THE ADMISSIBILITY OF COMPUTER-GENERATED EVIDENCE: AN OVERVIEW

Johanne Gauthier

Partner

OGILVY RENAULT, S.E.N.C.

INTRODUCTION

During my presentation, I will have focused on initiatives taken to foster electronic commerce and the resulting increased use of electronic data interchanges as well as computer records.

Most experts predict that electronic transactions will become in the next five years, a predominant method of contracting domestic and international sales.

Are our rules of evidence flexible enough to accommodate these developments? Should the use of the technology be delayed by rules of law adopted at a time when no one dreamed of a "virtual shopping centre"? Is the paperless transaction valid? How can one prove it?

This paper is not meant to give a complete answer to these questions. These issues could be reviewed by a panel at the next Seminar.

At this time, I will only endeavour to give a brief overview of existing rules dealing with the admissibility of computer-generated evidence in Canada as well as in the U.K., Australia and the United States of America.

THE BRITISH EXPERIENCE

Computer-generated evidence has been the object of special legislation in the United Kingdom for several years. The admissibility of electronic evidence, in British law, obeys to different rules than those

applicable to traditional documentary evidence. These special provisions are found in the *Civil Evidence Act 1968* and the *Police and Criminal Evidence Act 1984.*

Section 5 of the *Civil Evidence Act 1968* provides that a computer-produced document shall be admissible as evidence of the statement contained therein, provided the proponent demonstrates its authenticity. The party who wishes to tender an electronically-produced document as evidence must establish that:

(a) the document was prepared during a period over which the computer regularly stored or processed information;
(b) over the relevant period of time, information of this type was regularly supplied to the computer;
(c) the computer was operating properly; and
(d) the information contained in the statement reproduces information supplied to the computer[1].

If one of these conditions is not met, the document is simply inadmissible as evidence.

In addition to proving the authenticity of the document, the proponent of an electronically-produced document must also demonstrate its reliability, through the production of a certificate signed by a person responsible for the operation of the computer[2]. As for the probative weight of

---

1 *Civil Evidence Act 1968,* s. 5(2).
2 *Civil Evidence Act 1968,* s.5 (4).

computer-produced evidence, section 6 of the *Civil Evidence Act 1968* requires that in estimating the weight of the document, the Court must examine the contemporaneity of the recording of the information with the events described in that record, and the motive of any person to misrepresent the facts recorded. Finally, section 8 of the *Civil Evidence Act* establishes that the Rules of Court must require that the proponent of such evidence give notice to its adversary of its intention to use electronically-produced evidence.

Computer-generated evidence is also the object of special provisions applicable to criminal proceedings. Section 69 of the *Police and Criminal Evidence Act 1984* provides that computer-produced evidence is admissible in criminal proceedings as long as there exists no reasonable grounds for believing that the statement it contains is inaccurate because of improper use of the computer and that, at all material times, the computer was operating properly or that the malfunction did not affect the production of the document or the accuracy of the statement. Finally, section 69 of the *Police and Criminal Evidence Act 1984* requires that the Rules of Court concerning giving notice are satisfied[3].

The application of section 5 of the *Civil Evidence Act 1968* and section 69 of the *Police and Criminal Evidence Act 1984* has led to many uncertainties. The most often expressed criticism towards section 5 of the *Civil Evidence Act 1968* relates to its ambiguity and complexity opening the door to a number of technical arguments which could result in the exclusion

---

3 The *Police and Criminal Evidence Act 1984* requires, as does the *Civil Evidence Act 1968*, that the party who wishes to use computer-generated evidence give notice to its adversary of its desire to do so.

of vital evidence stored or produced by a computer[4]. The complexity of the legislation dealing with the admissibility of computer-generated evidence has led Courts into different directions, resulting in a somewhat confusing case law. The apparent confusion stems from the qualification given to computer-generated evidence: does it constitute hearsay or real evidence? For example, in ***R.*** v. ***Spiby***[5], the Court of Appeal held that printouts from an automatic telephone call logging computer installed in a hotel were admissible as they constituted real evidence. The Court concluded that in the absence of evidence to the contrary, the machine is held to be in working order at the material time.

In ***Camden London Borough Council*** v. ***Hobson***[6], the Court stated that computer-generated evidence constituted real evidence if the statement originated in the computer. It would then be admissible as the record of a mechanical operation in which human information had played no part; however, a statement originating from a human mind and subsequently processed by a computer would be inadmissible as hearsay[7].

