978, Jur. Liège, 21 October 1978.

(36) F. Chamoux, La loi du 12 juillet 1980: "Une ouverture de nouveaux moyens de preuve", J.C.P. 1980, II, B 491.

(37) As concerns arbitration, the State Arbitration Commission of the USSR has recommended to arbitration tibunals to give transactions concluded by computer the same value as those concluded by written document. See "Transnational Data Report", vol. 6, no 2, p. 75.

(38) R. David, "Les grands systèmes de droit contemporains", 4th ed. 1971, § 316.

(39) D. Kirby, "Aspects juridiques de la technologie de l'information", in "Une analyse préliminarie des problèmes juridiques dans l'informatique et les communications", Paris, OECD, 1983, 83.

(40) U.N.C.I.T., "Aspects juridiques du traitement automatique des données, A/CN. 9/238, p. 2, no 5.

(41) U.N.C.I.T. op. cit. note (40)