Dematerialized Transactions on Electronic Pathways: A Panorama of Legal Issues[1]

Karim Benyekhlef

Many habits will be changed, it is said, as multimedia take over communications pathways. The creation of communications networks carrying numerous types of information should allow users in their homes or workplaces to make purchases, perform banking operations, consult data banks and, possibly, download data files, order films, records or books (electronic editions), etc. Many of these operations are not new to such an electronic framework. European telematics experiments, especially in France using the Minitel, already permit reference to this type of electronic operation. However, these new means of communication (electronic highways) embody the ambition to push the experiment further. The transmission of voice, image, sound and data (Integrated Services Digital Network-ISDN) should lead to much more complex and diversified electronic operations than those occurring on the "traditional" telematics networks.

These new communications pathways have aroused the journalistic interest of the traditional media. Much ink has flowed concerning their technical capabilities and the supposed benefits and dangers of these capabilities. Analysis has often been limited to enthusiastic talk about the wonders of technology. No serious attention has been paid to the many legal issues related to these developments.[2] This is not to diminish the importance of the technical aspects of the phenomenon. Yet, one cannot claim to fully comprehend and understand this phenomenon if one reduces it to only its technical component. Obviously the latter might seem much more spectacular than its legal counterpart. However regardless of how impressive electronic highways may become, it remains undeniable that their integration and acceptance in the social and economic fabric will be dependent notably on the legal guarantees they can provide. In other words, the consumer will only be inclined to use these new services if they can offer a degree of legal security comparable to that provided in the framework of traditional operations. It goes without saying that this security can only be

1 This research was conducted with the support of the *Fonds FCAR* and the SSHRC.

2 Here we are obviously not referring to the, especially European, legal community which, with public and private support, has applied itself to these problems. This lack of attention is rather that of the media and the initiators of these new technologies.

E. Mackaay et al. (eds.), The Electronic Superhighway, 93–116.

offered after thorough analysis and consideration of the legal aspects of the new communications pathways.

We thus propose to give a brief presentation of the various legal issues raised by the new communications pathways in the domain of dematerialized transactions. Of course, this domain is only one aspect, among others, of the legal issue of new electronic communications pathways. The term "transaction" suggests that a relation of a commercial nature arises between a user and a service supplier. Most often, this relation is the purchase of material goods by a user through electronic means. This is called "teleshopping". However the term "transaction" can cover other types of operations. Thus, a user can subscribe to certain services which provide, for a fee, certain information (stock market and exchange rates, the timetables of transportation services, transportation purchase and reservation systems, downloading or consultation of books, films or records, etc.). We consider these too to be computer transactions.

The expression "transaction" also covers electronic data interchange (EDI). However, EDI represents a method of transaction proper to companies,[3] and we intend to limit our discussion to physical persons, to consumer-users of electronic services. Thus, computer transactions raise questions regarding evidence, consumer protection, civil liability and protection of the right to privacy. Similarly, it will be appropriate to say a few words about the resolution of conflicts likely to arise in the electronic context. Our discussion will concentrate more on giving a view of the panorama than on presenting definitive solutions and conclusions. This panorama will allow us to visualize the size of the task to be accomplished and the legal difficulties linked to the development of electronic communications networks. Before tackling these themes, we shall briefly describe the emergence and forms of communications networks.

1. Emergence and Forms

Here we will describe the Internet network which is often presented as paving the way for what is to be the electronic highway. Likewise, in light of European experiments, we will describe the various actual forms of telematic operations. This short discussion should allow us to better grasp the relations uniting the actors in this dematerialized universe.

---

3 On this subject, see especially: K. Benyekhlef, *Échange de documents informatisés. Contrat type commenté* (Québec, Publications du Québec, 1991); P. Trudel, G. Lefebvre and S. Parisien, *La preuve et la signature dans l'EDI au Québec* (Québec, Publications du Québec, 1993); S. Baum and H. H. Perritt Jr., *Electronic Contracting, Publishing and EDI Law* (New York, Willey & Sons, 1991); T. Piette-Coudol and A. Bensoussan, *L'échange de données informatisées et le droit* (Paris, Hermès, 1991).

About twenty years ago, the Internet saw the light of day. In fact, it was a network set up by the American Defence Department: the Arpanet network. The main goal of this experimental network was to allow uninterrupted transmission of information regardless of any imaginable catastrophe, including nuclear war.[4] Yet the network seemed fragile. At the same time, given the computer boom, researchers decided to create a single standard in order to allow different computers to communicate with each other. This resulted in the development of an Internet Protocol (IP).[5] In the early 1980's, the National Science Foundation, an American federal government organization, decided to create five super-computer centres and make them available to the whole university community. Thus these five centres were to be shared. It quickly became evident that a problem of communications traffic would arise. Rather than connecting each research unit to one of these five centres, it was decided that regional networks would be created to which the research units would be connected. Obviously, each of these regional networks would in turn be connected to one of the five super-computers. Over the years communications capacities were improved in order to prevent any system overload. This National Science Foundation program was to be the true source of the network of networks which is the Internet.

It is thus clear that the Internet's foundations are set in the will to give the scientific community the possibility to access super-computers for doing research. Researchers, noting that the various networks established could thus communicate with each other (IP), very naturally decided to use them in order to exchange information themselves. Moreover, the great number of networks coupled with the development of "packet switching"[6] permits data or a message to arrive at its destination using one of many available routes. In other words, a message sent from point A to point B does not necessarily take the route A-B. If this route cannot be used for whatever reason, the message can always, in principle, take the route A-C-B or A-C-D-B. This

---

4 Ed Krol, *The Whole Internet. User's Guide and Catalog* (Sebastopol (CA), O'Reilly & Associates Inc., 1993) at 11. See also: J. J. Quarterman and S. Carl-Mitchell, *The Internet Connection. System Connectivity and Configuration* (Reading, Mass., 1994) at 20.

5 Internet developers, responding to market pressures, began to put their IP software on every conceivable type of computer. It became the only practical method for computers from different manufacturers to communicate", Krol, *supra*, note 3 at 11.

6 "In packet switching, data to be sent over a network is divided into many discrete chunks of data, each usually not more than a few thousand bytes long and each called a packet. Each packet is self-contained and holds all the information required to send it to its final destination. Each packet is routed from one computer to the next across the network until it reaches its final destination. Dedicated computers are normally used to route packets from place to place, much like a smart relay; each of these computers is called a router", Quarterman and Carl-Mitchell, *Supra*, note 3 at 21.

extreme mobility and simplicity of circulation makes this mode of information transmission very attractive.