Proof of the reliability of a computer-generated document is also a crucial condition to its admissibility. In a recent judgment[8], the House of Lords accepted into evidence the information provided by an intoximeter although the computer clock was inaccurate. The Lords found that the inaccuracy did not affect the processing of the information supplied to the

---

4 R. BRADGATE, "Evidential Status of Computer Output and Communications", (1960) 6 Compute Law & Practice, 142.

5 [1991] Crim. L.R. 199 (C.A.Cr.D.).

6 *The Independent*, January 28, 1992, 24 (Clerkenwell Magistrate's Court).

7 *Id.*

8 *Director of Public Prosecution* v. *McKeown*, [1997] NLOR No. 135, (House of Lords)

computer. Section 69 of the Police and Criminal Evidence Act 1984 should be interpreted according to its purpose so as to not exclude otherwise accurate evidence. Lord Hoffman concluded that:

> "The purpose of section 69, therefore, is a relatively modest one. It does not require the prosecution to show that the statement is likely to be true. Whether it is likely to be true or not is a question of weight for the justices or jury. All that section 69 requires as a condition of admissibility of a computer-generated statement is positive evidence that the computer has properly processed, stored and reproduced whatever information it received. It is concerned with the way in which the computer has dealt with the information to generate the statement which is being tendered in evidence of a fact which its states."[9]

AUSTRALIA

In 1995, Australia adopted a new Commonwealth *Evidence Act*[10] One of the objectives of the new *Act* was to provide the rules of evidence which corresponded to the rapidly changing world of computer technology and information processing. In order to attain that objective, special provisions for electronic evidence were included in the new *Act*. Section 71 of the *Act* creates a new exception to the hearsay rule for documents transmitted by electronic mail, fax, telegram or telex. It stipulates that the hearsay rule will not apply to such a document provided the statement contained in such document goes to the identity of the author, the date or time at which the message was sent or the destination or identity of the person to whom the person the message was addressed.

---

9 *Id.*, para. 29.
10 *Evidence Act 1995 (Cth).*

Section 146 creates a presumption of working accuracy of a particular device or process. Indeed, it stipulates that:

> "If it is reasonably open to find that the device or process is one that, or is of a kind that, if properly used, ordinarily produces that outcome, it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that, in producing the document or saying on the occasion in question, the device or process produce that outcome"[11]

Section 147, on the other hand, provides a presumption of accuracy for business documents produced by a particular device used for the purposes of that business. The presumption can be set aside with sufficient evidence to raise a doubt as to the accuracy of the document. In other words, the *Evidence Act 1995 (Cth)* now removes the requirement for evidence as to the working accuracy of a particular device or computer.

Much like in the United Kingdom, the Australian legislation concerning the admissibility of computer-generated evidence is also the object of some criticism as the statutory provisions do not take into the account the accuracy of the input to the computer as well as errors propagated through computer systems[12]. However, it must be noted that sections 166 to 169 of the *Evidence Act* give the party against whom such evidence is adduced some degree of protection, by authorizing that party to request the production of documents and the right to examine, test or copy the whole or part of the

---

11 *Id.*, s. 146(2).

12 Lynda CROWLEY-SMITH, "The Evidence Act 1995(Cth): Should Computer Data be Presumed Accurate?", (1996) *Monash University Law Review* 166, 173.

document and to examine or test the way the document has been produced or kept.

THE UNITED STATES

There are hundreds of cases dealing with this topic in the United States and they are based on a variety of state laws. As there is no uniformity in the wording and requirements provided for in such statutes, there are often conflicting decisions which can create some confusion as to the admissibility of computer-generated evidence.

Although there exists no nation-wide comprehensive law on the admissibility of electronic evidence, the *Federal Rules of Evidence* provide the requirements for the authentication of documentary evidence, a prerequisite step for the admission of such evidence. The *Federal Rules of Evidence* deal with authentication without distinguishing between computer-generated evidence and other forms of documentary evidence. One must then conclude that the requirements for traditional documentary evidence also apply to computer-generated evidence.

Federal Rule of Evidence 901 describes authentication as a condition precedent to admissibility, "satisfied by evidence sufficient to support a finding that a matter in question is what its proponent claims"[13]. If a document is produced by a process or system, one must demonstrate that such process or system produces an accurate result[14].

