**University of Montréal**

**Faculty of Law**

**Public Law Research Center**

# Cyberspace and Electronic Commerce Law:

# General Principles and Legal Issues

**by**

Pierre Trudel[*]

June 1999

[*] Professor, Centre de recherche en droit public, Faculty of Law, University of Montréal, email : <trudelp@droit.umontreal.ca>. Address : Centre de recherche en droit public, Faculté de droit,Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec) CANADA, H3C 3J7; Ph.: (514) 343-6263; Fax : (514) 343-7508; URL : <http://www.crdp.umontreal.ca>

# Table of Contents

## INTRODUCTION

Many cybernauts demand that cyberspace be maintained as the realm of individual free will. Invoking the transnational nature of the network environment and the numerous possibilities of evading laws, they assert it is impossible to regulate this free space! Yet law exists in cyberspace because human interactions take place there. While it may be agreed that the net is and must remain a space for freedom, it is perfectly normal that regulations should emerge to identify and define the respective responsibilities of the participants in electronic communication. We inevitably come into contact with law as soon as some one is responsible for circulating prejudicial information on the network. However, because of cyberspace's virtual nature, law cannot be viewed there it in the same way it is in the physical world.

Present law, which refers to regulations adopted by states, can be applied in cyberspace. The rules stated in legislation apply with neither less nor more difficulty than in other contexts. Thus we cannot keep repeating that open networks such as the Internet are impossible to regulate. We must gain better understanding of the standard practices used in electronic environments because they prefigure the regulations that will be established.

State authorities continue to exercise control in cyberspace. However this control is not exercised through regulations dealing with the aspects most often associated with information highways. The law governing relations between individuals within a national legal framework, usual law, is naturally intended to apply to what is primarily and essentially interaction between subjects. We must be reminded of this because many people automatically view cyberspace law as principally following from telecommunications regulation and its host of micro-regulatory measures.

Cyberspace has four characteristics that gain importance when we consider the problem of regulating it. It is a virtual space, a space of interaction where the user is sovereign and regulations compete.

### A virtual space

Cyberspace is not located at a specific point in territorial space. The possibility of controlling the activities that take place there has little relation to the physical location of the parties. It is a virtual space resulting from the many interconnections made possible by network interoperability. While in the physical world the location of persons and companies within a national territory is a fundamental premise for application of the rules of law of a given state, in cyberspace everything is both present in and absent from a given physical space. The message is present everywhere there is a connected computer, so every state with such a reception point can claim to apply its law. However very few are able to ensure effective application of their laws.

### A space for interactions

The Internet is not a broadcasting space. It is more a place of interaction. We must leave aside approaches based on the premise that these virtual spaces are used for broadcasting and focus on the problem of the rules providing the framework for the activities taking place in spaces of interaction. With respect to such places of interaction, the rules target less regulating information broadcasting than they do establishing guidelines as a framework for the relations occurring there.

### The user's sovereignty

Information highways provide users with greater freedom to choose. Thus users also carry more responsibility for the interactions in which they agree to take part. The absence of centralised control puts the burden of self-protection back on users' shoulders: no one can do it in their stead or claim to provide guarantees against false or misleading information. On the Internet, the individual may do business with a company that operates in compliance with strict high standards or take chances and contract with a swindler.

Therefore, in order to survive, sites must offer optimal trustworthiness to consumers and users because it is possible to choose to visit only those sites that post guarantees of reliability and honesty. In sum, the ability to evade regulations goes both ways. In certain cases we may choose to move away from a site because it seems too regulated and the rules prevailing there do not suit us. In other situations, in particular when we are looking for a site with integrity and credibility, we will be inclined to visit sites that subscribe to regulations offering optimal guarantees of rigour and integrity.

### Competition between regulations

Electronic communication presupposes a voluntary action by the user and entail the possibility of connecting elsewhere. Moreover, the potential to establish other networks always remains available to those who are not satisfied with the regulations governing a specific network or electronic environment. This phenomenon has a major consequence: Internet regulation is an activity subject to competition. No authority can claim to have a monopoly over the statement of rules or their application.

Competition can concern the quality of the guarantees of honesty offered by each site soliciting users and the social pressure that users can generate. It is often possible to set up elsewhere in order to avoid undesirable rules. This phenomenon requires that we approach the problem of regulation in this environment by leaving aside the formal state paradigms that often provide the foundation for legal analyses. In cyberspace, law is one of the components of the trust required by all serious commercial activity.

## 1.- How to establish trust in a space beyond state borders? – regulatory approaches

Merchants and consumers need trust before they can engage in transactions on the Internet. When state law alone is unable to provide the desired level of trust, those involved must themselves provide strategies to establish the climate of trust necessary for transactions to take place.

Thus enterprises wishing to maintain or increase the capital in credibility they need to undertake commercial activities on the Internet will increasingly tend to adopt a proactive approach. It is neither necessary nor useful to wait for state law to establish rules before undertaking such activities. There is regulatory activity in cyberspace: it is often emergent and misunderstood, and employs novel techniques and media. The regulation presently operating on the Internet is largely a consequence of the rules dividing responsibility between participants in electronic communication. Such regulation essentially targets preventive assignment of responsibilities to the various participants in electronic communication. Whether what is at issue is “Frequently Asked Questions”, contracts offered on line or codes of conduct developed by different associations and enterprises, the concern is the same: there are conflicts between those who use cyberspace, and these conflicts must be prevented and, perhaps, managed. In the case of commercial activities, it is also important to guarantee a climate of confidence and trust.

There are several complementary paths available to maintain or build the trust needed for a company to be taken seriously in Internet commerce. Contracts and contractual policies are certainly the first elements of most such strategies. However, self-regulation and certification mechanisms may also be chosen.

### Contracts

Consent, and the user’s right to withdraw it, seem to constitute a regulating principle on the Internet. The importance of competition between sites with respect to regulation explains the central role that contracts are called upon to play in electronic environments. Since electronic environments are above all places of interactions, they presuppose that those involved choose to be in the presence of one another. Aside from unsolicited email, it is rather rare that interactions occur without each party expressing agreement. This shows the importance of contracting with respect to regulation of electronic environments, and it probably explains why so many authors speak about a contract paradigm[1].

Between persons subject to the same national framework, a contract is subject to the rules of contract law. Between persons in different national frameworks, the contract must determine the law applicable to the contract. However, in the case of contracts governed by public laws, the parties cannot avoid the application of provisions that are mandatory for all contracts considered to have been concluded on the territory in question. In certain situations a practice could develop whereby model contracts would generally be followed in a field of

[1] David R. JOHNSON and Kevin A. MARKS, “Mapping Electronic Data Communications Onto Existing Legal Metaphors : Should We Let Our Conscience (And Our Contracts) Be Our Guide? (The Congress, the Courts and Computer Based Communications Networks : Answering Questions About Access and Content Control)” 38 *Villanova Law Review* 487-515; Robert L.DUNNE, “Deterring Unauthorized Access to Computers : Controlling Behavior in Cyberspace Through a Contract Law Paradigm”, (Fall 1994) 35 *Jurimetrics Journal* 1-15; Trotter HARDY, “The Proper Legal Regime for Cyberspace”, (1994) 55 *University of Pittsburgh Law Review* 993; Steven A. BIBAS, “A Contractual Approach to Data Privacy”, 17 *Harvard Journal of Law & Public Policy* 591-611.

activity. This practice could sometimes be equivalent to de facto standards and end up imposing itself.

Contractual practices can lead to the development of true rules that are applied across the board and are voluntarily adopted by the parties. This is known as self-regulation.

### Self-regulation

Self-regulation refers to standards voluntarily developed and accepted by those engaging in an activity[2]. The primary nature of self-regulatory rules is that they are voluntary, in other words they are not obligatory as are laws enacted by the state. Those complying with self-regulation have generally agreed to do so. Its nature is fundamentally contractual. Most often persons agree to comply with self-regulatory standards because doing so has more advantages than disadvantages. For example, standardisation is above all considered to be a process of "formulating rules in the interest and with the co-operation of all the parties involved to optimise the global economy while taking into account manufacturing conditions and safety requirements". With respect to computer technology, approaches in standardisation are generally based on the results of scientific research, technical knowledge and experience acquired in the industrial or professional circles where they develop.

In a number or areas of activity, and to varying degrees, private associations have developed deontological principles and voluntary technical standards. In the field of services such as sales[3], advertising[4], banking[5], securities[6], accounting[7] and the media[8], this is how most voluntary regulation has appeared. This deontology is intended to underline the precepts of recognition of honest practices, practices considered good, in various professional and

[2] Pierre TRUDEL, "Les effets juridiques de l'autoréglementation", [1989] 19 *Revue de droit de l'Université de Sherbrooke*, 251.

[3] Kenneth COHEN and Ian ROHER, *Self-regulation by Industry : An In-Depth Study of the Better Business Bureau*, Toronto, Osgoode Hall Law School, April 23, 1974, 79 p.

[4] James P. NEELANKAVIL and Albert B. STRIDSBERG, *Advertising Self-Regulation : A Global Perspective*, New York, Hastings House, 1980; Dominique FORGET, *Le fonctionnement des organismes d'autoréglementation de la publicité au Canada*, Mémoire de maîtrise en sciences de la communication, Montréal, Université de Montréal, 1989; Maurice WATIER, *La publicité*, Montréal, Éditions Paulines & Médiapaul, 1983, pp. 95 and ss.; Bernard MOTULSKY, *La publicité et ses normes*, Québec, P.U.L., 1980, 165 p.; Daniel Jay BAUM, "Self Regulation and Antitrust : Suppression of Deceptive Advertising by the Publishing Media", [1961] 12 *Syracuse L.R.*, 289.

[5] David G. OEDEL, " Private Interbank Discipline", 16 *Harvard Journal of Law & Public Policy* 327-409; Jean PARDON, "Quelques normes propres au secteur bancaire" in COMMISSION DROIT ET VIE DES AFFAIRES, *Le droit des normes professionnelles et techniques*, seminar organised in Spa-Balmoral, 16 and 17 November 1983, Bruxelles, Bruylant, 1985, pp. 1 à 46.

[6] See : David L. RATNER, "Self-Regulatory Organizations", [1981] 19 *Osgoode Hall L. J.* 368; Alan C. PAGE, "Self-Regulation : The Constitutional Dimension", [1986] 49 *Mod. L. Rev*. 141.

[7] INSTITUT CANADIEN DES COMPTABLES AGRÉÉS, *Manuel de l'ICCA*, Toronto, l'Institut, 1968, pag mult.

[8] Francis COLEMAN, "All in the Best Possible Taste : The Broadcasting Standards Council 1989-1992", (1994)*Public Law* 488-515; Daniel L. BRENNER, "The Limits of Broadcast Self-Regulation Under the First Amendment", [1975] 27 Stanford L.R. 1527; Harvey C. JASSEM, "An examination of Self-Regulation of Broadcasting", [1983] 5 *Communications and the Law* 31; Michael BLAKENEY, "Leaving the Field - Government Regulatory Agencies and Media Self-Regulation", [1986] 9 UNSW L. J. 53-65; AUSTRALIAN BROADCASTING TRIBUNAL, *Self-Regulation for Broadcasters, A report on the Public Inquiry into the Concept of Self-Regulation for Australian Broadcasters,* July, 1977, 172 p.

commercial areas of activity[9]. A number of self-regulatory precepts take the form of recommendations. They originate from specialised organisations and most often apply because of the expertise such organisations have[10].

Use of the Internet reveals the main models of self-regulation prevailing there. Thus those controlling a site on the network have the choice of adopting policies with respect to access to the site, acceptable behaviour and prohibited acts. Most universities have policies and rules defining the rights and prerogatives of those using their computer facilities.

These policies, which are sometimes laid out in official documents and adhesion contracts signed by members and clients, state the rules of conduct regarding issues such as the private nature of electronic mail, conditions on use of software available on the network, the obligation to use one's real name, the right to engage in commercial advertising, the right to use network resources for personal purposes and responsibility for behaviour of subscribers and clients.

In order to be credible, self-regulation requires the establishment of meaningful rules, in other words rules that entail that the parties have real obligations. Self-regulation cannot be limited to a simple endorsement of existing laws. It is not credible if it does not try to go beyond the strictly interpreted requirements of legislation. Thus it is insufficient to proclaim one's commitment to complying with existing laws: generally what is needed is a more precise statement of the rights and obligations that will be assigned to parties to a transaction.

The limits intrinsic to self-regulation are well known. Self-regulation supposes a certain degree of consensus and cannot include obligations conflicting too directly with the interests of the parties. The sanctions that can be imposed under self-regulation are essentially limited. Since those it governs have subscribed to it, self-regulation's ultimate sanction remains exclusion or boycott. Self-regulation does not escape the principle of competition between regulations. Yet it is different: in cyberspace, self-regulation is almost as avoidable as state law! Here state law is not as clearly superior as it is in other environments.

While the sanctions entailed by failure to comply with self-regulation are often merely psychological, in certain cases they nonetheless remain the censure most difficult to endure. The Internet can allow considerable circulation of unfavourable information. Dissatisfied users can exact a high price for improper behaviour.

### Certification

Essentially, certification is *"a procedure by which a third party provides written assurance that a product, service, quality system or organisation complies with specified*

[9] D.J. LECRAW, *Voluntary Standards as a Regulatory Device*, Ottawa, Conseil économique du Canada, Mandat sur la réglementation, Cahiers de recherche n° 23, 1981, pp. 30 et ss.

