Computer Evidence

Amory, Bernard; Poullet, Yves

Published in:
International Computer Law Adviser

Publication date:
1987

Document Version
Publisher's PDF, also known as Version of record

without using a similar structure, sequence or organization in their audiovisual displays.

B. Publishers, distributors, and other marketers of third party software products should:
   1. Review the audiovisual display of proposed products for possible infringement;
   2. Obtain representations and warranties that the licensed work, both internally and as presented in its audiovisual display, is an original work of authorship; and
   3. Include indemnification clauses in license agreements that require modification or replacement of software to avoid infringement.

C. End-users or others who contract for the development or licensing of computer software should:
   1. Draft the agreements that assign copyrights and other rights in computer software to include all rights in its structure, sequence, and organization and in original screens and other audiovisual display material for the product;
   2. Insure that multi-user/single computer (single CPU) license agreements expressly provide for multiple terminal display of the licensed software (the statutory privilege under 17 U.S.C. § 117 to use the software on "a machine" is probably not sufficient to cover multiple terminal display of the visual screens of the product even when a single copy of the software is operated on only one multi-user computer); and
   3. Check indemnification clauses to assure that coverage extends to claims for copyright or other infringement of the audiovisual display of third party materials.

Mr. Russo is a partner in the Palo Alto, California, law firm of Nelson & Russo, and is a member of our International Editorial Board.

EUROPE

Computer Evidence—A Comparative Approach in Civil and Common Law Systems: Part I

BY BERNARD E. AMORY AND YVES POULLET

Introduction

The amount of information that companies must maintain, often for long periods, whether for legal reasons or in the interests of good business management, in some cases can cause serious storage problems, thereby affecting overhead costs.[1] One of the advantages of the use of computers in business is their ability to reduce the volume of documents kept in archives and facilitate their processing. There is no longer any doubt that companies need to be able to computerize 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, which is still at the initial stage of its development, 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 output microfilms) constitute the basis of valid evidence for the purpose of legal proceedings? Do these processes conform to the requirements of accountancy, fiscal, employment and social security laws relating to the preparation and storage of certain documents? Do transactions that nowadays can 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 and American law) and the civil law (more particularly French and Belgian law). This approach will be preceded by a general summary of the credibility of computer documents and followed by some thoughts on the technical solutions to the legal issues in question.

Credibility of Computer and Telematic Documents

To what extent do documents processed by computer and/or obtained by telematic medium faithfully reflect the information that they purport to contain? These documents are subject to two

types of risk: errors and fraud.

Risk of Error

Errors have different origins: human, technical or external. The type of error that would appear to be most frequent is human error.[3] The risk of such error occurring is greatest in two situations: when data is being loaded into a system and when it is being processed. So, for example, with electronic fund transfers, the absence of a universal language for messages creates the risk of human error in interpreting and coding by the involvement of different operators in the transmission of a bank order.[4]

External errors are attributable to the environment. Bad temperature or humidity conditions, the presence of dust, vibration, static electricity or electromagnetism, irregular power supply, etc., are all factors that can be the cause of a breakdown, which in turn can damage or destroy data.

Finally, technical error can be created by a malfunction of software, hardware or the data transmission system linking different computer systems. Due to technical progress, errors resulting from faults in hardware or software have become increasingly rare,[5] whereas failures in communication systems are still common. On the other hand, the former can entail serious consequences due to their often repetitive nature.

Generally, it can be said that computers and telematics have diminished the risk of error in the preparation, storage and transmission of data, but that the consequences of an error, which are always statistically possible, can be more serious than in traditional systems, given the large number of operations that can be carried out by one machine in a short space of time.[6]

Risk of Fraud

The element that distinguishes fraud from error is intent.[7] Its origin, therefore, is human. In contrast to error, fraud represents a very important risk and is at present considered by those in the computer industry to be a major problem.[8] In fact, although estimates are very difficult to make (very few cases of fraud are disclosed), fraud has been estimated to involve $100 million annually in the United States and $30 million per year in Japan.[9]

Fraud can be committed by employees of a company or bank who know how to operate the access keys to the computer system and use this knowledge to their own ends. The classic example is when a bank employee programs the computer to misappropriate funds. Third parties can also commit fraud by accessing and manipulating a system, notably in telematics networks where the use of telecommunication systems facilitates such fraudulent access. When the defrauder interferes with such systems, for example by deliberately blocking their lines, the term used is computer or telematic sabotage. Another form of fraud is an authorized users unlawful use of his right of access to a system, such as the use of an electronic fund transfer system above the credit limit set by the bank.

In the case of both fraud and error, the risk increases with the complexity of the system required for the processing or communication of information. This complexity results as much from the number of computers and the amount of software as from the number of operations performed. As a result, telematics networks are exposed to this risk to a greater extent than individual systems due to the involvement of a greater number of people and computers, and above all the vulnerability of the intercommunications between computers. Furthermore, data that is simply stored in a computer will be less at risk than valuable data that undergoes more complex processing.