---

13 *Federal Rule of Evidence* 901(a).
14 *Federal Rule of Evidence* 901(b)(9).

Business records are also the object of a special provision as regards their admissibility into evidence. Indeed, *Federal Rule of Evidence* 803(6) authorizes the admission into evidence of business records as an exception to the hearsay rule if shown by the testimony of a qualified witness that the records are made contemporaneously to the event recorded by a person with knowledge and are kept in the course of a regularly-conducted business activity, unless circumstances indicate lack of trustworthiness. This requirement for authentication remains in the case of computer-generated records.

Although recent case law seems to have adopted a more liberal view towards admitting computer-generated evidence, earlier decisions applied a certain number of constraints to the admission of such evidence. For example, in ***King*** v. ***State ex. rel Murdoch Acceptance Corp.***[15], the Supreme Court of Mississippi suggested that hardware is reliable in light of its general use and reliance in the business community. However, the Court, in this case, established guidelines for the admissibility of computer-generated business records. These guidelines included proof that the computing equipment was recognized as standard equipment, that the entries were made in the regular course of business, contemporaneously the event recorded, and that foundation testimonies satisfied the Court that the source of information method and time of preparation was such as to indicate its trustworthiness and justify its admission[16].

---

15 222 So. (2d) 393 (Miss. 1969).

16 *Id.*, 398.

Although these guidelines are very similar to those established by *Federal Rule of Evidence* 803(6), modern case law has been more generous with the admission of computer-generated evidence, shifting the debate towards the probative weight of such documentary evidence. For instance, in ***United States*** v. ***Linn***[17], the testimony of a hotel Director of Communications was sufficient to authenticate a record of telephone calls as he was on duty when the computer recorded the call in question.

In ***United States*** v. ***Catabran***[18], the Court admitted into evidence business records, although it was demonstrated that they contained inaccuracies. The Court held that these inaccuracies affected the weight and not the admissibility of the records. In another case[19], the security of a computer system was challenged by the party against whom the computer evidence was presented. In this case, the Court stated that:

> "the existence of an air-tight security system is not a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would be become virtually impossible to admit computer-generated records; the party opposing admission would have to show only that a better security system was feasible"[20].

CANADIAN LEGISLATION

Except for the *Civil Code of Quebec*, the provincial and federal laws of evidence do not provide any special treatment for deciding whether

---

17 880 F.2d 209 (9th Cir. 1988).
18 836 F.2d 453 (9th Cir. 1988).
19 *United States* v. *Glasser*, 773 F.2d 1553 (11th Cir. 1985).
20 *Id.*, 1559.

computer-generated evidence is admissible in any given case. The admissibility of electronically-produced evidence has been examined in many occasions, in the context of sections 29 and 30 of the *Canada Evidence Act*[21].

Before discussing the case law dealing with electronic evidence, we shall briefly review the statutory requirements regarding the admissibility of documentary evidence, including computer-generated evidence, in the federal legislation.

Section 29 of the *Canada Evidence Act* provides that copies of banking records shall be admitted into Court as evidence, provided that the party relying on the records demonstrates to the satisfaction of the Court that the entry in the record was made in the usual and ordinary course of business, that the record is in the custody of the financial institution and finally, that the copy is a true copy of the original[22]. Once these requirements are satisfied, the record is not only admissible, but also constitutes *prima facie* proof of the matters contained therein. Hence, section 29 not only provides the requirements for the admissibility of banking records, but also establishes their probative weight.

Since the *Canada Evidence Act* does not distinguish between computer-generated records and conventional paper records, it follows that electronically-produced banking records constitute *prima facie* proof of the statements they contain, provided the requirements for their admissibility are satisfied.

---

21 R.S.C. 1985, C-5.
22 *Id.*, s. 29(1).

Section 30 of the *Canada Evidence Act* establishes the requirements for the reception into evidence of business documents and records. According to the terms of this section, business records made in the usual and ordinary course of business may be received as evidence by production of the record, provided oral evidence is permitted[23]. Section 30 also allows the production of a copy of the record, if production of the original is not possible or not reasonably practical, provided the party relying on this evidence demonstrate the authenticity of the document. Authenticity is demonstrated through the production of affidavits attesting the nature of the impossibility and impracticality of producing the original document, identifying the source from which the copy was made and attesting the authenticity of the copy by the person who made it[24]. Once can immediately apprehend the problems the application of this section to computer-generated business documents may create. One of the questions raised by section 30(3) is whether a computer-produced business record printout is an original or a copy. What is considered as the original: the printout or the information contained in the memory of the computer? The application of either section 30(1) or 30(3) depends on the answer to this question, as yet unresolved in Canadian law.