[10] See: "Private Codes for Corporate Conduct : Should the Fox Guard the Henhouse?", [1993] 24 *Interamerican Law Review*, 399-433; S. F. STAGER, "Computer ethics violations : more questions than answers", *EDUCOM Review,* July-August 1992, 27-30.

*requirements”*[11]. There is no uniform model of the way various certification organisations operate[12].

While the technical side of certification may be obvious to the observer, this is not the case with respect to the normative aspect of this process. The primary goal of certification lies in the standardisation of technical features related to quality. However it is not a one-dimensional process. It covers three aspects of commercial relations with the following objectives: better sales, better purchasing and better regulation[13].

Certification appears to be a mechanism for making technical aspects uniform. Consider the work of the International Standardisation Organisation (ISO). However in certain cases this mechanism also allows rules of conduct to be developed that are, at first site, rather restrictive.

There are three types of certification: product certification, company certification and company/service certification. The goal of product certification is to attest to the fact that the product complies with certain set technical specifications. Company certification instead targets the ability of an enterprise to manufacture products in compliance with certain technical standards, but provides no definite guarantee based on results of samples. Finally, company/service certification is a hybrid process situated between product and company certification. The goal of this type of certification *“is to certify the internal organisation of the enterprise and its attention to client relations”*[14]. The type of certification chosen largely depends on the goal of the enterprise and the market in question.

In order to obtain the certifying organisation’s seal, a company must meet a set of pre-established criteria. With respect to services and product distribution, these criteria are in fact codes of conduct. An enterprise that fails to comply with such prescriptions would see its accreditation withdrawn. Through certification it thus becomes possible to impose rules. Certain organisations are trying to establish certification procedures in cyberspace.

### State law

State law is generally considered to be the only form of regulation able to use the force of state structures to ensure its effective application. However, in electronic environments state law displays its limitations. In principle it applies only on a determined territory and changes at a rate that is not always synchronised with that of changes occurring in electronic environments.

[11] Alain COURET, Jacques IGALENS and Hervé PENAN, *La certification*, coll. “Que sais-je?”, Paris, P.U.F., 1995, p. 91.

[12] Jonathan T. HOWE and Leland J. BADGER, “The Antitrust Challenge To Non-Profit Certification Organizations : Conflicts Of Interest And A Practical Rule Of Reason Approach To Certification Programs As Industry-Wide Builders Of Competition And Efficiency”, (1982) 60 *Washington University Law Quarterly* 357, 364.

[13] Alain COURET, Jacques IGALENS and Hervé PENAN, *La certification*, coll. “Que sais-je?”, Paris, P.U.F., 1995, p. 10.

[14] Alain COURET, Jacques IGALENS and Hervé PENAN, *La certification*, coll. “Que sais-je?”, Paris, P.U.F., 1995, p. 89.

In spite the clear limitations on applying it effectively in certain cases, state law can continue to be applied to many legal situations arising on the Internet. First, a significant number of transactions occur between parties in the same national jurisdiction. In contrast, for transactions involving parties subject to different national legal regimes, the issue of the application of the national law of a state is framed in accordance with the principles of private international law.

Transactions can be viewed according to the usual principles and rules of private international law. Thus the applicable law must be determined and an attempt must be made to obtain the sanction of the legislation invoked. The problems of applicability and effectiveness are not really different from those entailed by contracts concluded between persons subject to different jurisdictions. The difficulty is more acute in the case of consumer contracts. Most often such contracts are governed, under each national legal regime, by public provisions that the parties cannot evade.

In principle, state law applies to the territory of the state. Extraterritorial application of legislation remains the exception. Moreover, a state could very well enact a law that declares it has extraterritorial force, but practical obstacles could make such a law inapplicable beyond its borders. Thus the extraterritorial application of a law most often presupposes that the justiciable person targeted has goods or a place of business on the national territory. Attribution of extraterritorial scope to a law is of very little use when the subject of the law is located entirely outside the country.

National law must be continually revised because of the speed of change in communication in electronic environments. It is often noted that the law must be designed in such a way as to allow a sufficient degree of flexibility so as to maintain a certain degree of adaptability. This explains the frequent recourse to vague notions and standards referring to concrete appraisal of factual situations.

In this sense it is not unusual to note that laws often express vague or broadly worded assessment criteria and standards. Space must almost always be left for evaluation and the need to take into consideration the speed of technical changes explains the features that must be included in state law. In consequence, it is very unlikely that the law of the various states could formulate rules so precise and similar from one country to another that we could dispense with other regulations. Thus we cannot consider that state law will be able to provide the certainty sometimes needed for a framework for transactions.

The international nature of many interactions occurring on the Internet raises problems that cannot be entirely resolved by a contract concluded between the parties or by the law of a single state. Depending on the jurisdiction in which one finds oneself, different rules can be applied to preside over contract interpretation[15].

[15] Gregor HEINRICH, “Harmonised Global Interchange? - Unicitral's Draft Model Law for Electronic Data Interchange, [1995] 3 *Web Journal of Current Legal Issues*, http://www.ncl.ac.uk/~nlawwww/articles3 /hein3.rtf.

## 2.- Electronic commerce: the essential legal notions

Though it has been in use for some time, the expression “electronic commerce” has no formal, universally accepted definition. This term has been the subject of many comments by various people in the legal, computer and accounting world, but it still remains ambiguous[16].

For some, electronic commerce is simply defined as the performance of commercial activities using present information infrastructures. The American *National Information Infrastructure* (NII) sees electronic commerce as the evolution of electronic data interchange (EDI) to encompass other types of data and transactions[17]. Others opt instead for more elaborate definitions in which electronic commerce brings together communications, data management and security services to result in business applications within various organisations for the automatic exchange of information[18]. Thus the definition of electronic commerce is located between these two poles, going from the simple use of the capacities of communications infrastructures to the integration of communications systems, data management and security.

From a broader perspective, electronic commerce must deal with various problems. In electronic environments commerce is no longer considered without a set of principles ensuring privacy and the confidentiality of personal and commercial information. In the same way, protection of intellectual property is a central assumption in the legal framework of electronic commerce. However electronic commerce law is primarily concerned with the legal and para-legal framework that sets the rules for transactions.

### 2.1. The main forms of electronic commerce

The main information and communications technologies have considerable potential to improve business conditions. Here we will consider the main technologies used to perform commercial transactions.

#### 2.1.1 EDI

Generally, the expression “electronic data interchange” designates all sorts of data exchanges by electronic means. However, a stricter definition has been developed over the years.

[16] See in particular: Electronic Commerce Integration Facility (ECIF), http://waltz.ncsl. nist.gov/ECIF/prospectus.html; EMail World Conference, http://www. oec.com/ EMAILWORLD/ page03.html; John RATSAROS, “Using the Internet for Electronic Data Interchange?”, Internet World , vol. 5, n° 5, July/August 1994; Amelia H. BOSS, “The Emerging Law of International Electronic Commerce”, (1992) *Temple Int'l & Comp. L.J.* 293.

[17] “Electronic Commerce is the evolution of EDI into other types of data and transactions”, National Information Infrastructure : DRAFT FOR PUBLIC COMMENT, http://iitfcat.nist .gov:94/doc/ Electronic Commerce.html. Au même effet, voir le Rapport A/CN.9/373 (1993) du Groupe de travail sur les échanges de données informatisées de la Commission des Nations Unies pour le droit commercial international.

[18] “Electronic Commerce integrates communications, data management, and security services, to allow business applications within different organizations to automatically interchange information”, Information Infrastructure Technology and Applications (IITA) Task Group, National Coordination Office for High Performance Computing and Communications, February 1994, pp. 13-14.

EDI supposes data is transmitted between the computer system of one party and that of a co-contractor with the intent of producing legal effects. This transmission can be point to point (directly between two computers), or, more generally, through the intermediary of a value-added network (VAN) that receives, sorts and transmits messages to their addressees. Conclusion of a contract by electronic means thus implies the exchange of an electronic document between two computers that are able to automatically perform, without human intervention, the appropriate actions based on a pre-defined computer grammar adopted by the parties.

Automation is one of the main features of EDI. Contrary to simple transmission of electronic data where, as in the case of electronic mail, the data is generally translated into readable text, EDI data does not need to be printed on paper since the computer system and its applications are able to handle the complete process of creation, authorisation, transmission and interpretation of messages independently.

Use of a pre-defined grammar is the second main feature of EDI. While there are a number of different EDI standards specifically developed by various industrial and financial sectors, it should be noted that the UN/EDIFACT and ANSI X12 standards are important to the global progress of EDI. The UN/EDIFACT[19] standard plays an increasingly important role internationally while the ANSI-X12 standard remains used chiefly in North America[20].

The difference between an EDI message and a message exchanged by a text-based electronic messaging service lies precisely in the structure and content of the messages themselves:

> *An electronic message is not necessarily destined to be processed by the addressee's computer. It is made up of a few standardised zones, such as the addressee's address and the code that determines the beginning and end of the message. In contrast, the content of an EDI message is by definition intended to be automatically processed by the addressee's computer. In consequence, it must be formatted so the addressee's*

[19] "La norme UN/EDIFACT est conçue pour standardiser le contenu des documents faisant l'objet d'échanges informatisés. Elle comprend un vocabulaire normalisé, une grammaire des directives pour la conception de messages standardisés, des agencements de données en segments et en messages standards.
Le répertoire des éléments de données commerciales comprend 600 concepts types des transactions commerciales. Ces concepts sont accompagnés de règles de formatage et d'affichage à l'écran. La combinaison de ces éléments de vocabulaire permet de faire des messages standards répondant aux différentes possibilités. Les messages sont des éléments de dialogue neutres et stables. Élaborés dans le cadre des relations commerciales internationales, ils ne permettent aucune discussion ou polémique. Les messages forment des agencements de données, des phrases types de formes comparables d'une transmission à l'autre", *Id*., p. 82.

[20] "Le standard ANSI X12 est né à la suite des premières expériences d'échanges de données commerciales par voie électronique qui ont pris place aux États-Unis. En 1979, l'American National Standards Institute charge un comité de mettre au point une norme ayant vocation à un usage universel. C'est ainsi que, de 1979 à 1985, le Comité ANSI X12 développe une norme : le BDI (*Business Data Interchange Standard*)
Fondamentalement, le standard ANSI X12 est destiné à fournir une syntaxe, une structure et un contenu normalisé aux messages échangés entre ordinateurs. Le standard détermine une structure et un contenu aux transactions commerciales ainsi que des éléments destinés au contrôle des données échangée", *Id*., p. 81.

> *software can read and process it. The standardised format of documents is the main characteristic of EDI*[21].

Recent developments in communications tend to make EDI less impenetrable than it was in the past. Thus while EDI is presently planned only for point to point networks or VANs, there are major projects for bringing EDI to major open networks such as the Internet. Indeed, the development of EDI on the Internet, through electronic mail and videotex, is one of the goals of a number of public and private actors in the EDI world[22].

EDI is now supported by an important innovation: electronic forms, which have been called upon to replace various paper commercial documents. In contrast with their paper equivalents, electronic forms are active. They can process the data recorded on them[23]. The exchange of electronic forms generally supposes that the originator and addressee both have the software needed for processing and sending. Moreover, the flexibility of electronic forms allows hybrid exchanges to take place. In such cases, the electronic form is sent in EDI format and received by the addressee as a form. After it has been completed, the form can once again be converted into an EDI message and retransmitted as such[24].

### 2.1.2 Financial EDI and electronic funds transfer

Financial EDI is a specific branch of EDI and refers specifically to the transfer of funds. The expression “financial EDI” applies to the exchange of messages between a payer and a bank or between a bank and a beneficiary. Closely related to financial EDI, electronic funds transfer (EFT) is also the structured movement of data allowing value to be transferred from one financial institution to another[25]. Direct deposit is an example of this.

These two forms of electronic payment, EDI and EFT, have a number of points in common. Both of them contain the basic data required for payment: amount, effective date, account numbers, etc. Contrary to EFT, financial EDI nonetheless also allows the transmission of other information. It is said that financial EDI, unlike EFT, is not funds-driven but rather information-driven[26]. Among the information that could be transmitted with a payment are payment, credit or debit notes as well as any information likely to facilitate the establishment of management statements[27].

[21] *Échange de documents informatisés : réseaux à valeur ajoutée et logiciels de traduction*, Québec, ministère des Communications, Direction générale des technologies de l'information, January 1993, p. 7.

[22] CommerceNet : FAQ, http://www.commerce.net/information/faq.html.

[23] Gerry DIAMOND, *Sélectionner un réseau à valeur ajoutée pour le commerce international*, Direction des industries des services et des transports, Affaires étrangères et Commerce international, Canada, 1995, p. 13.

[24] *Id.*, pp. 14-15.

[25] Ned C. HILL and Daniel M. FERGUSON, “Electronic Data Interchange and Electronic Funds Transfer : The Basics”, (1995) édition spéciale, *EDI Forum* 9.

[26] S. CHAN, M. GOVINDAN, E. LESCHIUTTA, J.Y. PICARD, G.S. TAKACH, B. WRIGHT, T. PIETTE-COUDOL, *EDI pour les gestionnaires et les auditeurs*, 2e ed, Toronto, Institut canadien des comptables agrées, 1994, p. 81.

[27] *Id.*, p. 83.

### 2.1.3 Electronic mail

Electronic mail refers to the exchange of messages between computers. Messages exchanged by electronic mail are generally alphanumerical and written in the form of readable text. They can be read directly on the computer screen, printed, or stored on a floppy or hard disk. Generally, electronic mail is sent using an intermediate network: either a value-added network (VAN) or a network connected to the Internet.