The fact that there are risks that threaten the credibility of documents processed by computer or created by telematics does not mean that they cannot be relied upon. On the contrary, effective methods of prevention, detection and correction of errors and fraud significantly diminish their effects and increase the reliability of these documents. However, one must remember that the value of a computer document will always depend on the value of the data loaded into the computer in the first place, as expressed by the acronym "gigo" (garbage in, garbage out).

Common Law Approach

The law of evidence under the common law, which is characterized by the wealth, the precision and the technical nature of its rules, contains two fundamental principles that would appear to be major obstacles to the admissibility of computer and telematic documents as evidence of the information that they contain. These are the "hearsay" and "best evidence" rules.

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 a person who has personal knowledge of the fact he is asserting. He is 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.

When data, such as invoices, 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, those of the coder, who is not necessarily the author or even answerable to him, and finally the computer, since in processing and storing the information, the computer is capable of altering it. Since by their nature, computers cannot be cross-examined, legal writers[10] and the case law[11] 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 (*e.g.*, bills, order forms), which constitute the originals. The originals are often destroyed after being recorded on the computer. Even when there is no written document that could serve as the basis of a computer document, for example in the case of direct recording of information, 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 human readable form is only a transcription of that data and, as such, is not admissible in 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 be examined below.[12]

Hearsay Rule—English Law

Because of a lack of existing exceptions to the hearsay rule that would grant admissibility to computer documents as evidence of the facts that they contain, and given the fact that it is impossible for courts to create new exceptions to this rule,[13] Parliament acted in 1968[14] by introducing provisions relating specifically to computer documents as part of a series of new, general provisions concerning hearsay evidence.

The Civil Evidence Act 1968 (the "Act") makes admissible "first-hand" hearsay.[15] Applied to computers, this rule means that a computer document is admissible if the person who loaded the data into the computer had personal knowledge of it, or, acting within the scope of his duties, received the data from a person who had such knowledge.[16] These provisions do not apply when a computer document does not originate with a written document of which a person has direct and personal knowledge. Such is the case with a transaction performed at an automated teller machine, or a recording by optical reading. In these circumstances, section 5 of the Act sets forth specific conditions relating exclusively to the admissibility of evidence in the form of computer documents. Pursuant to these conditions, a computer documents is admissible if—

- it was produced by a computer regularly used for the normal activities of its user;
- the computer is regularly supplied with information of the kind contained in the document submitted as evidence;
- the computer was operating properly at the moment of the information was recorded; and,
- 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 its 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. It is then for the court to decide its probative value, taking into account all the circumstances, notably the degree of simultaneity between the occurrence of a fact and its recording on the computer, as well as any interest that any person who is implicated might have in altering the data.[17]

These provisions have been much criticised[18] for the definitions that they contain and the conditions of admissibility that 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 that 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 the adaptation of the law by the Civil Evidence Act, the English Parliament 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" include 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 that the Companies Acts oblige them to keep other than in directly readable form as long as they can be reproduced in readable form.

Hearsay Rule—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[19] and adopted without major alteration by a majority of states. This exception provides that business records[20] are admissible as evidence without the requirement of oral evidence by their author if the transactions that they record were performed in the normal and regular course of business and recorded at the time or shortly after they were performed.[21]

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 nevertheless can be criticised; information is often stored only in electronic or magnetic form and only printed in

legible form if this proves necessary (*e.g.*, 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,[22] which gave rise to much case law[23] on the subject. The judgment of the Nebraska 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 simultaneity 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.[24] 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, these 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,[25] and stated that the exception applies to information stored "in any form" that, according to official commentaries,[26] 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.

Best Evidence Rule—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.[27] 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 (*e.g.*, direct recording).[28] 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, for in reality only as a printout is the document legible by man, and therefore, able to be put before the court.

The requirement of proof of non-availability of the original was abolished in 1982 for copies of films and audio recordings by a decision that held that they are by their nature reliable.[29] According to certain writers, this decision could be applied to computer documents.[30] Such an interpretation should be qualified: an extension of this rationale to computer documents containing information that has undergone fairly complex processing does not seem well-founded since, under 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 (*e.g.*, 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 the courts have not yet clarified this point.

Best Evidence Rule—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.[31]

Another exception that can be used is the "voluminous records" exception, by virtue of which a summary (possibly in computer document form[32]) is admissible in the place of the original when the original is too complex of lengthy to be put before the judge and where the opposing party has had the opportunity to examine the originals; this presupposes that they have not been destroyed.

[Part II of this article will appear in the February 1987 issue of the Adviser.*]*

Bernard Amory is an associate with the law offices of Dechert, Price & Rhoads, and assistant at the Computer and Law Research Centre, University of Namur, Belgium.

Yves Poullet is a lecturer at the University of Namur and Director of the Computer and Law Centre at the University.

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

2. *Id.*

3. Dehetre, "Data Processing Evidence, Is it Different?" *Chicago-Kent L. Rev.* 570 (1975); Fenwick & Davidson, "Use of Computerized Records as Evidence," *Jurimetrics J.* 21 (1975); Reese, "Admissibility of Computer Kept Business Records," *Cornell L. Rev.* 1969-70; Sprowl, "Evaluating the Credibility of Computer Generated Evidence," *Chicago-Kent L. Rev.* 543 (1975).