---

23 *Id.*, s. 30(1). This requirement that oral evidence be permitted is crucial. It creates an impediment to the use of electronic documents whenever the law requires an act or contract to be done in writing. See for example, Carriage of Goods by Water Act, 1993. When a written document is required by law, oral evidence will not be admissible, thereby preventing the use of s. 30.

24 *Id.*, s. 30(3).

The Courts have attempted, in many occasions, to provide an answer to this question. In ***R.*** v. ***Sanghi***[25], the Court decided that the printout was an original record processed by a computer in the ordinary course of business. However, in ***Shah*** v. ***R.***[26], the defendant argued that printouts varying in form could not be considered as a record under section 30 of the *Canada Evidence Act*. The Court nonetheless accepted the records, concluding that the real record was the data electronically stored by the computer which took the form of strings of "ones" and "zeros". Such record may, however, be presented in different forms.

An area of uncertainty relates to the circumstances for the application of section 29 versus those for the application of section 30 of the *Canada Evidence Act*. In ***Symanski*** v. ***R.***[27], it was held that sections 29 and 30 of the *Canada Evidence Act* are independent sections. The document that may be inadmissible under one may be admissible under the other, and the particular sections can be interpreted in such fashion as to provide for the admissibility of computer printouts of financial institutions.

However, since the records of financial institutions are regulated by Section 29, shouldn't section 30 apply only to business records other than those kept by financial institutions?

In ***McMillan*** v. ***R.***[28], the Court noted that section 30 of the *Canada Evidence Act* differs from section 29 in that the probative value of

---

25 (1971) 6 C.C.C. (2d) 123 (N.S.S.C.).
26 [1991] B.C.J. No. 3869 (B.C.P.C.).
27 [1984] B.C.J. No. 200 (B.C.C.C.).
28 [1990] N.S.J. No. 335 (N.S.C.A.).

records admitted under section 30 is not fixed by statute but must be determined by the Judge. Once a document is admitted into evidence under section 30(3), its probative value is subject to the determination by the trial Judge under section 30(6).

As for the authentication of documents as required by the *Canada Evidence Act,* many decisions have dealt with this requirement in different fashions. The decision in ***McMullen*** v. ***R.***[29] deals with banking records under section 29 of the *Canada Evidence Act.* The summary conviction appeal court decided that the printout was a new type of copy made from a new type of record. The Court of Appeal agreed that "record" should be read broadly, but suggested that the proponent of a computer-generated evidence would have to lay fairly detailed foundations on the workings of the computer as a pre-condition to admission. A proponent will have to demonstrate the reliability of the computer evidence. According to this decision, the computer's memory would be the "record" and the printout would be a copy of that "record". The findings of the ***McMullen*** case were later reversed in the Supreme Court of Canada judgment ***Bell and Bruce*** v. ***R.***[30] which also deals with the admissibility of banking records under section 29 of the *Canada Evidence Act.* The Court concluded that the authenticity of a banking record as evidence was sufficiently guaranteed by compliance with section 29(2) of the *Canada Evidence Act.* The printout could then be admissible without foundation evidence as long as it complied with section 29(2).

---

29 (1979) 47 C.C.C. (2d) 499 (Ont. C.A.); (1978) 42 C.C.C. (2d) 67 (Ont. HCJ).

30 (1982) 65 C.C.C. (2d) 377 (Ont. C.A.); [1985] 2 R.C.S. 287.

As for documents falling under the scope of section 30(1), it was decided in ***Sheppard*** v. ***R.***[31] , that section 30(1) does not pre-authorize the admission in evidence of every record made in the ordinary course of business. Section 30(1) carries the necessary implication that such a record will be admitted when the Judge has examined it and exercised his discretion to accept it as being an authentic record of its contents made in the ordinary course of business.