The success of electronic mail can be explained largely by the international acceptance of the X.400 standard, developed by the ITU-T (formerly the CCITT). Its goal is to ensure the harmonisation of exchanges and the establishment of various functions able to ensure the integrity of messages transmitted[28].

There are various commercial applications for electronic mail. On the intra-enterprise level, it allows the exchange of various messages such as memorandums. It also plays an important role on the inter-enterprise level with respect to the exchange of various commercial documents and the exchange of electronic forms as presented above.

The growing popularity of electronic mail carries with it a proliferation of initiatives intended to increase its usefulness and security. In relation to this, we should note the existence of the ITU-T X.435 standard that is intended to allow EDI messages to be sent by electronic mail[29], and the PGP (Pretty Good Privacy) cryptography software, invented by Phil Zimmerman, that is considered by some to be a *de facto* standard for the securement of electronic mail[30]. Finally we must mention the MIME (Multi-purpose Internet Mail Extensions) protocol, available free of charge, that permits the exchange of multimedia documents with enriched text, pictures and sounds[31].

### 2.1.4 Fax

Fax machines (fax or telefax) provide many possibilities. With respect to commerce, the fax machine is a special tool that can be used to transmit various documents (shipping documents, sales orders, invoices, etc.).

The most well-known way to use a fax machine is to connect it directly to a telephone network. The fax machine produces an image of all forms of graphics (text, drawings, etc.). Such an image, transmitted in electronic form, is then faithfully reproduced on paper by the addressee's fax machine[32]. While most fax machines print messages as soon as they are received, some have memory functions and access control. Messages sent to a specific

[28] Eric ARNUM, “Computer-fax blends with LAN E-mail and EDI”, (1993) *EEMA Briefing* 16.

[29] Robert HARROLD, “X.435 Bringing EDI and E-mail Together”, (1994) *EDI World* 30.

[30] PGP utilise la technologie RSA. Pour plus d'information sur le logiciel PGP, voir http://www.mlink.net/~yanik/pgp/pgp2.html.

[31] On this subject, see : *MIME - Frequently Asked Question List* à http://www.math.uio.no/ nett/faq/ Mail/mime-faq/.

[32] Mireille ANTOINE, Marc ELOY and Jean-François BRAKELAND, *Droit de la preuve face aux nouvelles technologies de l'information*, C.R.I.D., Namur, Story-Scientia, 1992, p. 87.

addressee are printed only after that person enters a confidential access code. This provides a certain degree of confidentiality for exchanges.

Some software allows faxes to be sent and received directly from one computer to another, without printing on paper. Such faxes can be read directly on the computer screen, printed or saved in memory. The main difference between electronic mail and faxes is the fixed nature of faxes, which, once received, cannot be modified or processed using word processing or EDI software. The production of faxes that can also be processed, however, attenuates the differences between these two technologies.

### 2.1.5 Videotex

Videotex refers to bi-directional information services connecting a computer with a television set or another computer through telecommunications lines[33]. It is natural that such environments could become locations for commercial transactions.

The goal of videotex is to make a body of information available to different users in real time[34]. The simplest form of videotex is the electronic bulletin board[35], where the information is contained in a databank that can be accessed simultaneously by a number of users[36]. Thus videotex appears as an electronic catalogue that allows users to make purchases or place electronic orders, as well as engage in a whole variety of other transactions.

## 2.2. Communication media

The present section is devoted to presenting the main communication media: point-to-point communication, value-added networks and information highways.

### 2.2.1 Point-to-point communication

Point-to-point communication supposes direct communication between two or more users. The operation of such a communication medium requires the existence of a closed communication sub-system for the exchange of data in electronic form[37].

In such an environment, the users' respective computers communicate with each other over a public telephone network or another communication network. Each user must possess the equipment and software to make it possible for the computers to do this. The degree of

[33] Bob COTTON and Richard OLIVER, *The Cyberspace Lexicon, an Illustrated Dictionnary of Terms*, London, Phaidon Press, 1994, p. 208.

[34] Mireille ANTOINE, Marc ELOY and Jean-François BRAKELAND, *Droit de la preuve face aux nouvelles technologies de l'information*, C.R.I.D., Namur, Story-Scientia, 1992, pp. 88-90.

[35] Bulletin board (BBS).

[36] Benjamin WRIGHT, *The Law of Electronic Commerce : EDI, Fax and E-mail : Technology, Proof and Liability*, Boston, Little, Brown and Company, 1991, p. 12.

[37] Gerry DIAMOND and Edward G. HOWE, *Comprendre et choisir un réseau à valeur ajoutée*, Ottawa, Direction des industries des services et des transports, Affaires extérieures et Commerce extérieur Canada, May 1992, p. 15.

specialisation of the point-to-point communication generally requires that users hire qualified staff to see to the management and proper operation of exchanges.

### 2.2.2 Value-added network (VAN)

Value-added networks (VANs) relieve users of the need to create their own communication sub-systems. Such networks generally entail lower global communication costs and better verification controls and flow management[38]. Moreover, VANs take charge of the problems related to differences in transmission rates and communication methods between various types of computers.

As the following diagram shows, VANs provide electronic mailbox services[39].

Overview of a value-added network

Exporter, Insurer, Exporter, Bank, Warehouse Operator, Transportation Company, Exporter, Customs, Importer

A value-added network allows organisations to contact tens of thousands of other organisations virtually anywhere in the world by going through a single point of contact.

[38] *Ibid*.

[39] G. DIAMOND, *op. cit*., note 15, p. 16.

In such an environment, a user who wishes to transmit a message communicates with the VAN, to which he or she sends documents addressed to one or more addressees. The network operator is then responsible for sorting them and placing them in the addressees' mailboxes, where the intended recipients can pick them up. The addressees need only have computer systems compatible with the VAN's specifications.

### 2.2.3 Information highways, the Internet, extranets and intranets

The many networks and groups of networks are the key to the notion of an information highway. The principal players are the major public networks such as the *National Information Infrastructure Testbed* (NIIT)[40] and the *National Research and Education Network* (NREN)[41], to which we must add the private networks: *Prodigy*, *CompuServe*, *America Online* and *Microsoft Network*. Nevertheless, at present, the Internet is the main component of this highway, owing both to its popularity and to its global nature, as well as to the media attention it receives.

It has become a habit to describe the Internet as a virtual space in which people can communicate with each other, exchange information, etc. The Internet, as such, is not a homogenous entity. It is a result, a network of networks connected together. From those interconnections a cybernetic space results in which exchanges occur between all those who are able, in various ways, to access this environment.

[40] The first NIIT project is the Earth Data System (EDS) dedicated to the exchange of scientific information on the environment, see Mark L. GORDON and Diana J.P. McKENZIE, "A Lawyers Roadmap of the Information Superhighway", (1995) 13 *Journal of Computer & Information Law* 181.

[41] "The National Research and Education Network (NREN) was conceived in 1989 by then Senator Al Gore, and was later autorized by Section 102 of the High Performance Computing Act of 1991. The NREN is designed to build uppon and eventually replace the Internet. One of the key differences between the Internet and the NREN is the speed of data transfer. Whereas the Internet transmits at 45 megabits per second, the NREN transmits at 1.2 gigabits by second... To give an example of its capabilities, the NREN would be able to transfer the entier Encyclopedia Brtannica in approximately one second. This higher speed is especially important for researchers in fields like astronomy, meteorology, and high-energy physics, who require the higher data-transfer to develop more detailed models", Id., p. 182-183. See also *NREN : National Research and Education Network* à http://www.hpcc.gov/imp95/section.4.3.html.

Node A, Node B, Node C, Node D

The Internet is a collection of independent computers (nodes) that are situated virtually everywhere in the world and that communicate with each other. These nodes belong to and are managed by governments, universities and operating companies. Users of a specific node have access to other users and other nodes to exchange messages and transfer files.

Unlike a value-added network, the Internet is not a single enterprise.

The decentralised structure of the Internet, which was originally designed to resist any attempt to destroy it, excludes virtually any possibility of control by a single authority claiming to have mastery over it. Indeed, the Internet is a network of networks. It is the result of many connections between networks operating in accordance with the protocols that characterise it. The development of the Internet is also not the result of a planned approach: its growth is largely because of the spread of computer tools and the development of friendlier software and computer equipment.

The cybernetic space resulting from the Internet appears universal: it is not limited to a single national territory. Connections to the Internet most often occur through servers located in a given national territory. It is technically possible to connect to the Internet using most means of telecommunications.

Electronic communication is possible thanks to the establishment of connections between the various terminals of all those who wish to enter into communication: this is the notion of a network. The establishment of networks allows parties to be connected: these networks can themselves be connected to other networks and provide access to a multitude of correspondents. The network is the neuralgic element of the virtual environment often called "cyberspace"[42].

[42] Pierre TRUDEL and France ABRAN, Karim BENYEKHLEF and Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1997,p. 2 et ss..

### The Internet

The Internet is possible thanks to the existence of shared interconnection protocols and equipment supporting such technical protocols, thus allowing networks to be connected to each other. The Internet is a result of this: it follows from the fact that the networks are connected in accordance with shared protocols. It is characterised by the flow of information and works from one node to another. In consequence, the Internet would be impossible without the activities of organisations providing access to the various connected environments. These organisations are the networks.

The network is the constituent unit of the Internet. Networks of different sizes are connected to each other and the result of this is that access is provided to an immense interconnected network. This fact is expressed when the Internet is described as the "network of networks".

The Internet is not a unique environment: it is a result. The Internet is a result in the same way that a city is the result of an accumulation of activities, constructions and infrastructures. One does not regulate "the city", but the various activities that take place in it.

The Internet is not a homogenous entity. It is the result of interconnections uniting many participants in electronic communication. While the Internet is basically the sum of the networks that are connected together according to shared protocols, this should not lead us to lose sight of the fact that the basic unit of the Internet is the network. Networks are established by operators: without them there would be no Internet.

Since the Internet is the result of the connection of many networks according to shared protocols, control over the content flowing through it is ensured by the computer equipment that is connected to the network and that constitutes its components. Such equipment is controlled by network operators.

Message routing on the Internet is thus a function of the many computers in intermediate networks receiving, copying and retransmitting files carrying messages and works.

While not all computer networks belong to the Internet, network operation in compliance with the protocols characteristic of the Internet (TCP and IP) is clearly spreading, even in the cases of networks with access reserved for members or otherwise authorised persons, in other words, Intranets and Extranets.

### The intranet and the extranet

Sohier[43] explains that "the intranet, or inernetworking, is a concept in which Internet tools, such as the web and electronic mail, are used exclusively for an organisation".

[43] Danny J. SOHIER, *Guide de l'internaute*, Montréal, Éditions Logiques, 1998, p.464.

The concept of an extranet closely resembles that of the Intranet. It is a network accessible only by clients and suppliers of the organisation in question. Its goal is to facilitate the sharing of information between members of a specific group.

All the operations that can take place in a network environment are made possible by the hardware, software and human components of each network connected to the Internet.

### The hardware components of a network

The hardware component of a network is made up of its physical elements. Among such physical elements, the network nodes can be distinguished from the linkages. The nodes are the computers that contribute to routing transmissions and, in various contexts, they are called gateways, routers, etc. These computers receive, duplicate in live memory or elsewhere, and reroute works. The linkages connecting these nodes are telephone lines, cables, optical fibers, etc.

Among the nodes of a network, it is possible to identify those used to carry information. They are kinds of relays for network traffic and are dedicated to routing tasks. This is the case with switches, routers and gateways. The other nodes include the computers that perform computer applications. They are called hosts (host computers) since they host software applications.

With respect to hardware, users wishing to access the Internet must do so though the intermediary of a network operator connected to the Internet, which is usually called an Internet service provider. Users access the network by connecting at a point of presence.

### The software components of a network

Computers connected to the Internet communicate using a communication protocol called TCP/IP (Transmission Control Protocol/Internet Protocol). Dufour explains that "Communication protocols in the TCP/IP family ensure interoperability between heterogenous computers connected to the Internet. A communication protocol is a convention specifying the rules for exchanging information between two computers". In fact, the TCP/IP acronym refers to a large number of specialised communication protocols.

The basic functions of networks operating according to the TCP/IP protocol include mail (or messaging), transmission of files and distant connection.

The transfer of files allows information to be copied from one computer to another using the network as a medium of transmission. Several services offered in TCP/IP networks are based on the transfer of files from a computer to one or more client computers through computer-nodes connected to the network.

### The human "components" of a network

The notion of network also refers to an organisational context: that which allows people to connect their computers and transmit and receive messages and works. The network is thus a set of elements united by various organisational relations. Arnaud Dufour explains that “The human component of the Internet covers three categories of persons: network administrators, producers and service users”[44]. The network operator, generally the access provider, sees to the operation of the network. He or she has the means to solve the network’s hardware, software and interaction problems. The network is thus both an entrance and the place where it is possible to exercise a certain form of control.

Those operating a network have the possibility of inspecting what is travelling to and from the network they control or over which they have a certain hold. The fact that they choose to become involved, or not, in what is passing through their network does not change this fact. Users connect to the environment of a very specific network, not to the apparently infinite, centerless environment made up of the whole Internet.

The network operator is virtually the only one with the ability to regulate the actors participating. Only the operator knows the identity of its subscribers or clients, who can remain anonymous to other persons. It has mechanisms for measuring traffic and can have fee scales in accordance with various factors. In the Internet environment, only network operators have so many possibilities of exercising control over the activities occurring there.