The Internet network belongs to no one. Krol compares it to a kind of church in which free expression belongs to everyone but in which there is no pope or president.[7] As Krol explains,

> "[t]he ultimate authority for where the Internet is going rests with the Internet Society, or ISOC. ISOC is a voluntary membership organisation whose purpose is to promote global information exchange through Internet technology. It appoints a council of elders, which has responsibility for the technical management and direction of the Internet. The council of elders is a group of invited volunteers called the Internet Architecture Board, or the IAB [...] Internet users express their opinions through meetings of the Internet Engineering Task Force (IETF). The IETF is another volunteer organisation; it meets regularly to discuss operational and near-term technical problems of the Internet."[8]

Of course there are other networks, with far fewer subscribers,[9] in the private sector: CompuServe, Prodigy, etc. Naturally, telephone, cable and television giants attempt to exploit these new technologies for commercial ends, completely foreign to the goals inspiring the Internet.[10] The success of the latter has not failed to attract the interest of these giants regarding the immense potential of the new electronic means of communication.

Telematics, or the coupling of computer and telecommunications technology, is in fact the first general-public use of the new communications pathways. It is a system which certainly appears embryonic given the numerous predicted possibilities of what are known as electronic highways. Yet we should not overlook the reflections this technology has spawned. In effect, while legal thought on telematics is not yet mature,[11] a good number of rules developed in this context are perfectly pertinent in that of electronic highways. How could it be otherwise? Both are cases of assessing the legal system which could be established in the framework of a remote relation between a user and a service supplier. Certainly, the services offered, or

---

7 Krol, *supra*, note 3 at 13.

8 *Ibid.* at 14.

9 It is estimated that there are between 8.9 and 17.8 million Internet users (Quarterman and Carl-Mitchell, *supra*, note 3 at 5); this obviously makes it the largest electronic network in the world.

10 See, among others, Astrad Torres, "*Sur les 'autoroutes de la communication': la ruée des géants de la Finance*", and Herbert I. Schiller, "*Reléguer le bien public sur les bas-côtés*" (Paris, Le Monde diplomatique, March 1994) at 18-19.

11 Regarding Canada's situation in this domain, see P. Trudel and F. Abran, *Un état des questions juridiques posées par l'avènement de la télématique grand public*, Report written for the Ministère des Communications du Québec, Centre de recherche en droit public, Université de Montréal, July 1989.

rather which the communications giants propose to offer, demand the development of new legal solutions fitted to technological change. However, given the present situation, telematics is undoubtedly the most adequate model to be used as an analogy since it carries the seed of the aspirations of the new communications pathways. In fact, it is extremely possible that the term "telematics" will continue to designate, in the years to come, the most technically advanced forms of electronic communications. In this respect, the vocabulary should not obscure the legal stakes underlying dematerialised transactions. Moreover, the term "telecommunications" is defined as follows in the 1982 International Telecommunications Convention: "Any transmission, emission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems". This leads Poullet and Monville to say that telecommunications, which with computers composes telematics, "includes classical, new and also future services."[12]

The ends of telematics operations can be professional or concern the general public. A professional goal "relates to the transmission of data within a company or to the outside."[13] EDI, for example, falls under this definition. We will examine instead general-public telematics, in other words, the myriad of services offered to the consumer. Telematics brings together four main actors:

- the user benefits from the service.[14] He or she is thus a physical person who, in general, initiates the telematics.[15]
- the carrier is the public or private enterprise which provides the telecommunications network. It acts as a conduit.
- the supplier or producer is the organisation which collects information,[16] creates files which can be accessed. The supplier thus offers a bank of information or services. In the latter case, these services can take various forms (teleshopping, telebanking, various information services, etc.).
- the server is the computer company which makes a set of equipment and software available to the supplier or producer.[17] The server "thus wholly or partially assumes the duties of putting in electronic form, production, management and advertising of services offered by telematic networks."[18]

---

12 Yves Poullet and Claire Monville, *La demande finale en télématique. Aspects juridiques* (Paris, La Documentation Française, 1988) at 19. [Trans. note: my translation.]

13 *Ibid.* at 24. [Trans. note: my translation.]

14 *Ibid.* at 25.

15 Trudel and Abran, *supra*, note 10 at 29.

16 Poullet and Monville, *supra*, note 11 at 25.

17 *Ibid.* at 72.

18 Trudel and Abran, *supra*, note 10 at 28. [Trans. note: my translation.]

These categories are not closed. In effect, a supplier can also play the role of server. It is then known as an integrated server.[19] Likewise, a carrier can offer telematic services, thus playing the role of a supplier, or it can be a server. In short the distribution of roles is far from exclusive. Yet attributing a role to an enterprise or public organisation has major legal implications since it very often determines its range of liability. In other words, in case of a wrong, it is important to clearly identify the actors in order to determine their degree of responsibility. Naturally, the degree of liability varies depending on the facts of the case, but also on the role played by each actor in the telematic operation. Furthermore, as communications giants rush into the telematic field, their concentrating tendencies could be a cause for changing these categories. It is possible that a single entity will be server, carrier and supplier.

Moreover, telematic services can themselves be classified. To do so is not merely capricious. In effect, "the legal system dealing with these operations depends on the nature of the service".[20] Poullet and Monville identify four main types of computer telecommunications services:

- information services including, for example, information on timetables, prices and calendars; the news; electronic directories;[21]
- teletransaction services including, in particular, banking and financial transactions, orders for consumer goods, hotel and show reservations[22];
- teleprocessing services, which "are operations through which the user attempts to achieve a result through a dialogue with the computer system, in other words a set of data, programs and processes,"[23] (video games, courses, management, accounting, etc.);
- transmission services, which "transfer data, messages, documents, files from one place to another."[24] Communications exchanges are the very purpose of this type of service.

Clearly other classifications remain possible.[25] However we will concentrate on teletransaction and information services. In the latter case, it seems to us that offering information can be, in certain cases, a transaction. The word "transaction" must thus be understood to apply to information.

---

19 Poullet and Monville, *supra*, note 11 at 25.
20 *Ibid.* at 32. [Trans. note: my translation.]
21 *Ibid.* at 48.
22 *Ibid.* at 34.
23 *Ibid.* at 34. [Trans. note: my translation.]
24 *Ibid.* at 35. [Trans. note: my translation.]
25 *Ibid.* at 36-46.