4. See on this the efforts made by the International Standards Organisation (ISO). *Cf.* United Nations Commission for International Commercial Law, Doc. A/CN.9/250/Add. 4, 11 *et seq.*

5. United Nations Commission for International Commercial Law, Doc. A/CN.9/250/Add. 4, 10.

6. *Id.* at 11.

7. For a study of computer fraud, see Sieber, "Gefahr und Abwahr des Computer Kriminalität," *Betriebsberater*, Aug. 30, 1982.

8. D. Parker, Combattre la criminalité informatique (Paris, OROS, 1985); Comer, "How to Prevent Computer Fraud," *Asian Banking* 35-37 (1982).

9. Briat, "La fraude informatique," *L'Observateur de l'O.C.D.E.*, March 1984, at 36.

10. M. Scott, Computer Law, ch. 10 (1984); D. Bender, Computer Law: Evidence and Procedure (1978); Lacey, "Scientific Evidence," *Jurimetrics J.* 254 (1984); Note, "Appropriate Foundation Requirements for Admitting Computer Printouts into Evidence," 1977 *Wash. U.L.Q.* 59; Fenwick & Davidson, *supra* note 3; Roberts, "A Practitioner's Primer on Computer Generated Evidence," *U. Chi. L. Rev.* 254 (1974); Tapper, "Evidence from Computer," *Georgia L. Rev.* 562 (1974); Mills, Lincoln & Laughead, "Computer Output, its Admissibility into Evidence," *Law & Computer Tech.* 14 (1970); Reese, *supra* note 3; Smith, "Admissibility of Computer Business Records: An Exception to the Hearsay Rule," *N.C.L. Rev.* 687 (1969-70); Wallace, "Computer Printouts of Business Records and their Admissibility in New York," *Albany L. Rev.* 61 (1967).

11. *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. 39; *Regina v. Ewing*, [1983] 3 WLR 1.

12. We are not going to examine the situation in other common law jurisdictions. In Australia, the South Australian Evidence Act 1972 is based on the Civil Evidence Act 1968, while departing from it to take into account certain criticisms that had been levelled at the English legislation. The Australian legislation, however, has already been the subject of proposed reforms. *See* 56 *Australian L.J.* 153 (1982). Colin Tapper has written a commentary on the Australian provision. *See* Tapper, *supra* note 10, at 604-12. In South Africa, measures adopted in 1983 allow the presentation in evidence of computer documents on condition that their author may be cross-examined and on the production of an affidavit, from which obligation, however, banks, insurance companies, and government departments are exempt. In addition, Canada is planning a reform of the Canadian Evidence Act 1982 (s.33). *Cf.* 6 *Transnational Data Rep., No. 5, at* 245. Finally, on the subject of arbitration, the State Arbitration Commission of the USSR has proposed that arbitration tribunals should accept computer documents that are put before them. 6 *Transnational Data Rep.*, No. 2, at 75.

13. The House of Lords decided in *Meyers v. Director of Public Prosecutions*, [1965] AC 1001, that no new jurisprudential exceptions to the hearsay rule could be created.

14. Civil Evidence Act 1968, Halsbury's Statutes of England, Annual Volume 1968, 1211.

15. Civil Evidence Act 1968, § 2.

16. Or even other person also acting in the exercise of their duties as long as at the end of the chain is someone with a personal knowledge of the information. *See* Civil Evidence Act 1968, § 4.

17. 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, *supra* note 10, at 82. There is insufficient English case law on this subject to allow conclusions to be drawn.

18. A. Kelman & R. Sizer, The Computer in Court 21 (Gower 1982); Tapper, *supra* note 10, at 604-12; 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 831 (1982).

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

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

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

22. Transport Indemnity Co. v. Seib, 178 Neb. 253, 132 N.W.2d 271 (1965).

23. *See in particular* King v. State *ex rel.* Murdock Acceptance Corp., 222 So.2d 393 (Miss. 1969); Merrick v. United States Rubber Co., 7 Ariz. App. 433, 440 P.2d 314 (1968); United States v. De Georgia, 420 F.2d 889 (9th Cir. 1969).

24. *See in particular* United States v. Jones, 554 F.2d 251 (5th Cir. 1977); United States v. Verlin, 466 F. Supp. 155 (N.D. Tex. 1979).

25. Federal Rules of Evidence, Rule 803(6), (7) (1975).

26. *See* "A Reconsideration of the Admissibility of Computer Generated Evidence," 126 *Univ. Penn. L. Rev.* 432 (1977).

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

28. *See* in American law *King v. State ex rel. Murdock Acceptance Corp.*, 222 So.2d 393 (Miss. 1969).

29. Kajala v. Noble (1982).

30. A. Kelman & R. Sizer, *supra* note 18, at 20 (a contrario).

31. Roberts, *supra* note 10; *King v. State ex rel. Murdock Acceptance Corp.*, 222 So.2d 393 (Miss. 1969).

32. *See* Harned v. Credit Bureau, 513 P.2d 650 (Wyo. 1973).