Since network operators are the gatekeepers providing access to open electronic environments, it is in the framework of the relations they maintain with their clients that we see the emergence of certain standards and regulatory processes able to provide rules to ensure harmonious interactions. At this level there can be various forms of monitoring and verification of user and message compliance with standards existing in the network’s context.

The conjunction of the set of functionalities of interconnected networks such as the Internet has led several authors to consider it a cybernetic space of global dimensions. The technological environment allows one to be simultaneously, concomitantly or successively a producer, consumer, originator, receiver, place of origination and place of reception. The resulting commercial potential is virtually unlimited[45]. However it runs up against various security considerations.

The Internet is notorious for being less secure than VANs[46]. Obviously, the public nature of the Internet and the large number of users significantly increase the possibility of fraud. Nevertheless it is not very useful to compare these two communication media since VANs, as commercial entities, generally refrain from releasing information on the number and effectiveness of attacks on their networks. Thus it is not possible to establish a comparative ratio between the number of Internet users and of VAN users in relation to the number of successful attacks. Whether in the framework of a VAN or of the Internet, the main security guarantees of the originator’s identity, the authenticity of messages and their confidentiality lie not in the structure of the network itself, but in the securement of the messages carries on it. In this respect, electronic signature and encryption technologies are the best tools.

[44] Arnaud DUFOUR, *Internet*, coll. Que sais-je?, Paris, PUF, 1995 , p. 20. [My trans.]

[45] Torrey BYLES, “The Commercial Use of the Internet”, (1994) 7 *EDI Forum* 83.

[46] *Id.*, p. 83.

## 2.3. Risks inherent to electronic communication

As in the case of most commercial activities, electronic communication has risks. The present section is dedicated to identifying and presenting the main attacks on security in the context of computerised exchanges and the technologies able to counteract them.

The transmission of information between two parties is subject to certain risks inherent to any transaction. These risks are principally the non-identification of the originator, the alteration of data, repudiation and unauthorised disclosure of information. However, more globally, the generalisation of transactions in network environments has certain risks with respect to certain rights, social values and interests.

### 2.3.1 Non-identification of the originator

Impersonation, or masquerading, is a major risk in any transaction. It results from the unauthorised appropriation of an identifier or the simulation of an identifier belonging to another person. The risks of masquerading are in proportion to the accessibility of the network[47].

The consequences of impersonation must be considered serious. Thus, in the absence of formal identification, "*a competitor could use EDI to obtain, for example, a price list or confidential information concerning production plans. A bank could act on the basis of instructions seeming to come from a client but that, in reality, are transmitted by a hacker*"[48].

### 2.3.2 Alteration of data

The integrity of data is another major concern regarding information security. The data in a message can be changed, erased or inserted during transmission either accidentally or out of malice on the part of unauthorised people. The consequences of alteration of data composing a message can be major, especially when the message includes an authorisation accompanied by a signature. Thus, in such cases, once a message is signed any subsequent unauthorised modification of its content will render the object of consent invalid.

### 2.3.3 Unauthorised disclosure of data

Confidentiality is one of the major concerns in the transmission of dematerialised data. Respect for confidentiality can thus prove very important in the transmission of data of a personal nature or with economic value.

[47] Serge PARISIEN and Pierre TRUDEL, with the collaboration of V. WATTIEZ-LAROSE, *L'identification et la certification dans le commerce électronique : Droit, sécurité, audit et technologies*, Cowansville, Éditions Yvon Blais, 1996, p. 84.

[48] COMMISSION DES COMMUNAUTÉS EUROPÉENNES, *EDI et sécurité : Comment gérer le problème?*, Rapport préparé par le KPMG dans le cadre du programme TEDIS, 1992, p. 10.

In order to be effective, the confidentiality of information must be preserved at all stages, both during transmission and after reception. Moreover, since information can be derived from observing the flow of data, the confidentiality of the set of transmissions must sometimes also be ensured. For example, "*the level of economic activity of an enterprise can be determined by counting the number of messages sent and received, even if the content of the messages remains secret*"[49].

Attacks on confidentiality can be a result of a malfunction in the communication network, leading to erroneous routing of data, or caused by hacking.

### 2.3.4 Repudiation

Repudiation refers to when an originator denies, wholly or in part, having transmitted a message. Repudiation can be a consequence of a mistake, hacking, or simply the originator's refusal to acknowledge paternity and responsibility for a given message.

Repudiation can also occur when an addressee of a message who denies its reception or content. The consequences of repudiation must be considered seriously. For example, a company that produces a product on demand could, following repudiation of a message containing an order, be forced to cover the costs of manufacturing the product while receiving no revenue from its sale[50].

### 2.3.5 Breach of secrecy

Breach of secrecy is a violation under both common and civil law. Under both systems, it is considered that breach of trust causing harm is an offence and must be punished. Breach of secrecy through electronic mail or other means can cause significant harm and clearly engages the responsibility of the person who commits the indiscretion.

### 2.3.6 Harassment

Just as a telephone can be used to make inappropriate calls, it is possible to imagine use of electronic environments to harass people, to send them unpleasant or aggressive messages. This behaviour enlists the responsibility of the person who performs such an act. It could also possibly bring into question the responsibility of certain intermediaries.

### 2.3.7 Copyright infringement

Virtually all communication of protected works on the Internet, including those contained in private electronic messages, involve the reproduction of works in the sense of

[49] COMMISSION DES COMMUNAUTÉS EUROPÉENNES, *EDI et sécurité : Comment gérer le problème?*, Rapport préparé par le KPMG dans le cadre du programme TEDIS, 1992, p. 11. [My trans.]

[50] Serge PARISIEN, and Pierre TRUDEL, with the collaboration of V. WATTIEZ-LAROSE, *L'identification et la certification dans le commerce électronique : Droit, sécurité, audit et technologies*, Cowansville, Éditions Yvon Blais, 1996, p. 85.

copyright legislation. Electronic environments can be used to commit copyright infringement[51]. Under the terms of international agreements any unauthorised reproduction of a work, including a disguised imitation, that is made or imported contrary to the provisions of legislation is a counterfeit. The infringement may be direct, in other words result from the actions of a person, or indirect, when an intermediary knows the infringement is taking place but does nothing to stop it.

### 2.3.8 Criminal acts

Criminal acts committed using electronic environments obviously entail the responsibility of those who commit them. Presently, aside from certain difficulties respecting evidence, the courts in many countries have applied provisions of their criminal law to activities taking place on the Internet in the same way as to activities taking place in other environments. However the issue remains problematic with respect to intermediaries that do not take an active role in the criminal activity but that could, under certain circumstances, be considered accomplices to criminal acts occurring in electronic environments wholly or partially under their control.

## 3. Legal admissibility of dematerialised data – The *Model Law on Electronic Commerce*

A legal transaction is not generally admissible as evidence unless it is recorded in writing. In most countries, the imagination of jurists remains strongly marked by the belief in the superiority of documentary evidence in the form of a writing. This shows the importance of initiatives to determine the conditions of admissibility, as evidence, of dematerialised data.

The *Model Law on Electronic Commerce*[52] was developed by UNCITRAL to deal with a profound change in the means of communication between parties using computerised and other modern techniques to conclude business. Its purpose is to serve as a model for countries in the evaluation and modernisation of certain aspects of their legislation and practices with respect to communications involving the use of computers and other modern techniques, and in the adoption of relevant legislation when it is lacking.

The model law could have a strong ripple effect on new areas of government legislation, such as electronic commerce. This model law contains seventeen articles. It is divided into two parts, one dealing with electronic commerce in general and the other with electronic commerce in specific fields.

Articles 6 and 8 cover, respectively, the notions of “writing” and “original”.

According to Article 6:

[51] Joseph R. PRICE, “Colleges and Universities as Internet Service Providers : Determining and Limiting Liability for Copyright Infringement”, [1996]23 *Journal of College and University Law*, 183, p. 191.

[52] UNCITRAL, Model Law on Electronic Commerce with Guide to Enactment *1996*, New York, United Nations, 1997.

> *(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:* [...]

The purpose of Article 6 is to define the basic standard to be met for a data message to be considered to fulfil the requirements entailed by legislation, regulations or case law.

When the model law was developed, special attention was paid to the roles traditionally played by various forms of "writings" on paper. Thus, the Commission considered that it would not be appropriate to adopt an excessively general definition of the roles of a writing since the requirement that the data must be presented in writing is often combined with the concepts of signature and original.

In accordance with the functional approach, the requirements inherent to a "writing" must be considered low on the hierarchy of formal conditions provided in national legislation. Thus the minimum requirement that data be presented in writing must not be confused with stricter requirements, such as the production of a "signed writing", a "signed original" or an "authenticated legal act".

Among other things, the Commission chose to consider the notion of inalterability as not being inherent to that of a writing since, for example, a document written in pencil could still be considered a "writing" under certain legal regimes.

Thus, Article 6 does not target provisions stating that in all cases data messages must perform all possible functions of a writing. Rather than focussing on specific functions of the "writing", for example its function as evidence in the context of tax law or as warning in civil law, Article 6 refers to the fundamental criterion of reproducible, legible information.

Paragraph 3 of Article 6 is intended to allow a state to provide for exceptions to this principle in the case of certain specific situations.

The notion of the original certainly appears to be one of the most problematic to transpose into the virtual world. In computer environments it is difficult to separate what is an original from what is a copy. Moreover, in digital environments, the differences in quality between the original and the copy tend to be blurred. The notion of original seems deeply marked by the conditions and limitations inherent to the paper world. Thus Article 8 of the model law provides that:

> *(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:* [...]

The model law dedicates an article to the notion of original. First it is to remedy the difficulties that are often raised by the definition of this notion. If what is meant by "original" is the medium on which the information is recorded for the first time, the transmission of original electronic messages proves impossible because the addressee of a data message in fact always receives a copy of the message. Moreover, it seemed useful to the Commission to provide a functional definition of the notion of "original" given that, in practice, a number of disputes focus on the issue of the originality of documents. The requirement that originals be presented is one of the main obstacles that the law tries to eliminate.

In a paper environment, only the "original" is generally accepted as evidence, so as to reduce the risk of alterations. In order to solve this problem, Article 8 thus states various means to certify the content of a data message in order to confirm its originality.

Article 8 must be considered as defining the minimal acceptable formal condition for a data message to be considered the functional equivalent of an original. On this view, Article 8 underlines the importance of the integrity of information in determining its "originality" and states the criteria to be taken into consideration to evaluate integrity by referring to:

- systematic recording of information;
- assurance that all the information was recorded;
- and protection of the data against any alteration.

Article 8 in fact states the notion of originality in terms of a specific method that it defines. Thus the subparagraph of paragraph 3 states the criteria used to assess the integrity of a document while taking care to distinguish alterations that could be considered fraudulous (or unauthorised) from use-related additions to an original message, such as endorsements and certification of identity. These additions in no way diminish the original nature of a message.

In fact, if an electronic certificate is added to the end of a data message or if data is automatically added to the beginning and end of a data message for transmission purposes, such additions should be considered, for example, as the envelope and stamp used to send a paper message.

Legal recognition of data messages is provided for in the model law. Articles 9 and 10 cover the admissibility and evidential weight of data messages. Under the terms of Article 9:

> *(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.*

The purpose of Article 9 is to increase the admissibility and evidential weight of dematerialised documents. With respect to admissibility, Paragraph (1)(a) simply provides that data messages must not be rejected as means of proof in legal proceedings for the sole reason that they are in electronic form. Paragraph (1)(b) provides for the inclusion of the rule of best evidence as a possible criterion for evaluating evidence, primarily to meet the requirements of common law systems.

Finally, with respect to assessing the evidential weight of a data message, Paragraph (2) contains various indications of how to do so, for example, by assessing whether they were created, stored and communicated reliably.

Article 10 states a set of rules relating to present requirements concerning the storage of information[53]. According to Article 10:

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

[53] UNCITRAL, Model Law on Electronic Commerce with Guide to Enactment *1996*, New York, United Nations, 1997, p. 44.

> *(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.*

Under the terms of paragraph (1)(a), the word “accessible” implies that information presented in the form of computerised data must be legible and interpretable. The word “reference” refers not only to reference by humans but also to computer processing. The expression “for subsequent reference” was chosen instead of notions of “durability” and “unalterability” because, according to the Commission, they would have been excessively strict standards. Likewise, the member states of the Commission considered that notions such as “legibility” and “intelligibility” were, generally, too subjective to be useful as criteria.

Paragraph (1)(b) emphasises that the message need not be retained unmodified so long as the information retained precisely represents the data message as it was transmitted. According to the Commission, it would not be appropriate to require that the information be retained without modification since, in general, messages are decrypted, compressed and converted in order to be saved.

Paragraph (1)(c) is intended to cover, in addition to the message itself, certain information that is related to transmission and can be necessary for identifying the message. We must note that this is a criterion that is stronger than most criteria applied under national legislation for the storage of communications on paper. However, paragraph (2) states that this requirement does not extend to information that has no purpose other than to permit the transmission and reception of data messages.

Finally, paragraph (3) of Article 10 is meant to recognise the validity of the practice according to which message retention is ensured by a person other than the originator or the addressee, such as an intermediary or trusted third party.

In sum, the model law is inspired by a global approach to electronic commerce. It advances an approach allowing a solution to be found for the problem of admissibility and evidential weight of dematerialised evidence and so free legal regimes from dogmatic belief in the written’s superiority over the digital.

## 4. Technical security mechanisms

There are security solutions that could counteract the risks entailed by the exchange of computerised documents and their signature.