2. Evidence

A dematerialised transaction, for example the purchase of a consumer good, can raise difficulties in evidentiary law. The absence of a written document recognizing the transaction, and the absence of the traditional signature sealing the transaction, are undoubtedly the main problems concerning electronic transactions.[26] The telematic network, through its interactive nature, is used notably for producing juridical acts.[27] However it can also simply constitute the record of certain facts.[28] Quebec evidentiary law, in spite of its French civil origins, has been influenced by common law. Thus computer evidence runs up against principles forbidding hearsay and the best evidence rule, common law concepts, and the civil law principle of the document certifying the juridical act. We must first distinguish between evidence of acts and that of facts. We will also say a few words about signatures.

The new Quebec *Civil Code* deals with evidence of juridical acts in a section titled "Computerized Records".

> 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 is 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. "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 persons where the data were entered by an enterprise."
>
> Art. 2839. "A document which reproduces the data of a computerized juridical act may be contested in any manner."

---

26 A. P. Meijboom and A. Oskamp, "Evidence", in: Y. Poullet and G. P. V. Vandenberghe (eds.), *Telebanking, Teleshopping and the Law* (Deventer, Kluwer Law and Taxation Publishers, 1988) at 33.

27 Trans. note: "Juridical act" will be used as the translation of "acte juridique". This usage follows the English version of the Québec *Civil Code* even though it seems unlikely that jurists outside Québec will find this term familiar. "Acte Juridique" appears to include legal instruments in the broad sense as well as any action having legal import.

28 Claude Fabien, "*La communicatique et le droit civil de la preuve*", in *Le droit de la communicatique - Actes du colloque conjoint des Facultés de droit de l'Université de Poitiers et de l'Université de Montréal* (Montréal, Éditions Thémis, 1992) at 161.

As Professor Trudel explains, this legislation gives "full recognition as evidence to documents reproducing the data contained in a juridical act entered on a computer system."[29] In conformity with the wording of Article 2837, it must be ensured that the document is intelligible and presents sufficient guarantee that it is reliable. Furthermore, this provision has the effect of excluding the best evidence rule stated in Article 2860. Professor Fabien writes:

Certainly, the best evidence of the act is the "invoice" signed by the client. However, the new *Code* does not seem to impose a hierarchy of means of proof which would render inadmissible a computerized record of the same operation, subject to the quality of its proof of authenticity. Regarding admissibility, Article 2837 appears to be an autonomous provision which can bring into competition, before the courts, a record of operations and the original invoices which were entered in the system.[30]

Transactions concluded through telematic operations, such as teleshopping, thus appear to be covered by this provision. The "document" in Article 2837 must be intelligible, in other words, human beings must be able to understand it. This does not necessarily mean that the document must be on paper. A diskette, for example, can be a document which, when inserted in a computer, presents an intelligible text and not binary computer language.

As well as being intelligible, the document must give guarantees of reliability. This can be achieved in two ways. The first can be found in the second paragraph of Article 2837. This paragraph states that the tribunal, in order to assess the quality of a document, must take into account the circumstances under which the data was entered and the document reproduced. Professor Trudel asserts:

In virtue of this article, the testimony of the person who entered the data is not required. It is a sort of exception to the rule against hearsay. The reliability of the data entry and its reproduction could, for example, be attested by the person responsible for the computer department of the company in question or by an expert. This person will have to demonstrate that the data was entered correctly and that its reproduction on a document was done in the same manner.[31]

The second method for establishing the reliability of a document is stated in Article 2838 in the form of a presumption of reliability when the data entry "is carried out systematically and without gaps and the computerized data are protected against alterations". Thus, it is incumbent

---

29 Pierre Trudel, "*La preuve et la signature dans les transactions dématérialisées selon le nouveau Code civil du Québec*", unpublished paper presented at the Journées de formation de l'Institut des vérificateurs internes, Montréal, February, 1994 at 4. [Trans. note: my translation.]

30 Fabien, *supra*, note 26 at 186. [Trans. note: my translation.]

31 Trudel, *supra*, note 27 at 7-8. [Trans. note: my translation.]

on a system operator intending to use a computerized document against a third party to demonstrate that the data entry is performed systematically and that the data is protected against any alterations. In contrast, if the third party uses a computerized document from the operator and the operator argues that this document is not authentic, it is again the latter who carries the burden of proof since this document has the advantage of a presumption of authenticity.[32]

The legislation regarding the admissibility of dematerialized judicial acts has the advantage of giving the courts discretion respecting computer evidence. Contrary to the agreements financial institutions impose on their clients regarding automatic teller cards,[33] legislation does not elevate computerized company documents to the status of indisputable gospel truth. This re-balancing protects the user of telematic services from being charged with burden of proof which would be, in many cases, impossibly heavy.[34] It remains to be seen whether the rules of evidence are public or not.[35] The possibility of contradicting these rules by agreement could certainly contain the potential for an attack on the equality of the parties. As unrealistic as the legal principle of equality might be, it remains that telematics companies could thus set up an iniquitous system of proof in which the burden would rest only on the user's shoulders. Meijboom and Oskamp show that most European countries give the judge the power to overrule rules of evidence in agreements imposing excessively heavy burdens which are often impossible for users to carry in a computer context.[36]

Articles 2837 to 2839 apply only to juridical acts. We cannot therefore have recourse to them to prove legal facts entered on computer media. However, as Professor Trudel rightly points out, the rules of the new *Civil Code* "are flexible enough to permit evidence to be submitted in the form of documents reproducing data entered on a computerized medium."[37]

The rule prohibiting hearsay, maintained under the new code,[38] is in principle opposed to a material fact entered on computer media, for example

---

32 Fabien, *supra*, note 26 at 187.

33 See, for example, N. L'Heureux and L Langevin, *Les cartes de paiement. Aspects juridiques* (Québec, P. U. L., 1991).

34 On the burden of proof in the comparative law of dematerialized transactions, see especially Meijboom and Oskamp, *supra*, note 25 at 46.

35 Fabien, *supra*, note 26 at 182-183.

36 The authors cite the cases of Denmark, Italy, Germany and Holland. Regarding the last country, they write: "In the Netherlands, for instance, this is put explicitly in draft article 180 of the Code of Civil Procedure, which states that 'Agreements which set aside law on evidence are not admissible when they concern the proof of facts, which have legal consequences, and are not free to parties. The same is applicable if it would be unfair to call in the agreement'. If this is the case, so the Explanatory Memorandum on the Bill of Civil Proceedings states, the judge may decide to alter the burden of proof", Meijboom and Oskamp, *supra*, note 25 at 50.