The Courts have also examined the issue of the probative value of electronic evidence submitted under section 30 of the *Canada Evidence Act* in ***McMillan*** v. ***R.***[32], the Court of Appeal of Nova Scotia stated that the probative weight of records admitted under section 30 is not established by statute but must be determined by the Judge under section 30(6) of the *Canada Evidence Act.*

In ***McCulloch*** v. ***R.***[33], the Court concluded that a telephone call record showing that a call was made from one phone to another at a certain time was not admissible under section 30 of the *Canada Evidence Act,* since in that specific case, these records were not made in the usual and ordinary course of business of the telephone company. They were made as an extraordinary procedure for the purpose of producing evidence against the accused. The Court refused to admit the computer evidence under the common law exceptions to the hearsay rule but instead proceeded to treat these printouts as material or best evidence. It then found that the weight to

---

31 [1992] N.J. No. 73 (N.Fld S.C.T.D.).
32 *Supra,* note 35.
33 [1992] B.C.J. No. 2282 (B.C.P.C.).

be attached to such evidence will depend on the accuracy and integrity of the process employed.

On the other hand, in ***Kinsella*** v. ***Logan***[34], the Court accepted printouts of the nature of credit reports under the common law exception to the hearsay rule. The Court indicated that these records are not as reliable as primary financial records would be, but received the credit file as *prima facie* proof of the facts it contained.

As one can see, the application of sections 29 and 30 of the *Canada Evidence Act* to computer-generated documents raises some uncertainties. These uncertainties make it difficult for litigants to predict whether electronically-produced documents will be declared admissible under the relevant sections of the *Canada Evidence Act*. However, one must also recognize that although the grounds on which the documents are admitted into evidence tend to differ from one case to another, there seems to be a willingness to accept these documents into evidence.

In the last few years, the Uniform Law Conference of Canada (the "Conference") has studied the issue and attempted to resolve the uncertainties created by the application of section 30 of the *Canada Evidence Act* with respect to computer-generated evidence. The Conference has now proposed a series of amendments to the *Canada Evidence Act* in order to facilitate the admissibility of computer-generated documents[35].

---

34 (1995) 38 C.P.C. (3d) 128.

35 Gregory J.D., and Tollefson, E., Q.C., "Proposals for a Uniform Electronic Evidence Act", *Appendix N to the Proceedings of the Uniform Law Conference of Canada, 1995* (www.law.ualberta.ca/alri/ulc/95pro/e95n.htm).

In an effort to clarify the question of whether the printout of a record is a copy or an original, the Conference proposes a definition of "record" which should be applicable to all the provisions relating to documentary evidence. The Conference also proposes to define the term "computer" by referring to the definition found in section 342.1(2) of the *Criminal Code.* Moreover, the Conference suggests a definition of the word "original" so as to include both the data stored in the memory of the computer and the printout of that information. This approach would, according to the Conference, be consistent with the ruling in ***R.*** v. ***Bell and Bruce*** v. ***R.***[36].

In order to clarify the requirements for authentication of computer-generated documents, the Conference also proposes new requirements for authentication. The recommended requirements for the authentication of a computer-generated document are contained in sections 18.13 to 18.15 of the proposed *Canada Evidence Act.* The proposed amendments provide a description of authentication and establishes that the proponent of a record has the burden of establishing its authenticity[37]. The proposed amendments also suggest that the proponent be required to notify the other party of its desire to present computer-generated evidence[38]. The Conference also proposes that proof of the authenticity of the record be deemed to be waived unless, within five (5) days after receiving notice from the proponent, the other party has filed with the Court a notice requesting

---

36 *Supra.*

37 Proposed amendments to the *Canada Evidence Act*, S. 18.13. This definition of authentication is similar to the one established by the *United States Federal Rule of Evidence* 901(a).

38 *Id.*, S. 18.14.

proof of the record's authenticity[39]. Finally, section 18.15 of the *Proposed Canada Evidence Act* provides indications as to how the proponent of an electronically-produced record can satisfy the evidential burden as to its authenticity.

These amendments and others suggested by the Conference are aimed at resolving some of the problems related to the application of sections 29 and 30 of the *Canada Evidence Act* to computer-generated evidence.

While waiting for Parliament to amend the *Canada Evidence Act*, it is crucial that the rules concerning the admissibility of computer-generated evidence are not giving too narrow an interpretation, so as to avoid the exclusion of otherwise relevant evidence. In order to do so, Courts may be inspired by the Supreme Court of Canada decision in ***R.*** v. ***Khan***[40], where the Court concluded that even a statement consisting of hearsay should be received "[...] provided that the guarantees of necessity and reliability are met, subject to such safeguards as the Judge may consider necessary and subject always to considerations affecting the weight that should be accorded to such evidence."[41]. The Federal Court of Canada can and should also take full advantage of the discretion given to it by Section 53(2) of the *Federal Court Act*.