### 4.1 Encryption mechanisms

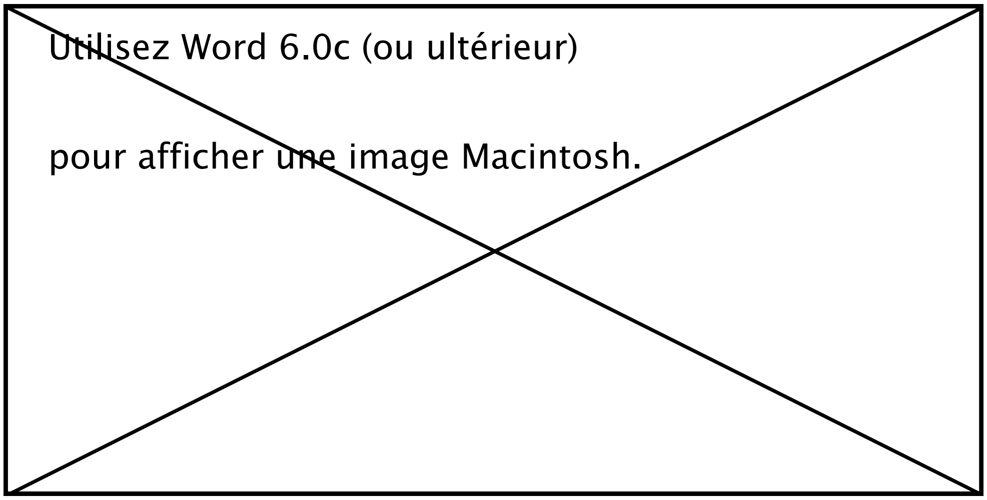
Encryption technologies allow the confidentiality of exchanges to be ensured. Most of the products presently available on the market are based on the *Data Encryption Standard* (DES). The operation of the DES, and its advantages and disadvantages in relation to public key encryption and the *Escrow Encryption Standard* (EES), are presented here.

#### 4.1.1 Symmetrical cryptography (DES)

Promoted by the American *National Security Agency* in 1977 as a standard for the American Administration, the *Data Encryption Standard*[54] is the most widespread secret key encryption system in the world.

Symmetrical secret (or single) key cryptography systems use algorithms that, as their name indicates, encrypt and decrypt messages using a single key. As an illustration of how single key cryptography works, see how Alice sends an encrypted message to Bob.

*Figure I* Alice; message (clear text); encryption algorithm, encrypted text; decryption algorithm; message (clear text); Bob


Utilisez Word 6.0c (ou ultérieur)
pour afficher une image Macintosh.

[54] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *FIPS Publication 46-1 : Data Encryption Standard*, 22 January 1988.

The computer milieu almost unanimously considers the DES to be perfectly secure and able to resist most attacks by individuals. In fact, in spite of the efforts of a number of researchers, attacks on the DES have not yet been crowned with success[55].

Regarding encryption, the security of a cryptosystem is generally evaluated in terms of time and money. In the case of the DES, it is estimated that a specialised computer able to break a secret key in 3.5 hours of work would cost one million US dollars[56]. In this sense, while it is unlikely that an individual armed with a simple personal computer could manage to pierce DES defences, this potential remains entirely within the scope of large companies and governments. The interconnection of a number of personal computers also allows a substantial increase in the effectiveness of attacks on the DES. Thus it is estimated that 500 interconnected "Pentium 100" computers would have one chance in 40 000 to break a secret key in a single day[57].

This scenario is not purely fictional. A group of mathematicians and computer engineers recently connected over 600 computers in order to perform some 100 quadrillion mathematical operations over an eight-month period[58]. According to experts, the mathematical problem solved in this way clearly surpassed the complexity required to break a DES secret key.

One of the solutions considered to reinforce the DES and prevent such attacks rests on the use of a triple DES. A triple DES supposes that each block of a message is encrypted under three different keys[59]. This technique allows more powerful attacks to be checked, though it does increase the time needed to encrypt and decrypt messages. In fact, it seems improbable that the possibilities of computer calculation, in spite of its remarkable progress, could threaten the confidentiality of messages encrypted in this way in the near future[60]. Moreover, the watertightness of triple DES appears so remarkable that it has not gone without raising some concern on the part of the American government. The latter's establishment of the *Escrow Encryption Standard*, intended to replace the DES, is probably related to this.

Whether or not triple encryption is used, DES security is not infallible. Indeed, one of the problems related to this technology lies in the fact that the single key must, at some point, be transmitted to the addressee of the message or that person will not be able to decrypt it. Thus is it clear why it could be dangerous to transmit the secret key using uncertain means on a computer network. A third party who intercepted the key could decrypt the accompanying

[55] RSA, *DES*, http://www.rsa.com/rsalabs/faq/faq_des.html.

[56] Douglas R. STINSON, *Cryptography : Theory and Practice*, Londres, CRC Press, 1995, p. 83.

[57] Gilles GARON and Richard OUTERBRIDGE, "DES Watch : An Examination of the Sufficiency of the Data Encryption Standard for Financial Institution Information Security in the 1990s", (July 1991) 15 *Cryptologia* 177.

[58] Brian HAYES, "The Magic Words Are Squeamish Ossifrage", (1994) 82 *Am. Scientist* 312.

[59] See : R.C. MERKLE and M.E. HELLMAN, "On the security of multiple encryption", (1981) 24 *Communications of the ACM* 465. See also Douglas R. STINSON, *Cyptography : Theory and Practice*, Londres, CRC Press, 1995, p. 93.

[60] RSA, *DES* : http://www.rsa.com/rsalabs/faq/faq_des.html.

message, and any other message protected by that key, at leisure[61]. Nevertheless, as mentioned above, the use of public key cryptography could remedy this situation.

Finally, it should be noted that since the DES is considered a weapon under the *Export Administration Regulation*[62], and the *International Traffic in Arms Regulations*[63], in theory it cannot be exported outside of the United States. However neither of these pieces of legislation have been sufficient to prevent the spread of the DES, which remains widely used everywhere in the world[64].

### 4.1.2 The Escrow Encryption Standard (EES)

The goal of the *Capstone* project is to develop a series of obligatory cryptographic standards for the government and for any private entity transacting with it[65]. This project is supported by the *National Institute of Standard and Technology* (NIST) and the *National Security Agency* (NSA).

The *Escrow Encryption Standard* (EES) is an integral part of the *Capstone* project, which contains, in addition to this encryption algorithm, three other components: a signature algorithm, the DSS; a hashing function, the *Secure Hash Standard* (SHS)[66] and a key exchange protocol that has not yet been completed. Each of these components is included in a microprocessor called the *Capstone Chip*, which is intended to be built into computer modems. In contrast, only the EES is included in the *Clipper Chip*, which is intended to be included in telephone equipment.

The EES encryption algorithm, also known as *Skypjack*, was adopted in 1994 as the *Federal Information Processing Standard* (FIPS)[67]. It operates in a way analogous to that of the DES in that only one key is needed to encrypt and decrypt messages, The main difference

[61] Phil ZIMMERMAN, *PGP User's Guide Volume I : Essential Topics*, PGPDOC1.TXT, 1993, p. 3.

[62] *Export Administration Regulation*, 15 C.F.R., sect; 768-99 (1994).

[63] *International Traffic in Arms Regulations*, 22 C.F.R., sect; 121.1 (XIII)(b)(1) (1994).

[64] See : Michael FROOMKIN, “The Metaphor is the Key : Cryptography, the Clipper Chip and the Constitution”, (1995) 143 University of Pennsylvania Law Review 709; also available at: http://www-swiss.ai.mit.edu/6095/articles/froomkin-metaphor/ partIC.html#ToC25 : “The ITAR have failed to prevent the spread of strong cryptography. The ITAR prohibit export of cryptographic software, nevertheless software created in the United States routinely and quickly finds its way abroad. For example, when version 2.6 of PGP, a popular military-grade cryptography program, was released in the United States by graduate students at MIT as freeware, a researcher at the Virus Test Center at the University of Hamburg, in Germany, received a copy within days from an anonymous reMailer. He then placed it on his internationally-known Internet distribution site. [...]

Meanwhile, enforcement of the ITAR has produced absurd results. The State Department has refused to license the export of a floppy disk containing the exact text of several cryptographic routines identical to those previously published in book form. The refusal was all the more bizarre because the book itself was approved for export. The only reasons given by the State Department for its refusal were that “[e]ach source code listing has been partitioned into its own file and has the capability of being compiled into an executable subroutine”, and that the source code is “of such a strategic level as to warrant” continued control. The State Department also concluded that the “public domain” exception to the ITAR did not apply and--most bizarrely of all--that its decision was consistent with the First Amendment”.

[65] As provided for in the *Computer Security Act*, 1987, Pub. L. No. 100-235, 101 Stat. 1724.

[66] NIST, *FIPS Publication* 180 : Secure Hash Standard (SHS), 11 May 1993.

[67] NIST, *FIPS Publication* 185 : Escrow Encryption Standard (EES), 4 February 1994.

remains the possibility the EES offers American authorities of decrypting messages encrypted using the *Clipper Chip* and the *Capstone Chip*[68] at will.

Indeed, each of these microprocessors has a unique serial number and a unique encryption key, which are held simultaneously by the American government and the user[69]. In order to ensure the key possessed by the government is protected, it is divided into two segments that are entrusted to two different governmental organisations. These organisations then act as Escrow Agents[70] with responsibility for preserving the confidentiality of the key segment entrusted to them. That segment may be communicated only under certain circumstances to authorised persons, for example when a valid search warrant is issued by a competent court[71]. Under such circumstances, both segments of the key can be united and it becomes possible to decrypt any messaged protected by it.

The EES uses 80-bit mathematics[72]. Thus it appears more secure than the single DES used without the triple encryption technique[73]. Nevertheless it is important to note that aside from the way it is presented in the FIPS 185, the details of the EES are protected by state secret. This decision on the part of the American government has provoked some criticism. Since the EES cannot be given meticulous examination by the public and experts in cryptography, many hesitate to endorse the claims of the NIST and NSA regarding its security[74]. Since the details about how the DES operates have been public for several years, such examination has allowed the failures and weaknesses of that algorithm to be detected

[68] The details relating to this technology are complex and, in part, covered by state sectret. For a technical presentation of the EES, see RSA, *Capstone, Clipper and DSS*, http://rsa.com/rsalabs/faq/faq_ccd.html#ccd.3 : "When two devices wish to communicate, they first agree on an 80-bit "session key" K. The message is encrypted with the key K and sent; note that the key K is not escrowed. In addition to the encrypted message, another piece of data, called the law-enforcement access field (LEAF), is created and sent. It includes the session key K encrypted with the unit key U, then concatenated with the serial number of the sender and an authentication string, and then, finally, all encrypted with the family key. The exact details of the law-enforcement field are classified. The receiver decrypts the law-enforcement field, checks the authentication string, and decrypts the message with the key K. Now suppose a law-enforcement agency wishes to tap the line. It uses the family key to decrypt the law-enforcement field; the agency now knows the serial number and has an encrypted version of the session key. It presents an authorization warrant to the two escrow agencies along with the serial number. The escrow agencies give the two parts of the unit key to the law-enforcement agency, which then decrypts to obtain the session key K. Now the agency can use K to decrypt the actual message." See also Dorothy E. DENNING, "The Clipper Encryption System", (1993) 81 *Am. Scientist* 319-323.

[69] RSA, *Capstone, Clipper and DSS*, http://rsa.com/rsalabs/faq/faq_ccd.html#ccd.3.

[70] En anglais : "Escrow Agent".

[71] See Michael FROOMKIN, "The Metaphor is the Key : Cryptography, the Clipper Chip and the Constitution", (1995) 143 *University of Pennsylvania Law Review* 709; aussi disponible à : http://www-swiss.ai.mit.edu/6095/articles/froomkin-metaphor/ partIC.html#ToC27.

[72] NIST, *FIPS Publication* 185 : Escrow Encryption Standard (EES), 4 February 1994.

[73] RSA, *Capstone, Clipper and DSS* : http://rsa.com/rsalabs/faq/faq_ccd.html#ccd.3. : "It uses an 80-bit key to encrypt 64-bit blocks of data; the same key is used for the decryption. Skipjack can be used in the same modes as DES (see How does one use DES securely?), and may be more secure than DES, since it uses 80-bit keys and scrambles the data for 32 steps, or "rounds"; by contrast, DES uses 56-bit keys and scrambles the data for only 16 rounds".

[74] Oreover, the other disadvantage of this statute is that the EES can be used only as « hardware », and not as software.

and necessary corrections made[75]. This explains, at least with respect to security, why the DES is more popular than the EES[76].