37 Trudel, *supra*, note 27 at 9. [Trans. note: my translation.]

38 See Articles 2832 and 2843.

a writing which is a bill, being presented as evidence by any person other than the author of that writing (in other words the person who entered the data.) Yet Article 2870 of the *Civil Code* greatly tempers the effects of this prohibition. Let us examine it:

A statement made by a person who does not appear as a witness, concerning facts to which he could legally testify, is admissible as testimony on application and after notice is given to the adverse party, provided the court authorizes it.

The court shall, however, ascertain that it is impossible for the declarant to appear as a witness, or that it is unreasonable of him to do so, and that the reliability of the statement is sufficiently guaranteed by the circumstances in which it is made.

The reliability of documents drawn up in the ordinary course of business of an enterprise, of documents entered in a register kept as required by law and of spontaneous and contemporaneous statements concerning the occurrence of facts is, in particular, presumed to be sufficiently guaranteed.

The common law exceptions regarding business records and statements made in the normal course of business are recognizable in this provision.[39] This attenuation of the rule of hearsay should facilitate the use as evidence of computerized data noting, in law, a material fact, especially respecting the difficulty in identifying the author of the data entered.[40] Obviously, to be admissible, the reliability of this evidence must be "sufficiently guaranteed". Regarding this provision, Professor Fabien asserts:

This broad exception to the proscription of hearsay should permit the liberalization of the evidentiary use of computer documents for proving facts, especially when such documents are those produced in the course of the activities of an enterprise: records of the times of departure and arrival of trains to prove their punctuality, records of pharmaceutical prescriptions entered in the computerized file of an individual to prove abuse, computerized records of gas or electricity deliveries to prove a certain level of consumption. Indeed, any record which reports facts entered in a computer by a human actor can be admitted as evidence if the reliability of the document is demonstrated and the other conditions for the application of Article 2870 C.C.Q. are fulfilled.[41]

Another rule of evidence stands in the way, in principle, of the admissibility of a computerized document when proving a material fact. This is the best evidence rule. It means that a party must present the original of a document, for example, rather than a copy it may have received by fax. The problem in telematics, as Professor Trudel emphasizes, "comes from the fact that it is possible to maintain that the original in question is represented

---

39 Fabien, *supra*, note 26 at 177.

40 Trudel, *supra*, note 27 at 10.

41 Fabien, *supra*, note 26 at 177. [Trans. note: my translation.]

by the data contained in the computer in magnetic or electronic form, in other words in a language incomprehensible to common mortals".[42] The version printed on paper of data entered in the memory of a computer would then be only a copy. Here again the new *Civil Code* softens the rigor of the principle of best evidence. Article 2860 states:

A juridical act set forth in a writing or the content of the writing shall be proved by the production of the original or a copy which legally replaces it.

However, where a party acting in good faith and with dispatch is unable to produce the original of a writing or a copy which legally replaces it, proof may be made by any other means.

In consequence, it will generally be possible to submit computerized documents as evidence regarding material facts since the original is not available or has never existed.[43] A party intending to use this provision must demonstrate his or her good faith and diligence. He or she cannot however invoke "simple reasons of convenience to be excused from producing these originals".[44] Nonetheless, according to Professor Fabien, it does not seem that Article 2860 allows the submission as evidence of computerized documents which transcribe data on paper (invoices, account or credit card statements, etc.). Thus a company issuing a credit card could not invoke this article "to avoid producing the instrumental writings signed by the client when he or she uses the card".[45]

Article 2827 of the *Civil Code* defines a signature as follows:

> "A signature is the affixing by a person, on a writing, of his name or the distinctive mark which he regularly uses to signify his intention."

As Professor Trudel emphasizes, the wording of this provision in no way prohibits the use of so-called electronic signatures.[46] A signature plays two roles: it identifies the signatory and expresses his or her intention to adhere to the contents of the instrument.[47] Professor Trudel considers, rightly we think, that in the end an electronic signature plays these two roles. It is of course important to ensure that an electronic signature meets certain criteria of security. The question then becomes technical rather than strictly legal.

---

42 Trudel, *supra*, note 27 at 11. [Trans. note: my translation.]
43 *Ibid.* at 11.
44 Fabien, *supra*, note 26 at 179. [Trans. note: my translation.]
45 *Ibid.* at 179. [Trans. note: my translation.]
46 Trudel, *supra*, note 27 at 12.
47 *Ibid.* at 14.

3. Liability

The issue of contractual or civil liability also arises in telematics. In this respect, it is undoubtedly important to determine whether access to the service is based on a contract. In other words, did the server and the user first agree on the nature, limits, exceptions, restrictions, etc. of the service offered? The existence of a contract governing these issues can help to determine the nature and extent of a wrong, if one occurs. What happens when a user has *free* access to a service without any prior agreement sanctioning such access? The authors of *Lamy informatique* consider that there is a tacit contract since "the telematic merchant is in a permanent state of offer, whether this is manifested indirectly through its advertising or directly in the title page which appears and proposes a menu when a 'connectee' calls. The connected user responds to this offer by 'playing the game' proposed."[48] In any case, the authors believe that in the end this difference is not very important since there is a great deal of similarity between the contractual terms and the standards (by the rule) a judge would be led to consider when there is no contractual relation.[49] While signing a contract for each telematic service used might seem difficult, it is possible to establish a model contract which could be appropriate for the entire range of telematic relations. A user could be required to sign this contract when his or her system is connected. This would increase the legal security of servers and users. However, it is also true that, in any case, the general rules of common law apply, which can thus compensate for the absence of a contractual relation.

Liability in teleshopping can result from three situations: the non-performance by the server of an order made by the user, an order fraudulently made in the name of the user by an unauthorized third party, an infringement on the right to privacy of the user.[50] The last case will be studied separately.[51] Regarding the other two situations, in the absence of any special contractual provisions, the law on obligations prevails. Thus each case must be examined in light of the facts and applicable provisions. In Quebec and Canada there are no special rules on telematic relations. In consequence, in the absence of any specific rule, common law is complementary.