---

39 *Id.* This proposed amendment is similar to article 89 of the *Quebec Code of Civil Procedure* which provides that the contestation of a document reproducing the data of a juridical act that are entered on a computer must be expressly alleged and supported by affidavit. Failing such affidavit, the document is held to be admitted.

40 [1990] 2 R.C.S. 531.

41 *Id.*, 548.

QUEBEC

Section 40 of the *Canada Evidence Act* provides that the laws of evidence in force in the province in which the proceedings are instituted will also apply. Section 53(2) of the *Federal Court Act* gives the Federal Court of Canada the discretion to rule evidence admissible if such evidence would be admissible in a similar matter in a Superior Court of a province notwithstanding section 40 of the *Canada Evidence Act*[42].

It is thus very interesting and very appropriate to review the Quebec experience as this province is the only one to have adopted specific provisions dealing with computer-generated evidence. In effect, since 1994, the *Civil Code of Quebec* contains a set of provisions which enable a party to prove the existence and terms of a contract by means of a computer-generated document. For convenience, the text of the relevant articles of the *Civil Code of Quebec* are reproduced hereinafter.

ART. 2837

> Where the data respecting a juridical act are entered on a computer system, the document reproducing them makes proof of the content of the Act, if it intelligible and if its reliability is sufficiently guaranteed. To assess the quality of the document, the Court shall take into account the circumstances under which the data were entered and the document was reproduced.

ART. 2838

---

42 See *Cornforth* v. *The Queen*, [1982] C.T.C. 45; *Kemanord AB* v. *PPG Industries Inc.*, [1981] 1 C.F. 567; *Network Music Inc.* v. *Distributions Madacy Inc.* (1990) 31 C.L.R. (3d) 174 (C.F.)

> The reliability of the entry of the data of a juridical act on a computer system is presumed to be sufficiently guaranteed where it is carried out systematically and without gaps and the computerized data are protected against alterations. The same presumption is made in favour of third parties where the data were entered by an entreprise.

ART. 2839

> A document which reproduces the data of computerized juridical act may be contested in any manner.

It should be noted that these articles only deal with the admissibility of computer-generated juridical acts. Therefore, they do not deal with the admission into evidence of information which is simply stored on a computer, such as records. Articles 2837 to 2839 would therefore apply to a situation where a contract was concluded by way of electronic data interchange or in other words, computer-to-computer communication (pure EDI). These articles would also apply to situations where individuals or corporations conclude a transaction by way of electronic communication. In such a case, a party who desires to prove the existence and the content of such a juridical act may do so by producing to the Court the document reproducing the data entered on the computer system, provided he or she demonstrates that the document is intelligible (ie. that the document is accessible and can be understood) and that its reliability is sufficiently guaranteed. Article 2838 establishes a presumption of reliability if it is demonstrated that the entry of data on the computer system is carried out systematically and without gaps, and that it is protected against alterations.

Therefore, once the party relying on the computer-generated document has demonstrated that it is intelligible and reliable, the document not only makes proof of the existence of the juridical act, but also makes proof of the contents of the act[43].

There exists some controversy as to whether article 2837 may be applied to juridical acts concluded by the traditional methods (verbal or written agreements) and subsequently entered on a computer system. The consensus amongst authors seems to be that such an interpretation of article 2837 is impossible since in order to be admitted into Court as evidence of a juridical act, a document must still satisfy the general requirements of admissibility of documents, one of which is the Best evidence Rule. Hence, if a juridical act was transferred on an electronic medium and the original hard copy destroyed, it is not certain whether the document reproducing the act entered on computer system would be admissible in Court since it would not constitute the best evidence, but secondary evidence[44]. It should also be noted that the *Code of Civil Procedure* provides that one may contest a document reproducing the data of a juridical act entered on a computer. However, such contestation must be expressly alleged and supported by affidavit, failing which, the document is held to be admitted[45]

As for other computer-generated documents, such as business records, they are admissible as testimony if notice is given to the adverse

---

43 It can however be contested by any means, ie. by means of oral as well as documentary evidence; see article 2839 C.C.P. but see also article 89 C.P.C.