### 4.1.3 Asymmetrical cryptography (RSA)

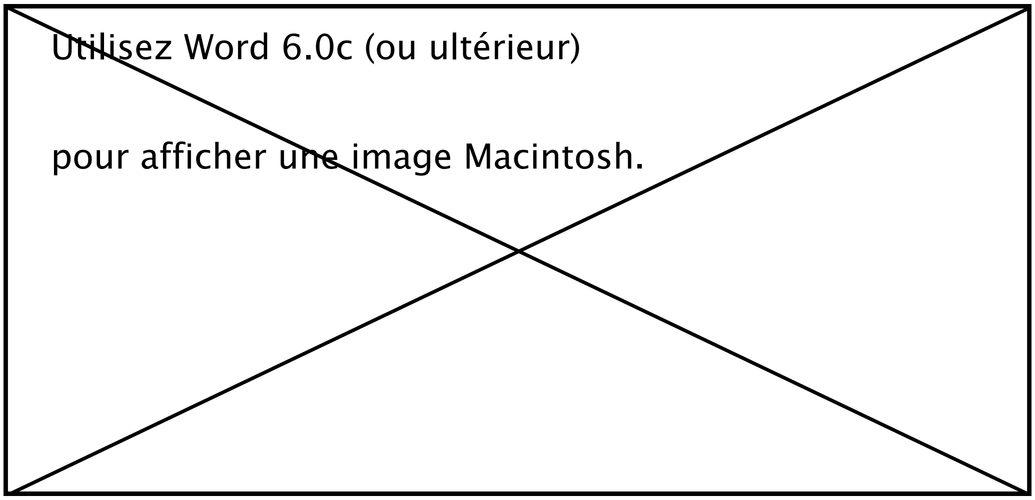
The main commercial application for public key encryption is that proposed by RSA. In encryption systems based on public key encryption, users have a pair of complementary mathematical keys, one of which can be revealed publicly and one that must remain private. These complementary keys are intimately related: one is the encryption, or “public” key, while the other is the decryption, or “private” key. Only the private key makes it possible to decrypt a message encrypted with the complementary public key. Moreover, it should be noted that the private key can not be deduced from the corresponding public key.

As an illustration, here is how Alice can transmit a message to Bob with complete confidentiality. After having written a message, Alice uses Bob’s public key (his encryption key) to encrypt the message. Even if a third party were to intercept the message transmitted by Alice, Bob would still be the only person able to decrypt it because he alone has the complementary private (decryption) key. Even Alice, who wrote and encrypted the message, is unable to decrypt it.

[75] RSA, *Capstone, Clipper and DSS* : http://rsa.com/rsalabs/faq/faq_ccd.html#ccd.3.

[76] In order to respond to this criticism, the government has invited a group of independent cryptography experts to analyse the details of the EES. In their report, these experts came, however, to the conclusion that their study is too limited to be able to provide a definitive judgement on the level of security offered by the EES. See E.F. BRICKELL, D.E. DENNING, S.T. KENT, D.P. MAHER et W. TUCHMAM, *Skipjack Review, Interim Report : The Skipjack Algorithm*, 23 July 1993.

*Figure II* Alice; Message (clear text); encryption algorithm; encrypted text; decryption algorithm; message (clear text); Bob’s public (encryption) key; Bob’s secret (decryption) key



Utilisez Word 6.0c (ou ultérieur)

pour afficher une image Macintosh.

Nu

Public key encryption and the DES are both relatively secure encryption technologies. The major advantage of public key encryption lies in the fact that the secret key does not need to be known by the originator. Unlike in the case of the DES, it is thus not necessary to transmit the decryption key to allow the addressee to decrypt the message. However the main disadvantage of such a system lies in the speed of execution of the encryption and decryption functions. As a comparison, when it is installed as software, the DES allows such operations to be performed 100 times faster than does the RSA software[77], while in the case of hardware, the DES proves 1000 to 10 000 times more rapid. While it is legitimate to claim that this difference will diminish in the future, it is very unlikely, as RSA itself admits, that public key encryption will someday manage to equal the performance of the DES[78]. For this reason, with the exception of very short messages, the use of the DES is recommended.

Joint use of public key cryptography and the DES, or even the triple DES, is however a promising alternative[79]. Using to this option, the message is encrypted using the DES (see Figure I), while the secret DES key permitting decryption of the message is encrypted using public key cryptography (see Figure II)[80]. The transmission of the message, encrypted using the DES, and the secret key, encrypted using public key cryptography, provides secure and effective encryption while avoiding the risks entailed by the transmission of the secret DES key.

Use of this technique is not however necessary under all circumstances. Thus, when the parties agree on a secure means of transmission for the secret DES key, for example from person to person, the use of public key encryption proves needless. Likewise, it is not used for encrypting archives or internal transaction logs that will not be transmitted by computer means.

RSA's public key encryption technology is subject to the same export restrictions as the DES. Nonetheless it is commercialised abroad by non-American bodies, in spite of the export policies of the United States government[81]. Finally, as will be discussed below, it should be noted that public key encryption can also be used to produce electronic signatures.

### 4.2 Network security mechanisms

The operation of a communication network, whether it is open or closed, exposes dematerialised exchanges to certain risks that require the existence of appropriate security measures. The more complex the system, the more likely it is to have breaches in its security.

[77] RSA, *RSA* : http://www.rsa.com/rsalabs/faq/faq_rsa.html.

[78] RSA, *RSA* : http://www.rsa.com/rsalabs/faq/faq_rsa.html.

[79] This technique is sometimes called a digital ”envelope”.

[80] RSA, *RSA* : http://www.rsa.com/rsalabs/faq/faq_rsa.html.

[81] “RSA used for authentication is more easily exported than when used for privacy. In the former case, export is allowed regardless of key (modulus) size, although the exporter must demonstrate that the product cannot be easily converted to use for encryption. In the case of RSA used for privacy (encryption), the U.S. government generally does not allow export if the key size exceeds 512 bits. Export policy is currently a subject of debate, and the export status of RSA may well change in the next year or two. Regardless of U.S. export policy, RSA is available abroad in non-U.S. products”, RSA; *RSA* : http://www.rsa.com/rsalabs/faq/faq_rsa.html.

Every point of entry to the system (integrated servers, interpreters, etc.) is a target for hackers. More modest operating systems are thus less exposed to such attacks. Nevertheless, particularly with respect to commerce, security sometimes gives way to flexibility and convenience[82].

Essentially, network security is in inverse proportion to the number of users. This is why there are various mechanisms for restricting and controlling access to networks[83].

### 4.2.1 Firewalls

Firewalls are systems that reinforce control over access to a network. They are bi-directional barriers able, depending on their configuration, to control access from the outside into the network as well as to control what leaves the network toward the outside[84].

A firewall must be part of a general, consistent security infrastructure. Its operation rests on the premise that those who wish to access the network must pass through a point of access protected by the firewall. In consequence, the firewall will be ineffective if there are unprotected points of access.

It is not appropriate to base the security of a network solely on a firewall, particularly when confidential information is transmitted. It seems more prudent to add various security techniques to it, such as restrictions by address or domain name. Finally, it is important to remember that a firewall cannot protect the network from attacks initiated from the inside[85].

### 4.2.2 Restriction by address or domain name

It is possible to protect individual directories and documents so that only specific browser software, connecting to the network from predetermined addresses, can have access to them. Such restriction of access is useful against the simply curious, but it cannot withstand attacks by hackers with sufficient resources to counter it. Thus it is possible for the latter to give fraudulent information to the host server, telling it that the connection is made from an authorised address. In order to be secure, this type of access restriction must be used in conjunction with an identification mechanism. The use of a firewall able to detect and reject successive, fraudulent attempts at access can increase the general level of security.

Restricting access using domain names carries the same risks as restricting access by address. Thus it is possible for a user to fraudulently present the name of an authorised host as belonging to a foreign address. In order to fight against this sort of attack, certain servers have acquired a domain name search function for each access request. This allows them to ensure that the address really does correspond to the domain name indicated.

[82] Lincoln D. STEIN, “The World Wide Web Security FAQ” : http://wwwgenome.wi.mit.edu/WWW/faqs /www-security-faq.html.

[83] “Almost Everything you ever wanted to know about security” : http://www.cis.ohio-state.edu/hypertext/faq/usenet/security-faq/faq.html.

[84] William DUTCHER, “If you can't reach them, they can reach you” : http://www.crpht.lu/CNS/html/PubServ/Security/Documents/Pcweek-Online/tfire.html.

[85] “Firewalls FAQ”, http://www.cis.ohio-state.edu/hypertext/faq/usenet/firewalls-faq/faq.html.

### 4.2.3 Password or personal identification number (PIN)

A personal identification number is another method for restricting access to a network. At the time of access, the system requires the user to enter a personal, confidential password. If the password is valid, access to the network is authorised.

However, there are certain disadvantages to restriction by user name and password (PIN). Prudence is required when choosing a password. Too often users choose password hackers find easy to identify, such as their birth dates or telephone numbers. Moreover, it is important to note the existence of programs specifically designed to identify passwords.

A password shared among various users also creates risks for infringement of access control security, just as does the unsecured transmission of the password to the server. Thus password confidentiality must be ensured, in particular by the use of encryption technology.

## 4.3 Identification mechanisms

The present section is dedicated to various mechanisms for identifying actors in a dematerialised environment. Special attention is given to electronic signature, personal identification numbers (PINs) and biometric technology.

### 4.3.1 Digital signature based on asymmetric cryptography (RSA)

The asymmetrical cryptography known as “public key” was conceived in 1975 by two electrical engineers, Whitfield Diffie and Martin Hellman of Stanford University, and made a reality by Ronald Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology[86]. Public key, or digital, signature procedures are currently used in electronic commerce and have advantages, in addition to identification of the parties. They provide an assurance of the integrity of the message. In other words, they guarantee that the message has not been altered between the time it was signed and the time it was received by the other party. Moreover, with respect to confidentiality, they provide a guarantee that only the computer system of the addressee is able to read the message transmitted. These are undeniable advantages that do not exist in a paper environment and that will meet the strictest security requirements.

In a public key system, the performance of various identification operations supposes that a person has two complementary mathematical keys: a private key that must be kept secret, and a public key that can be distributed freely. The private key allows one to sign the message. The decoding operation is performed according to the complementary nature of the keys: a message encrypted with a private key can be decrypted only with the complementary public key. The following example illustrates how digital signature works.

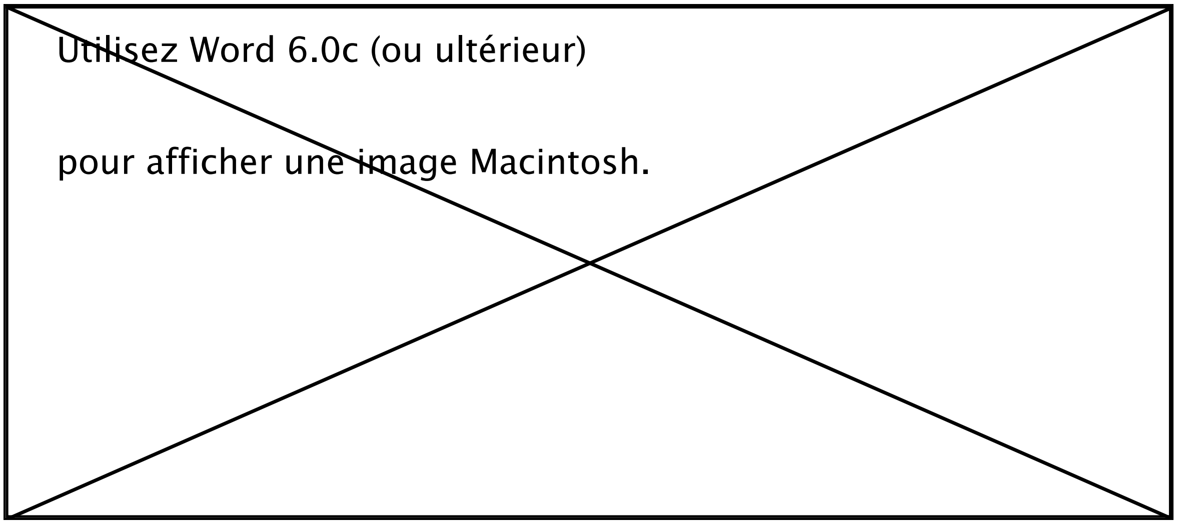
Alice wishes to send Bob a computerised message signed electronically. After writing the message, Alice performs a message digest using a mathematical operation. This digital

[86] *Report of a Special Panel of the ACM U.S. Public Policy Committee (USACM)*, June 1994, p. 44 : ftp://ftp.cpsr.org/cpsr/privacy/crypto/acm_crypto_study.txt.

digest is the result of a function called a “one-way hash function”, or a “message digest function”. This function allows the concise generation of a sequence of data representing the message in question. This representation is secure, very concise and allows the detection of any change made to the message. All the addressee needs to do is apply the “hash” function to the message received and compare the digest so obtained with that transmitted by the originator. Any difference between the digests means the message was altered during transmission.

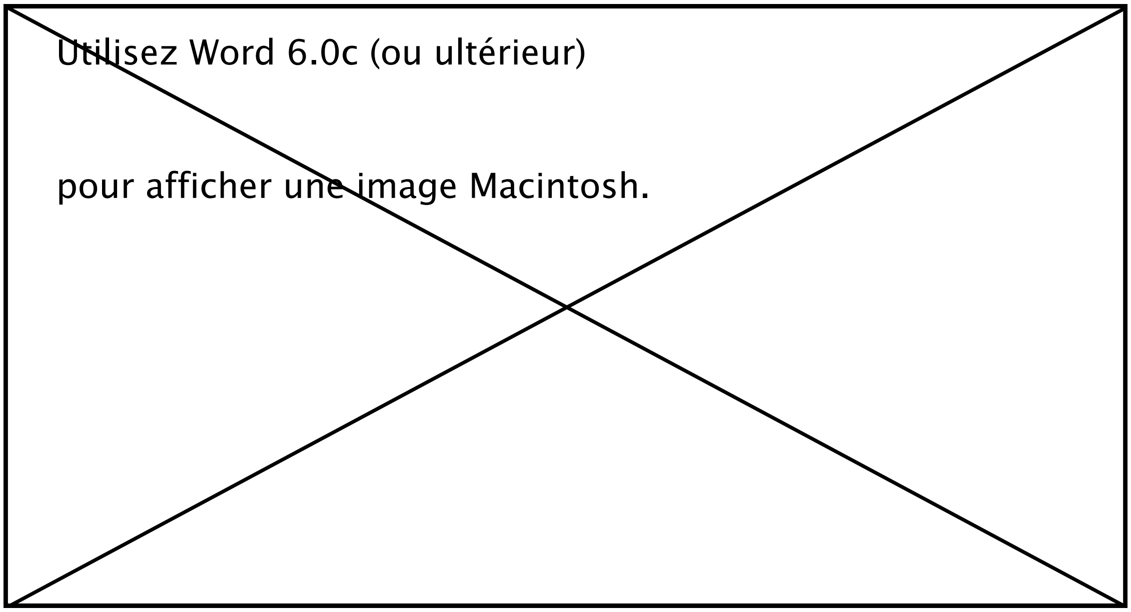
This digest is then encrypted (made illegible and inaccessible) using Alice’s private key. This encrypted digest is the digital signature. Alice sends Bob the message (in clear text) accompanied by the digital signature.