Liability can also be incurred concerning information services. Thus, a user who bases his or her behaviour on erroneous information obtained

---

48 Michel Vivant (ed.), *Lamy droit de l'informatique* (Paris, Lamy S. A., 1993) at 1091, No 1642. [Trans. note: my translation.]

49 *Idem*.

50 M. Schauss, "Issues of Civil Liability", in: Y. Poullet and G. P. V. Vandenberghe (eds.), *Telebanking, Teleshopping and the Law* (Deventer, Kluwer Law and Taxation Publishers, 1988) at 98.

51 See *Infra*, point E.

through telematics (computer transactions) could have grounds to sue. An example which springs to mind is that of a work on edible fruits and plants which led a consumer to mistake hemlock for wild carrots.[52] The French court ruled "that the publisher should have ensured that users could depend on the work and judged its behaviour to be wrongful."[53] Likewise, supplying erroneous information regarding stock markets can make telematics actors liable. Beyond the falseness or inaccuracy of the information supplied, liability may occur when defamatory messages or information circulate in the network. The same argument can be made when information contrary to the provisions of the *Criminal Code* circulate in the network. Think of hate propaganda, obscenity or false news.

When this occurs, the major problem is to identify the telematics actor liable for the wrongdoing. We saw in Part B that many actors play roles in the telematics network and that their operations can sometimes be combined. The confusion or integration of roles (server *and* supplier being the same entity, for example) like the clauses disclaiming responsibility which are found almost systematically in all the national carrier domains[54] make the attribution of and redress for the wrongdoing problematic. In effect, this point is central to the problems since common law (civil and criminal) is relatively well-armed and adapted to treating this type of situation. There is not yet, in Quebec or Canada, any legislative rule likely to permit the disentangling of this functional knot created in the telematics universe.[55]

4. Consumer Protection

Teleshopping raises a number of issues regarding consumer protection. These issues become even more pressing when consumers deal with merchants established in other countries. Remote sales are a domain in which fraud is frequent[56] and thus the consumer must be protected. Besides fraud, other problems such as non-delivery of goods ordered, long delivery delays, slow reimbursement of deposits or amounts paid, the inadequate nature of the good delivered, etc., are common.

It must be admitted that the Quebec *Consumer Protection Act*[57] treats these issues very briefly. Thus, Section 20 of the Act defines the expression "remote-parties contract":

> "A remote-parties contract is a contract entered into between a merchant and a consumer who are in the presence of one

52 Lamy, *supra*, note 46 at 1095, No. 1653.
53 *Idem.* [Trans. note: my translation.]
54 Schauss, *supra*, note 48 at 106.
55 Trudel and Abran, *supra*, note 10.
56 Nicole L'heureux, *Droit de la consommation*, 4th Edition (Cowansville, Yvon Blais, 1993) at 339.
57 R.S.Q., c. P-40.1.

> another neither at the time of the offer, which is addressed to one or more consumers, nor at the time of acceptance, provided that the offer has not been solicited by a particular consumer."

Doctrine recognizes that this provision covers teleshopping. However, it is not clear what is the exact meaning of the last part of the section: "provided that the offer has not been solicited by a particular consumer". In effect, does not a consumer consulting the pages on the screen of a terminal solicit the offer? Perhaps we should consider that when a server advertises products it is always systematically making an offer. It is likely that the latter hypothesis will be the one retained by the courts since it ensures a level of consumer protection which is in conformity with perhaps not the letter but the spirit of the law. Yet in certain cases the consumer may be in a situation in which he or she solicits the offer through communicating, using telematics, with a merchant whose products are not advertised but whose name appears in the electronic directory listing "televendors". This would no doubt require that the provision be clarified regarding technological developments.

Whatever the case may be, if a contract falls under the definition in Section 20, Section 21 then provides that such a contract be considered as concluded at the consumer's address. In consequence, on the view of international private law, the applicable act is the *Consumer Protection Act* and the competent court is that of the consumer's residence. Section 22 deals with inconveniences related to the payment of partial or complete deposits. This provision forbids retailers to request complete or partial payment from the consumer before executing their principal obligation, in other words, before delivering the good. However, the President of the *Office de la protection du consommateur* can exempt a retailer from the requirements of Section 22 on the condition that the latter forwards to the Office a guarantee ensuring "payment of the capital, interest and charges awarded in any final judgment"[58] against it.

It must be admitted that in international private law, Section 21 appears deficient. In effect, the statement of material rules of international private law appears slightly derisory given technological developments. What is the worth of such a mechanism when the server-vendor is established in another country with no business address in Quebec or Canada? Telematics allows transborder purchasing. A consumer with a contract with a Texan server-vendor, for example, will be quite defenceless in case of difficulty.

The Commission of the European Communities has noted the increasingly strong growth of long-distance sales. The *Council Directive of 20 December 1985 to protect the consumer in respect of contracts*

---

58 L'Heureux, *supra*, note 54 at 341. [Trans. note: my translation.]

negotiated away from business premises[59] does not apply to teleshopping.[60] In 1992, the Commission proposed a draft Council directive concerning consumer protection in remote-parties contracts.[61] This draft directive has three goals: to ensure the legal security of the consumer, to ensure the consumer's right to choose (the quality of the information transmitted and the right not to be disturbed by certain kinds of solicitation) and, finally, to ensure reimbursement in case of non-fulfilment of the contract.[62] Furthermore, Article 11 of the draft directive provides that the consumer shall have a period of at least 7 days from the date of reception of the product or service to annul the contract with no penalty. This right of retraction is clearly to the consumer's advantage since it allows the evaluation of the quality of the merchandise and its conformity to advertised claims. The legislation of many European countries, including France, Denmark and Belgium, already contains this right of retraction. Regarding the rules of international private law, the draft directive is limited to stating that members shall provide adequate and efficient means to ensure the provisions of the directive are respected. The very nature of a directive renders it difficult to be more precise.[63] In this respect, Article 5 of the June 19, 1980 *Convention on the law applicable to contractual obligations*[64] states that the law applicable in the case of a contract concluded with a consumer is that of the usual place of residence of the consumer. This provision is echoed in Section 21 of the Quebec act.