44 Francine CHAMPIGNY, "L'inscription informatisée en droit de la preuve québécois", *Développements récents en preuve et procédure civile (1996)*, Cowansville, Les Editions Yvon Blais, 1996, 1, 10-11.

45 Art. 89, *Code of Civil Procedure.*

party and authorization of the Court is obtained[46]. When examining the request for such authorization, the Court shall ascertain whether it is impossible for the declarant to appear as a witness or that it is unreasonable to require him to do so, and that the statement presents sufficient guarantees of reliability[47]. However, in the case of business documents, article 2970(3) provides that documents drawn up in the ordinary course of business of an entreprise, documents entered in a register kept as required by law, and entries spontaneous and contemporaneous to the occurrence of the facts are presumed reliable.

Case law in Quebec has generally accepted as evidence computerized business records such as Hydro-Québec's records of consumption of electricity by a particular person. In fact, several cases have concluded that such computer-generated records can be admitted as proof of the services rendered by Hydro-Québec without the necessity of testimony by each and every employee who participated to the creation of the record[48].

CONCLUSION

The importance of the question of admissibility of electronic evidence has increased tremendously with the advent of the Internet. Electronic commerce is now accessible to everybody. Countries such as the

---

46 Art. 2870 al. 1, *Civil Code of Quebec.*

47 Art. 2870 al. 2, *Civil Code of Quebec.*

48 *Hydro-Québec* v. *Mondor*, C.P. Joliette, No. 705-02-000209-841, February 6, 1986, j. Charette; *Hydro-Québec* v. *Malouf*, C.Q. Montréal, No. 500-02-014314-897, December 17, 1983, j. Sylvestre; *Hydro-Québec* v. *Benedek*, [1995] R.L. 436 (C.Q.).

United Kingdom and the United States are in the process of reviewing their legislation in that respect. So is Canada.

In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted a Model Law on Electronic Commerce. This was a compromise between the Treaty process and the purely unilateral action of nations. It is a flexible approach that is likely to produce uniformity of national commercial laws as well as rules concerning the admissibility of computer-generated evidence. The Model Law addresses the question of authenticity and probative weight of computer-generated evidence. For example, its article 9(2) provides that:

> [i]nformation presented in the form of a data record shall be given due evidential weight. In assessing the evidential weight of a data record, regard shall be add to the reliability of the manner in which the data record was created, stored or communicated, and where relevant, the reliability of the manner in which the information was authenticated.

The Model Law also deals with issues such as "writing", "original" and "signature", concepts which also impact on the ability of a party to use and prove the contracts it concluded electronically.

Amendments to section 2 of the American Uniform Commercial Code have already been proposed to implement the Model Law with some adjustment and more details. The Uniform Law Conference of Canada started to work this fall on the text of the Statute for the implementation of the Model Law in Canada.

Canada is a leader in the field of software and high technology. It is therefore important that there be as little legal impediment as possible to the use and evolution of electronic commerce in our country. Certainty as to the admissibility of computer-generated evidence is therefore crucial. Companies must be able to determine how they should keep their electronic records and what they should do to avoid evidentiary problems if and when litigation occur. This is a big challenge for our governments but for our Courts as well.

UNCITRAL Model Law on Electronic Commerce

[Original: Arabic, Chinese, English, French, Russian, Spanish]

Part one. Electronic commerce in general

CHAPTER I. GENERAL PROVISIONS

*Article 1. Sphere of application**

This Law** applies to any kind of information in the form of a data message used in the context*** of commercial**** activities.

---

*The Commission suggests the following text for States that might wish to limit the applicability of this Law to international data messages:

"This Law applies to a data message as defined in paragraph (1) of article 2 where the data message relates to international commerce."

**This Law does not override any rule of law intended for the protection of consumers.

***The Commission suggests the following text for States that might wish to extend the applicability of this Law:

"This Law applies to any kind of information in the form of a data message, except in the following situations: [...]."

****The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

Article 2. Definitions

For the purposes of this Law:

(a) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

(b) "Electronic data interchange (EDI)" means the electronic transfer from computer to computer of information using an agreed standard to structure the information;

(c) "Originator" of a data message means a person by whom, or on whose behalf, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message;

(d) "Addressee" of a data message means a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message;

(e) "Intermediary", with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message;

(f) "Information system" means a system for generating, sending, receiving, storing or otherwise processing data messages.