*Figure III* Message; hashing function; message fingerprint; digital signature; private key; message; to addressee


Utilisez Word 6.0c (ou ultérieur)
pour afficher une image Macintosh.

When Bob receives the message and the signature, he decrypts the digital signature by performing a mathematical operation involving Alice’s complementary public key. If he manages to decrypt the signature, Bob is assured that it was encrypted using Alice’s complementary private key. He knows for certain that she is the author of the message. Thanks to the hashing function, he is also assured of the integrity of Alice’s message.

*Figure IV* From signatory; message; digital signature; hashing function; message fingerprint; verification of validity; public key



Utilisez Word 6.0c (ou ultérieur)

pour afficher une image Macintosh.

The chief application for public key (digital) signature is that proposed by RSA. Its reliability and high degree of security make it a *de facto* standard in electronic commerce[87]. RSA technology is an integral part of various official standards throughout the world. Thus it figures in the ISO 9796 standard as an accounting algorithm, and in the ITU-T (CCITT) X.509 standard. RSA technology is also incorporated into the SWIFT and ETEBAC 5 standards and is part of the draft ANSI X9.31 standard[88].

RSA technology is patented. The patent, held since 1983 by Public Key Partners (PKP) of Sunnydale, California[89], will expire in the year 2000. A license and payment of a fee are thus required to be able to use or sell RSA. Nevertheless, both in the United States and Canada, PKP generally authorises the non-commercial use of RSA technology for personal, academic and intellectual purposes[90]. This authorisation is not presumed: it is subject to the written approval of PKP. The American government has the benefit of unlimited free use of RSA since this technology is a result of research it partially funded.

#### 4.3.2 The Digital Signature Standard

Having begun its work in 1989, the *National Institute of Standard and Technology* (NIST) announced the completion of the *Digital Signature Standard* (DSS) and its adoption as the *Federal Information Processing Standard* (FIPS)[91]. on May 19, 1994. The signature algorithm specified in the DSS is the *Digital Signature Algorithm* (DSA). It can be used for electronic messaging, electronic funds transfer, EDI, archiving or, more generally, any application requiring that the integrity and origin of transmitted data be assured[92]. Its purpose is to be used as a standard by the public sector and, on a voluntary basis, by anyone in the private sector[93]. This algorithm is made available to the public free of charge. Moreover it is one of the reasons given by the NIST not to adopt the popular RSA as a standard. This organisation preferred to choose an unpatented algorithm that could be used free of cost by the private sector[94].

The DSA uses a private key in order to create a signature and a complementary public key to verify it. It is based on a cryptosystem proposed by ElGamal[95]. Unlike RSA technology, the DSA is not, however, reversible and so cannot be used to encrypt a message.

[87] RSA, *RSA's FAQ About Today's Cryptography :* http://www.rsa.com/rsalabs/faq/ faq_rsa.html.

[88] RSA, *RSA's FAQ About Today's Cryptography :* http://www.rsa.com/rsalabs/faq/ faq_rsa.html.

[89] *U.S. Patent* 4,405,829, accordé le 9/20/83.

[90] RSA, *Miscellaneous* : http://www.rsa.com/rsalabs/faq/faq_misc.html#misc.10.

[91] NIST, *FIPS Publication* 186, 19 May 1994.

[92] UNITED STATES OFFICE OF TECHNOLOGY ASSESSEMENT (OTA), *Information Security and Privacy in Network Environments, Annexe C : Evolution of the Digital Signature Standard*, 15 September 1994 : http://otabbs.ota.gov/E511T93.

[93] NIST, *FIPS Publication* 186, 19 May 1994.

[94] UNITED STATES OFFICE OF TECHNOLOGY ASSESSEMENT (OTA), *Information Security and Privacy in Network Environments, Annexe C : Evolution of the Digital Signature Standard*, 15 September 1994, http://otabbs.ota.gov/E511T93.

[95] US Patent 5, 231,668. Voir T. EL GAMAL, “A public-key cryptosystem and a signature scheme based on discrete logarithms”, dans *IEEE Transactions on Information Theory*, vol. IT-31, 1985, pp. 469-472.

This is thus one of the reasons the process of selecting a signature algorithm has been so arduous. The NIST, while wishing to promote a secure signature algorithm, did not, in contrast, want such an algorithm to be useable for encrypting messages so that the forces of order could not decrypt them[96].

The DSA has had a somewhat lukewarm reception from the private sector. Many would have preferred that RSA be selected as the official standard of the American government[97]. Given the RSA is a *de facto* standard, NIST is criticised for creating confusion among users, software manufacturers and the computer industry in general by introducing the DSA. Moreover, the NIST is reproached for using a secret, arbitrary selection process to decide on the DSA.

Among the other criticisms directed at the DSA, we can underline the one concerning signature verification. While the initial signature function is faster under the DSA, signature verification is more rapid under the RSA. It seems the latter characteristic is more sought after in the industry than is the ability to sign a document quickly[98].

Nevertheless, the strongest criticism of the DSA is related to security. While the original model proposed a 512-bit cryptographic key, the DSS has now authorised the use of cryptographic keys of up to 1024 bits[99]. Still, according to experts in cryptography, the creation of the DSA is too recent and has not been the object of enough studies for users to be able to rely on it[100]. As a general rule, a cryptosystem must be available on the market for several years before inevitable design errors can be identified and suitably corrected. In this sense, some researchers have recently warned DSA users about the existence of "hidden doors" apparently allowing its defences to be pierced more easily[101].

In spite of this, the DSA's future does not seem to be in danger. It is an integral part of the *Capstone* project, for which it constitutes the signature algorithm. However since it is irreversible and does not allow encryption, the DSA has not yet engendered the same enthusiasm as certain other components of this project, such as the *Clipper Chip* and the *Escrow Encryption Standard*, which are dedicated exclusively to message encryption. Also for this reason, the DSA is subject to no restriction on export.

[96] UNITED STATES OFFICE OF TECHNOLOGY ASSESSEMENT (OTA), *Information Security and Privacy in Network Environments, Annexe C : Evolution of the Digital Signature Standard*, 15 September 1994, http://otabbs.ota.gov/E511T93.

[97] See in particular: E. MESSMER, "NIST stumbles on proposal for public-key encryption. Network World", (1992) 9 *Network World* 30; NIST, "The Digital Signature Standard : Proposal and Discussion", (July 1992) 35 *Communications of the ACM* 36-54.

[98] RSA, *Capstone, Clipper and DSS* : http://www.rsa.com/rsalabs/faq/faq_ccd.html#ccd.3.

[99] UNITED STATES OFFICE OF TECHNOLOGY ASSESSEMENT (OTA), *Information Security and Privacy in Network Environments, Annexe C : Evolution of the Digital Signature Standard*, 15 September 1994, http://otabbs.ota.gov/E511T93.

[100] M.E. SMID et D.K. BRANSTAD, "Response to comments on the NIST proposed Digital Signature Standard", dans *Advances Cryptology - Crypto '92*, New York, Springer-Verlag, 1993.

[101] M.E. SMID et D.K. BRANSTAD, "Response to comments on the NIST proposed Digital Signature Standard", dans *Advances Cryptology - Crypto '92*, New York, Springer-Verlag, 1993.

### 4.3.3 The PIN and biometric technologies

There are various mechanisms for electronic signature, aside from the digital signature based on RSA technology and that based on the DSA. The cards and codes presently used in the banking sector are obvious examples of this. As well as restricting access to a network, the personal identification number allows people to be identified.

With respect to electronic signature, several cryptosystems based on mathematical operations – in particular involving the calculation of elliptic curves – have been proposed in recent years[102]. It should also be noted that quantum cryptography, using both mathematics and the properties of light, is proving to be a promising avenue[103]. However these systems do not yet have commercial applications.

This is not the case with biometric technology. The most well known example is that of PenOp™ [104], which operates a biometric signature system to authenticate messages. Contrary to an electronic signature, a biometric signature is produced in the same way as a traditional onee inscribed on a paper document using a pen. However, the paper is replaced by the screen of a computer pen – in other words, a computer with the ability to record text written on a screen using a special pen - or using a digitising tablet on which one can write with a special pen[105]. The digitising tablet captures the movement of the hand signing and reproduces it on screen. Then all that is required is that the signed message be transmitted.

Before using this system, the user must, however, provide a certain number of samples of his or her signature. These are preserved by a signature verification service responsible for checking the authenticity of the signatures that will later be sent by the user[106].

The verification of the authenticity of biometric signatures is performed by the signature verification service through calculation of probabilities[107]. Based on the specific features of the sample signatures, the system evaluates, at the request of the addressee, the percentage of probability that the signature transmitted with the message is authentic. It can, for example, determine the probability that a signature is authentic as 60% or 80%.

[102] N. KOBLITZ, "Elliptic curve cryptosystems", (1987) 48 *Mathematics of Computation* 203; V. S. MILLER, "Use of elliptic curves in cryptography", dans *Advances in Cryptology - Crypto '85*, New York, Springer-Verlag, 1986, 417.

[103] Gilles BRASSARD, *A Bibliography of Quantum Cryptography* : http://www.iro.umontreal.ca/people/ crepeau/Biblio-QC.html.

[104] PenOp™ is a software belonging to *Peripheral Vision Limited.*

[105] James Mc LEAN, "Mécanismes de chiffrement et signature électronique", talk given in Montréal, 10 November 1995, at the conference *L'autoroute de l'information : convergence du droit et de la technologie* (AQDIJ) : http://www.droit.umontreal.ca/AQDIJ/ Colloque_10_11_95/McLean/mclean. html.

[106] James Mc LEAN, "Mécanismes de chiffrement et signature électronique", talk given in Montréal, 10 November 1995, at the conference *L'autoroute de l'information : convergence du droit et de la technologie* (AQDIJ) : http://www.droit.umontreal.ca/AQDIJ/ Colloque_10_11_95/McLean/mclean. html.

[107] James Mc LEAN, "Mécanismes de chiffrement et signature électronique", talk given in Montréal, 10 November 1995, at the conference *L'autoroute de l'information : convergence du droit et de la technologie* (AQDIJ) : http://www.droit.umontreal.ca/AQDIJ/ Colloque_10_11_95/McLean/mclean. html.

Biometric signature technology also uses the irreversible hashing function to ensure the integrity of the message transmitted. As in the case of public key cryptography, this function allows the concise generation of a sequence of data representing the message in question. The result is a concise, secure representation permitting the detection of any alteration to the original.

## 5. Certification authorities and trusted third parties

Use of certification authorities, (also known as certifying third parties or trusted third parties) increasingly seems to be one of the conditions for success for initiatives in electronic commerce. The certification system used by such third parties is intended to reinforce the reliability and security of signature mechanisms based on public key cryptography. Their definition, functions, guarantees of integrity and liability are analysed in this section.

### 5.1 Definition and functions

The ITU-T defines the notion of certification authority as *"an authority charged by one or more users with creating and assigning their public key and certificate"*[108]. The notion of certification authority can be understood only in the framework of a public key, or digital signature.Use of the public key permits verification of a digital signature produced using the corresponding private key. However it must be ensured that such keys really do correspond to the identity claimed by the signature. It is possible to imagine the fraudulent use of a pair of asymmetric keys to create the impression they correspond to the identity of a third party or a fictional person. The use of certificates, issued by a certification authority, allows this difficulty to be offset.

Certification authorities can be public or private. When they are private, they are generally authorised by public authorities to offer such services, and can be established through legislation. In all cases, such private entities can be called upon to perform their duties in cooperation with and under the regulation of one or more hierarchically classed certification authorities. The tip of the pyramid is where we would find the supreme certification authority, probably a government agency.

Finally, certain responsibilities of a certification authority, such as gathering information to appear in certificates, can be performed by a registration authority, as provided, in particular, by the EDIRA project. In this scenario, the supreme authority is generally the registration authority. It is charged with ensuring a formal relation between a person and a pair of asymmetrical keys and with communicating this information to the certification authorities.