Given the growing development of transborder teleshopping operations, it undoubtedly appears necessary to provide for mechanisms to resolve conflicts which can arise between a consumer residing in country A and a

---

59 O.J. (1985) L372/31.

60 "It does not appear that this Directive applies to home-shopping. In particular, Article I provides that the Directive only applies to contracts concluded during an excursion organized by the merchant away from his business premises (which is certainly not the case with teleshopping) or during a visit by a merchant to the consumer's home or place of work where the visit does not take place at the express request of the consumer. Even if one were to equate the process of ordering over a telematics network to a visit by a merchant, it may not be asserted, at least in the case of teleshopping, that this order is placed without the express request of the consumer as the very nature of the medium requires the consumer to voluntarily call up pages on his screen to place an order for goods or services," M. Schauss, "Issues of Contract Law", in Y. Poullet and G. P. V. Vandenberghe (eds.), *Telebanking, Teleshopping and the Law* (Deventer, Kluwer Law and Taxation Publishers, 1988) at 81-82.

61 COM (92) 11 Final-SYN 411 (May 20, 1992).

62 *Ibid.*, *Explanatory Memorandum* at 11-12.

63 Louis Cartou, *Communautés européennes*, 8th Edition (Paris, Dalloz, 1986) in which the authors write on the nature of directives at page 180: "A directive binds all member states to which it is addressed regarding the result, but it leaves national authorities to choose the form and means to achieve it. (Art. 159) A directive can be a general or specific law: but it addresses the member states and is applied through the intermediary of these member states". [Trans. note: my translation.]

64 J.O.J. (1980) L266/1.

server residing in country B. A material rule declaring the law of the consumer's residence to be the law of the contract is not sufficient. There must also be a provision for a mechanism to deal with the inconveniences associated with the fact that telematic operations are no longer located in a set place regarding the territorial jurisdiction of the courts.

5. Protection of Privacy

The establishment of a vast electronic communications network offering users a large number of services is not without danger to the protection of privacy. This theme is not new. Beginning in the 1970s, many European countries developed legislation protecting the individual from the misuse of computer technology. Transactions pose a few specific problems: the possibility of compiling a profile of consumption habits, knowing the financial status of the user (telebanking) and monitoring the consumer's movements (withdrawal cards, sales outlets).[65] Other infringements will undoubtedly occur as the technical potential of electronic communications pathways develops. There are two main issues. On one hand, are the present personal data protection mechanisms adequate given the new technologies? On the other hand, how is the protection of personal data ensured internationally?

In Canada, Quebec stands out. Following the federal government and certain other provinces, in 1982 Quebec passed an act protecting personal information in the public sector.[66] In 1993, one of the events differentiating Quebec occurred: it adopted the *Act Respecting the Protection of Personal Information in the Private Sector*, which came into force on January 1, 1994.[67] The domain of private and public relations is thus, in principle, covered by the two sets of legislation. Obviously, this protection appears partial from the point of view of the whole country since neither the federal government nor the other provinces offer private personal data the same sort of protection as Quebec. Given the interprovincial flow of data, in particular when we consider the new communications routes in which Canada is a *single* market, this absence of protection in the other areas can only decrease the range and efficiency of the Quebec legislation. We will come back to this point when we discuss international protection of nominative information. For now, we shall turn to the question of new technologies and the adequacy of the Quebec legislation.

---

65 Yves Poullet, "Privacy", in Y. Poullet and G. P. V. Vandenberghe (eds.), *Telebanking, Teleshopping and the Law* (Deventer, Kluwer Law and Taxation Publishers, 1988) at 159.

66 *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, R.S.Q., c. A-2.1.

67 S.Q., 1993, ch. 17. This act complements the provisions of Articles 35 to 40 of the Québec *Civil Code*. See Section 1 of the act.

Here we will not study the Quebec act section by section. It is sufficient to say that it affirms the fundamental principles of personal information management which are found in European legislation and international regulations.[68] Do these basic and general principles[69] provide an adequate response to technological change? We must recognize, with Professor Poullet, that these regulations "have fought the risk related to the processing of information received *a priori* by the processing centres"[70] while the dangers posed by the new communications routes "concern data generated *a posteriori* by the use of the service itself".[71] In effect, the services offered on electronic highways are generally interactive. The user must *act* in accordance with the options posted. This *action* is what generates new information about the user and which allows, for example, the compilation of a profile of his or her habits of consumption. Likewise, the definition of "file" found in much European legislation and in the European Convention can pose problems.[72] The development of the integration of computers and telecommunications leads to, among other things, decentralization of operations, making automated processing commonplace, and leading to a diversification of the types of data collected.[73] A Council of Europe committee of experts, working on the new information technologies, is now examining the value of the definition of "automated file" found in the Convention:

---

68 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted by the OECD (1980); the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, adopted by the Council of Europe (1981); the *Guidelines for the Regulation of Computerized Personal data Files*, adopted by the United Nations Human Rights Commission (1988) and the draft directive of the 1982 Commission of the European Communities: *Proposal for a Council Directive on the Protection of Individuals in Relation to the Processing of Personal Data and on the Free Movement of Such Data*, COM (92) 422 final-SYN 287. See also the *Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks*, COM (90) 314 final-SYN 288. On these two proposals, see Karim Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes", [1992] 2 *Media & Communications L.R.* 149.

69 On the generality, terms and structure of these principles, see Karim Benyekhlef, *La protection de la vie privée dans les échanges internationaux d'nformations* (Montréal, Éditions Thémis, 1993) at 97-146.

70 Yves Poullet, "Le marché de l'information. Aspects contractuels: les clauses de confidentialité", unpublished text, Namur, p. 42. [Trans. note: my translation.]

71 *Ibid.* [Trans. note: my translation.]

72 It should be noted that in the Québec act there is no definition of the expression "automated file". The Québec act has the advantage of targeting personal data in whatever medium. The act is thus not constructed on a computer model of protection of nominative information.

73 H. Burkert and M. Rankin, "The Future of the OECD Privacy Protection Guidelines: Building Trust in Electronic Data Networks" (Paris, OECD, June 1989) ICCP (89) 14 at 5.

It may be, however, that the notion of file as used in the Convention suggests centralised storage and processing and is not in keeping with the new reality of distributed processing and networks which allow data to be dispersed and yet linked up at will through the possibility of computer to computer, or terminal to computer, dialogue.[74]

The idea that personal data are stored and organized in a file, located in a precise place, has been exploded. The notion of file is not appropriate. Today data is scattered (in various locations) and thus it is no longer found in a single organized set (a file). Yet the traditional notion of a file fulfilled the requirements of transparency and easy access of data by the person who was the subject of the file.[75] The Committee of Experts of the Council of Europe proposes the concept of "logical file". That data is not located in a single place and is scattered presents no obstacles to the creation of a virtual file. In other words, it is possible, especially through coupling, to reunite dispersed data to make a single ordered set. This then becomes a potential file.[76] Who would perform these operations? This is where the notion of "file controller" comes into play. The provisions on file controllers found in the OECD guidelines[77] and the European Convention[78] are essentially similar. It is a physical or moral person empowered to decide on the goals, recording and use of data. File decentralization makes the identification of a file controller complex.