Article 3. Interpretation

(1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

(2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Article 4. Variation by agreement

(1) As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of chapter III may be varied by agreement.

(2) Paragraph (1) does not affect any right that may exist to modify by agreement any rule of law referred to in chapter II.

CHAPTER II. APPLICATION OF LEGAL REQUIREMENTS TO DATA MESSAGES

Article 5. Legal recognition of data messages

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

Article 6. Writing

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

(3) The provisions of this article do not apply to the following: [...].

Article 7. Signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) The provisions of this article do not apply to the following: [...].

Article 8. Original

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

(3) For the purposes of subparagraph *(a)* of paragraph (1):

(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

(4) The provisions of this article do not apply to the following: [...].

Article 9. Admissibility and evidential weight of data messages

(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) on the sole ground that it is a data message; or,

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

Article 10. Retention of data messages

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

(a) the information contained therein is accessible so as to be usable for subsequent reference; and

(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs *(a)*, *(b)* and *(c)* of paragraph (1) are met.

CHAPTER III. COMMUNICATION OF DATA MESSAGES

Article 11. Formation and validity of contracts

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

(2) The provisions of this article do not apply to the following: [...].

Article 12. Recognition by parties of data messages

(1) As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

(2) The provisions of this article do not apply to the following: [...].

Article 13. Attribution of data messages

(1) A data message is that of the originator if it was sent by the originator itself.

(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:

(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or

(b) by an information system programmed by, or on behalf of, the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:

(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

(4) Paragraph (3) does not apply:

(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or

(b) in a case within paragraph (3)*(b)*, at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

Article 14. Acknowledgement of receipt

(1) Paragraphs (2) to (4) of this article apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by

(a) any communication by the addressee, automated or otherwise, or

(b) any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

(3) Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.

(4) Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or

agreed or, if no time has been specified or agreed, within a reasonable time, the originator:

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in subparagraph *(a)*, may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.

(6) Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

(7) Except in so far as it relates to the sending or receipt of the data message, this article is not intended to deal with the legal consequences that may flow either from that data message or from the acknowledgement of its receipt.

Article 15. Time and place of dispatch and receipt of data messages

(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:

(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:

(i) at the time when the data message enters the designated information system; or

(ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;

(b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).

(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;

(b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.

(5) The provisions of this article do not apply to the following: [...].

Part two. Electronic commerce in specific areas

CHAPTER I. CARRIAGE OF GOODS

Article 16. Actions related to contracts of carriage of goods

Without derogating from the provisions of part one of this Law, this chapter applies to any action in connection with, or in pursuance of, a contract of carriage of goods, including but not limited to:

(a) (i) furnishing the marks, number, quantity or weight of goods;

(ii) stating or declaring the nature or value of goods;

(iii) issuing a receipt for goods;

(iv) confirming that goods have been loaded;

(b) (i) notifying a person of terms and conditions of the contract;

(ii) giving instructions to a carrier;

(c) (i) claiming delivery of goods;

(ii) authorizing release of goods;

(iii) giving notice of loss of, or damage to, goods;

(d) giving any other notice or statement in connection with the performance of the contract;

(e) undertaking to deliver goods to a named person or a person authorized to claim delivery;

(f) granting, acquiring, renouncing, surrendering, transferring or negotiating rights in goods;

(g) acquiring or transferring rights and obligations under the contract.

Article 17. Transport documents

(1) Subject to paragraph (3), where the law requires that any action referred to in article 16 be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data messages.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for failing either to carry out the action in writing or to use a paper document.

(3) If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique.

(4) For the purposes of paragraph (3), the standard of reliability required shall be assessed in the light of the purpose for which the right or obligation was conveyed and in the light of all the circumstances, including any relevant agreement.

(5) Where one or more data messages are used to effect any action in subparagraphs *(f)* and *(g)* of article 16, no paper document used to effect any such action is valid unless the use of data messages has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of data messages by paper documents shall not affect the rights or obligations of the parties involved.

(6) If a rule of law is compulsorily applicable to a contract of carriage of goods which is in, or is evidenced by, a paper document, that rule shall not be inapplicable to such a contract of carriage of goods which is evidenced by one or more data messages by reason of the fact that the contract is evidenced by such data message or messages instead of by a paper document.

(7) The provisions of this article do not apply to the following: [...].