The notion of file controller[79] is primordial in the general mechanism for protecting personal data because it is the pivotal point defining the effective extent of the rights of the person who is the subject of the file (the principle of individual participation). The Committee of Experts considers that the concept of file controller remains globally valid. It believes that the last known user can be considered to be responsible:

Accordingly, a distributed, decentralised processing system may still give rise to a person or body ultimately responsible for particular "files" if regard is to be had to the ultimate authorised user of the data - is it a PTT, or a cable company operator, or a service provider, or an electricity company? Even if the ultimate authorized user so identified - and for this reason it is

---

74 Council of Europe, *New Technologies: A Challenge for Privacy Protection?* (Study prepared by the Committee of Experts on Data Protection, (CJ-PD) (Strasbourg, Council of Europe, 1989) at 35 (hereafter "*New Technologies*").

75 *Ibid.* at 24. See also Jon Bing, "Impact of Developing Information Technology on Data Protection Legislation", OECD, Paris, DSTI/ICCP (86) 5, February 1986 at 14-31.

76 *New Technologies*, *supra*, note 72 at 25.

77 Article 1a).

78 Article 2b).

79 The Québec act does not explicitly define this term. However, it imposes various duties and obligations on those possessing data. Thus it is presumed that there is a physical or moral person who is ultimately responsible for operations concerning personal data.

essential that the roles of the various actors involved in any telematic service should be clearly communicated to the user - operates a distributed data processing system it should still be possible to regard him/her as in control of all processing operations in regard to a particular file and in particular as being the repository of the sum total of personal data located in a network - the so called "logical file".[80]

Moreover, the Committee refers to network managers. These technological changes have a certain effect on the fundamental principles of personal information management.[81] However it is equally appropriate to note that the generality of fundamental principles fortifies them against obsolescence when faced with new technology. Regarding the European Convention, the Committee of Experts asserts:

At the outset the point should be made that the Convention's principles have the value of generality. As with constitutional and international guarantees of human rights, the principles of data protection are set out in a manner which allows adaptation to evolving situations.[82]

Remember that the fundamental principles found in the Quebec act are, in the end, philosophical statements which define the stakes by imposing limits. However it must be recognized that the development of specific rules can prove necessary in order to clarify, in a practical, operational framework, the application of fundamental principles. The development of such rules is related to the sector-based approach used in recent years by the Council of Europe. We know that the goal of the various recommendations adopted in specialized sectors (direct marketing, medical data, social security, for example)[83] is to complete and define the general mechanism of the European Convention. The sector-based approach is not permitted under the Quebec legislation. In other words, the act does not recognize the possibility of developing specific rules proper to a sector through regulations developed by the *Commission d'accès à l'information* or of controlled self-regulation on the Dutch model,[84] for example. The development of norms governing the new technologies falls under this sector-based perspective. The possibility of completing the general provisions of the act with norms appropriate to the new communications pathways can only ensure a right to respect for privacy adapted to technological change. Such sector-based norms can be, furthermore, brought up-to-date regularly. This flexibility is a clear advantage compared with the long, ponderous process of adopting legislation.

---

80 *New Technologies*, *supra*, note 72 at 25-26.

81 For an examination of these effects, see Benyekhlef, *supra*, note 67 at 370-376.

82 *New Technologies*, *supra*, note 72 at 31.

83 On these recommendations, see Benyekhlef, *supra*, note 67 at 322-336.

84 *Ibid.* at 75 and ss.

Let us now briefly examine the issue of international protection of personal data. The new electronic communications pathways ignore national boundaries. The mobility of information makes national means of protection extremely fragile. It is thus very easy to transmit and store data in a foreign country which has no legislation on the protection of personal data or where the legislation is particularly lax. Thus the letter and the spirit of national legislation is avoided through the export of personal data. While there may be those who purely and simply desire to escape national law, it must also be recognized that in order to conduct business, companies must sometimes export data to other countries. Most European legislation contains provisions meant to prevent undue export of personal data. National law thus submits the export of nominative information to certain controls or conditions in order to prevent its provisions from becoming derisory.[85]

The Quebec act contains no such provision. It has no explicit answer to the problems caused by the extremely high international mobility of personal data. Quebec legislation is clearly deficient in this respect since the United States, the main destination of personal data from Canada,[86] gives only fragmentary protection to nominative information in the private sector. The same can be said about the federal government and the other Canadian provinces. Thus, just when new electronic communications routes are being established, when the mobility of information is increasing, the Quebec act ensures only *territorial* protection to personal data concerning its citizens.

Section 17 of the Quebec act is the only provision concerning transborder transmission of personal data:

> "Every person carrying on an enterprise in Quebec who communicates, outside Quebec, information relating to persons residing in Quebec or entrusts a person outside Quebec with the task of holding, using or communicating such information on his behalf, must take all reasonable steps to ensure:
>
> (1) that the information will not be used for purposes not relevant to the object of the file or communicated to third persons without the consent of the persons concerned, except in cases similar to those described in sections 18 and 23;
>
> (2) in the case of nominative lists, that the persons concerned have a valid opportunity to refuse that personal information concerning them be used for purposes of commercial or philanthropic prospection and, if need be, to have such information deleted from the list."

---

85 *Ibid.* at 245-273.

86 R. Laperrière, R. Coté, G. Lebel, P. Roy and K. Benyekhlef, *Crossing the Borders of Privacy. Transborder Flows of Personal Data from Canada* (Ottawa, Department of Justice, 1991) 212 and ss.

Transborder transmission is neither prohibited nor subject to conditions requiring equivalent protection. Section 17 absolutely does not enshrine the principle of equivalence found in European legislation.[87] It simply states that the data communicated must not be used for ends different from the original goals. Likewise, the importer shall not communicate the data except in the cases provided for by the act itself. Legislators have perhaps too much confidence in the good faith of the importer. Moreover, it is assumed that the exporting Quebec company will sign a contract with the non-Quebec company, whether or not it is in the same group, in order to guarantee the prescriptions of the act. This is how, it seems, the words "all reasonable steps" in Section 17 must be interpreted. What happens if the importer disregards the prescriptions of Section 17? Should the Quebec company be punished? Nothing is less likely. If the Quebec company took all *reasonable steps*, in particular by signing a contract, it is difficult to see how it could be held responsible for a failure of the other contracting party. In this respect, the *Commission d'accès à l'information*, responsible for applying the act, seems poorly equipped to prevent such a case from occurring. In effect, it could not prohibit transborder communication or subject it to certain conditions because the act is silent on these points. These are perhaps the only means able to prevent this type of situation.

Furthermore, even if we consider that Section 17 grants a certain form of protection to transmitted data, the wording of the section forces us to note that only data relating to citizens residing in Quebec can benefit from this presumed protection. Data concerning a citizen of Germany, Holland or Canada (not residing in Quebec) is not protected if it is stored in Quebec. This is utterly contrary to the spirit of European legislation and to Article 1 of the European Convention. In this legislation, it is clearly provided that legislative guarantees apply to all physical persons regardless of their nationality or place of residence.

It is obvious that the development of electronic highways intensifies the urgency of the need to create a normative framework protecting personal data. In North America, such a framework appears even more imperative given the virtual non-existence of norms concerning personal data in the private sector. One solution, among others, would be for Canada and the United States, next to adopting legislation in due form, to adhere to the European Convention. In Article 23, this agreement provides for the possibility of countries which are not members of the Council of Europe to adhere to it. Thus following this agreement would have the notable

87 The principle of equivalence can be defined as follows: a country shall not oppose the transmission of personal data to another country provided the latter ensures protection of personal data which is equivalent in substance to that in the exporting country. This principle is also enshrined in international legislation: see Article 17 of the OECD guidelines, Article 12 of the European Convention and Article 26 of the draft directive of the Commission of the European Communities.

advantage of ensuring adequate and efficient protection for personal data circulating in the international communications networks.[88]

6. Conflict Resolution

A normative framework proper to telematics is not defined in Canada. We must thus take recourse, as we have just seen, to common law in order to sketch out the solutions to problems raised by dematerialized transactions. It goes without saying that a great many aspects have not been treated in this study, such as issues linked to freedom of expression and access to the network,[89] the control of certain information exchanges in the name of public interest or national security,[90] etc. Here again a normative framework must be established in order to ensure use of the new communications pathways is, legally speaking, optimal and secure. The term "normative framework" is intended to be neutral. In other words, it does not necessarily presuppose legislative intervention. Other modes of regulation can be imagined. As Trudel and Abran emphasize, "in telematics, parliaments and ministers must determine in what form the norms within their competence will be stated."[91] There are a number of forms: codes of conduct, guidelines, free or controlled self-regulation, regulation by an administrative organization, ministerial directives, strict or flexible legislative action, etc. The development of a normative framework is however but a step, though certainly an essential one, in the general supervision of the new communications pathways. It is equally important to determine the mode of conflict resolution. This issue is often, but not always, largely shaped by the choice of normative framework. For example, the legislative route might be favoured and arbitration be provided for as the mode of conflict resolution rather than recourse to judicial tribunals. Many combinations are possible.[92]

In fact, the approach chosen depends on the policy. It is true that this choice is fraught with practical considerations. Furthermore, the choice of a normative framework undoubtedly depends on the aspect one intends to govern. Now, these aspects are very diverse in the new communications pathways. Dematerialized transactions cannot be regulated in the same way

---

88 On the international cooperation provided for by the European Convention in the application of the fundamental principles regarding personal information management, see Benyekhlef, *supra*, note 67 at 352-357.

89 See, among others, E. J. Naughton, "Is Cyberspace A Public Forum? Computer Bulletin Boards, Free Speech, and State Action", [1982] 81 *The Georgetown L.J.* 409 and Henry H. Perritt Jr., "Tort Liability, the First Amendment, and Equal Access to Electronic Networks", [1982] 5 *Harvard Journal of Law & Technology*, 65.

90 Karim Benyekhlef, "La souveraineté nationale et le contrôle des échanges internationaux d'informations", [1991] 25 *Revue Juridique Thémis*, 434.

91 Trudel and Abran, *supra*, note 10 at 15. [Trans. note: my translation.]

92 Henry H. Perritt, Jr., "Dispute Resolution in Electronic Network Communities", [1993] 38 *Villanova L.R.* 349.

as freedom of expression on electronic bulletin boards, or access to the network for such ends. The first aspect requires, it seems, more active intervention since it has to do with protecting the user from co-contractors which are often much more powerful. There is an unbalance to be corrected.

Regarding the nature of the mode of conflict resolution in dematerialized transactions, one is inclined to believe that the law courts are best qualified to ensure user protection. Yet, it seems that in this context a more flexible formula would be more appropriate. In effect, we must avoid the situation in which the user takes legal action to recover small amounts of money or to annul a contract the object of which is minimal: a small sum, everyday consumer merchandise, etc. In this respect, the telematic actors could agree to refer all suits to a sort of network ombudsman. In principle, the ombudsman would have the power to decide electronic conflicts. Obviously, there would be the possibility of providing for appeal, and recourse to law courts could be limited to cases analogous to those involving issues of judicial control over administrative acts.[93]

The exact nature of the formula is of little importance. What is important is to favour flexibility, simplicity and economy in conflict resolution. The electronic environment, through its speed and incessant change, seems to require this type of intervention. Internationally, moreover, the establishment of a flexible method of conflict resolution in the communications networks would have the advantage of reducing the difficulties associated with the many legal systems and competent jurisdictions. This path must be explored.

7. Conclusion

This overview has allowed us to identify several points of tension between the legal and the technical. These points of tension are in fact the technological advances with which the law has not yet caught up. While common law can get around many difficulties, it remains that a normative framework proper to the new communications pathways must be instituted, in particular for reasons of legal security. As was mentioned in the introduction, this legal security is essential to the efficient development of the communications networks. There remains much to be done. In effect, the aim of our discussion was to underline the many issues which doctrine must submit to careful analysis in the coming years. This task is all the more difficult in that the technology is continually changing. The development of a-technological norms, in other words norms independent of the state of the technology at a given point in time, is undoubtedly the goal for which we must strive. This normative quest must not be strictly legal. Other disciplines

93 *Ibid.* at 362-363.

must be associated. This is an investment which should permit the development of solutions fulfilling the expectations of the third millennium.