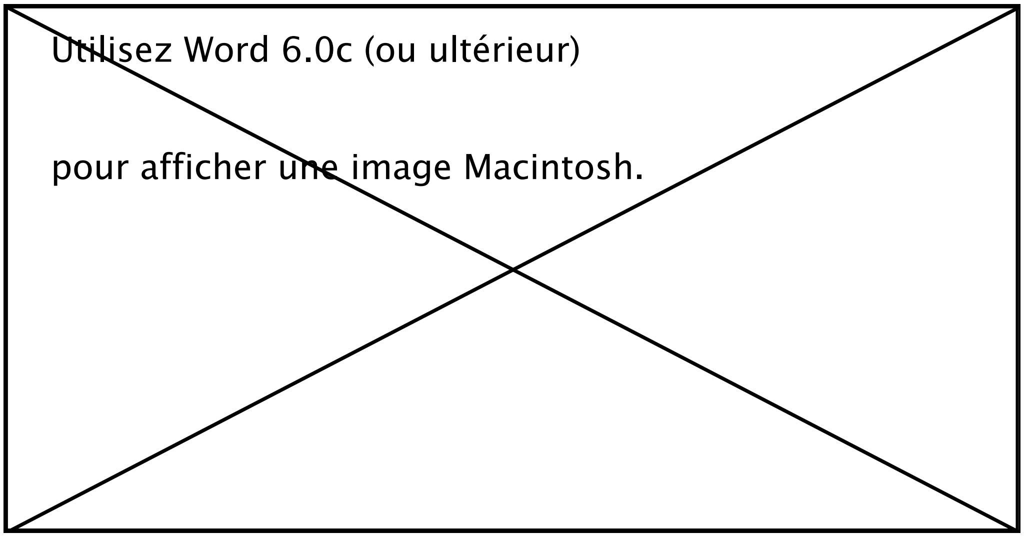
The primary role of a certification authority lies in issuing identification certificates. In addition, it can also accomplish archiving, creation and preservation of asymmetric keys.

[108] UIT-T, Recommandation X.509, Annuaire - Cadre d'authentification, Fasc. VIII.8, 1988, art. 3.3 *c).*

A certificate is an electronic document with the purpose of establishing a relation between a person and a pair of asymmetrical keys. Thus the certificate contains various pieces of information on the identity of the signatory, in particular the public key of that person. It is produced and signed by the certification authority using asymmetrical cryptography and is, by this very fact, protected from alterations. It can be issued, on demand, for any signatory registered with the certification authority. The following example illustrates a possible use of certificates.

Alice transmits a message to Bob along with her signature produced using her private key. She also transmits a digital certificate signed by a certification authority to him. After receiving these documents, Bob first verifies the certificate using the certification authority's public key. If the verification is conclusive, he is assured of the integrity of the information contained in the certificate, in other words of the identity of Alice and her public key. Next he can use Alice's public key so obtained to verify the signature on the message she sent.

*Figure V* Information on the identity of the signatory; Signatory's public key; Information on the identity of the certification authority; Digital signature of the certification authority; Message; Certificate


Utilisez Word 6.0c (ou ultérieur)
pour afficher une image Macintosh.

Since the information contained in a certificate cannot be changed, it can also be published in a directory accessible to all users. Thus Alice would not have to send a certificate with her message. To check the relation between Alice and her message, Bob would have only to consult the certificate directory. This directory would also attest to the fact that the certificate is still in effect and has not been revoked or suspended.

Certificates are generally valid for a period of two years from the date they are issued. They can be suspended or revoked for various reasons, including the death of the signatory, modification of the corporate status of an enterprise, termination of a company's activities, unauthorised disclosure of the private key, or simply on the signatory's request. Moreover, they can generally be suspended or revoked by the certification authority, without the signatory's authorisation, when it is reasonable for the authority to believe that the security of the private key has been compromised or the information contained in the certificate is inaccurate[109].

Under the ITU-T X.509 recommendation, a certificate must contain the: *"public key of a user and certain other information in a form that cannot be falsified..."*[110]. According to the FAST project[111], the "other information" includes the name generally used by the signatory, the distinctive name of the signatory[112]; the unique serial number of the certificate, and the date and time the certificate expires.

### 5.2 Guarantees of integrity and security

In order to perform its duties, the certification authority must present sufficient guarantees of integrity and security. These guarantees entail the minimal presupposition that the certification authority uses a reliable computer system and provides adequate protection for the private key it uses to sign indentification certificates. They also suppose that the certification authority has sufficient financial means to perform its activities and provide compensation if users suffer damages[113].

User confidence in the integrity and security of certification authorities is a *sine qua non* condition for the success of a certification infrastructure. Their integrity and security must not only be known, users must recognise them as having such qualifications. Certification authorities can compete with each other, though their proliferation would make it difficult to monitor these requirements. While it is possible to imagine the existence of fraud in the message signature, this possibility must also be considered in the case of certification. Moreover, in the case of international electronic commerce, effective monitoring of certification authorities is also liable to raise certain difficulties.

The solution to these problems lies in the mutual recognition of certification authorities. Certification authorities should perform their activities in compliance with standards that have received mutual consent.

The supreme certification authorities must meet the highest requirements of independence and integrity. Ideally, they must have an international reputation and certainly the material abilities and necessary expertise to conduct their activities. This is why the establishment of networks of certification authorities acting according to high standards of quality is one of the most promising avenues.

[109] Serge PARISIEN et Pierre TRUDEL, *L'identification et la certification dans le commerce électronique*, Rapport final, Montréal, Centre de recherche en droit public, April 1996, pp. 157 et suiv.

[110] UIT-T, Recommandation X.509, Annuaire - Cadre d'authentification, Fasc. VIII.8, 1988, art. 3.3 *b)*.

[111] COMMISSION EUROPÉENNE, *First Attempt to Secure Trade* (FAST), TEDIS (DG III), section D, p. 8.

[112] COMMISSION EUROPÉENNE, *First Attempt to Secure Trade* (FAST), TEDIS (DG III), section D, p. 1 : "Information which unambiguously distinguishes an entity"; Utah Digital Signature Act, Administrative Rules, Utah Admin. Code R 154-10, art. 101 (2) a) : ""Distinguished name" means data unambiguously identifying the person bearing the name".

[113] Serge PARISIEN and Pierre TRUDEL, *L'identification et la certification dans le commerce électronique*, Rapport final, Montréal, Centre de recherche en droit public, April 1996, p. 178.

### 5.3 Liability

The civil liability incumbent on certification authorities could result from failure to meet security requirements or from negligence in suspending or revoking certificates or identifying signatories. It is clear that if the harm resulting from an error in the identification of a signatory is caused mainly by the bad faith of that signatory, the certification authority's liability will be only subsidiary[114].

## 6.- Civil liability: Who answers for information?

The Internet raises much controversy regarding civil liability. Thus we must study the criteria used to assign liability to the participants in communications occurring on the Internet.

The Internet allows many different communications contexts to be established and the variety of these activities makes it impossible to employ a parallel established with a single traditional means of communication (radio, press, telephone, etc.) to analyse the legal framework of liability[115]. Since the major characteristic of the Internet is its great volatility, depending on the circumstances, the situations that can be encountered there can correspond to various situations that could occur in diverse known communications contexts. Thus the need to consider a plurality of analogies[116].

Metaphors are conceptual tools useful for clarifying the analysis of situations in which we attempt to determine the liability of the various participants in communications taking place in a universe like the Internet. Metaphors[117] can provide clues to the types of relations there are and to the rules that should be applied in various situations[118]. However we must

[114] Serge PARISIEN and Pierre TRUDEL, *L'identification et la certification dans le commerce électronique*, Rapport final, Montréal, Centre de recherche en droit public, April 1996, pp. 177 et suiv.

[115] David R. Johnson and Kevin A. Marks, "Mapping Electronic Data Communications onto Existing legal Metaphors: Should We Let Our Conscience (and Our Contracts) be Our Guide?" (1993) 38 Vill. L. Rev. 487 at 487.

[116] Henry H. Perritt, "Discussion Paper: Metaphors for Understanding Rights and Responsibilities in Network Communities: Print Shops, Barons, Sheriffs and Bureaucracies" Online 15 October 1992, (http:/www.law.vill.edu/ chron/articles/metafin.htm).

[117] This way of borrowing already existing concepts is not new. Metaphors have long been used in the computer domain. For example, program salespersons explain to consumers wondering about the regulations governing program permits that they must treat computer programs as if they were books. See: David R. Johnson and Kevin A. Marks, *supra*, note 1 at 488.

[118] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 488. See also David Loundy, "Whose Standards? Whose Community?" (1 August 1994) Chicago Daily Law Bulletin, 5, (http:/www.leepfrog.com/E-Law/CDLB/AABBS.html).

avoid applying such metaphors mechanically and extending a type of regulation to an electronic environment which is likely to present many paradigm cases and is characterised by rapid changes in roles, functions and technical possibilities[119].

Thus we must provide for an Internet liability regime by recognising the hybrid nature of this environment and by applying in consequence the concepts of liability law, as they have developed to date, while taking into account the various means of communication[120].

### 6.1 Overview of Internet situations generating civil liability

The more the Internet becomes the location of multiple interactions, the more it becomes a theatre of conflict between the participants in the various communications situations it makes possible. Attacks on reputation and on other interests are among the situations for which it is necessary to situate the responsibilities of the participants in Internet communications.

In this respect, Michael McCormack notes that:

> *Unfettered free speech on the Internet is now a thing of the past. [...] Already more than 100 civil actions have been raised for libel in the US after unflattering comments were made in forums, discussion groups, and even on E-mail.*[121]

Yet the Internet is a multi-faceted universe: it is not always easy to evaluate the size of the problems likely to engender liability. As Braithwaite, Carolina and Chance point out, the sizes made familiar to us by traditional media contexts are no longer necessarily the same on the Internet:

> *The inevitable effect of the multimedia revolution is a deluge of information, so users will have to filter inflows, while authors will strive to target their output*

[119] Richard M. Neustadt, Gregg P. Skall and Michael Hammer, "The Regulation of Electronic Publishing" (Summer 1981) 33 Federal Communications Law Journal, 331 at 332.

[120] Eric Schlacter, "Cyberspace, the Free Market and the Free Marketplace of Ideas: Recognising Legal Differences in Computer Bulletin Board Functions" (1993) 16 Hastings Comm/Ent L.J. 87 at 100.

[121] Michael McCormack, "Tell it to the Judge," .net, issue 9, August 1995 at 60.

> *more specifically. A libel juror might reasonably ask how seriously a plaintiff's reputation is harmed by relatively narrowcast bulletin board defamation, in comparison with the widespread damage caused by a broadcast of printed libel. Given the specialised nature of bulletin boards, such scepticism would be misplaced. In the academic community, for example, bulletin boards are often the chosen method of correspondence in certain fields of study. Scurrilous bulletin board messages, even if not widely disseminated by conventional mass media standards, may be nicely targeted to achieve maximum damage to professional or business reputation.*[122]

We shall thus examine the principal situations that generate civil liability on the Internet, and how the regulations applicable to such situations are formulated at present.

### 6.2 Actors and responsibilities

While it is generally easy to accept that the individual who personally accomplished the justiciable action is responsible for the resulting damages, the Internet context raises important questions regarding the responsibilities of those who intervene in the transmission of messages and in the provision of an environment making communications possible.

In order to shed light on the legal situation of these various actors in Internet communications, it is useful to employ metaphors in order to analyse the factors that should be considered in the evaluation of their liability.

The law establishes frameworks for new phenomena using analogies with known situations. Present law already contains a set of principles intended to regulate broadcasting and the exchange of information. The goal of legal research is to identify precisely how these principles apply to novel situations. This task is often made easier through the use of metaphors, such as that of a highway, which allow the identification of analogies and possible legal regimes[123].

In many situations in which damage results from information circulation, the criteria for assigning liability

[122] Nick Braithwaite, Robert Carolina, Clifford Chance, "Multimedia Defamation" International Media Law, March 1994 at 19.

[123] David R. Johnson and Kevin Marks, *supra*, note 1 at 487; Henry H. Perritt Jr., *supra*, note 2.

take into account the roles assumed by the various participants in the process of the assignment of value to information. Thus it is asked who played the role of a publisher, a simple carrier, a broadcaster, a newspaper, etc., for the duties and responsibilities linked to each of these roles are well established in liability law.

Thus by extrapolating both from the characteristics which are presented by the various communications contexts found on the Internet and from the analogies demonstrated by the roles and functions of the various actors, it is possible to get a bearing on liability law resulting from the transmission of information on the Internet.

We will note that there is a close link between the control exercised over information presumed harmful and the liability which follows from it. Thus, the greater the discretion to make decisions on what is to be published (transmitted), the greater the liability implied by such decisions[124].

With respect to the circulation of information, three sorts of roles are assumed in the Internet, each of which has variations and combinations entailing that in certain situations a single entity may assume more than one role. In any case, in open network environments, there are invariably system operators, information providers, among which there are users and one or more information carriers. What magnifies the impression of a so-called "legal vacuum" regarding the Internet is the absence of consensus on the metaphors which should aid in situating the roles of the participants in electronic communications and, in many respects, the inability of each of the metaphors to portray the roles which are effectively performed in computer communications.

### 6.2.1 The publisher

A publisher publishes information. To publish means to communicate information to third parties knowing that the information will be read, seen or heard. Voluntary publication supposes knowledge of the content of the

[124] Joseph P. Thornton, Gary G. Gerlach and Richard L. Gibson, "Libel (Symposium: Legal Issues in Electronic Publishing)" (Sept. 1984) 36 Federal Communications Law Journal 178-181.

information transmitted[125]. In the Internet context, publication can result from the transmission of files, from discussion in the framework of electronic conferences, or from making available information in files that can be transferred through the network[126].

In all of these situations, there is one constant: the decision to publish belongs to the publisher. For this actor, this is an option: there is no obligation to publish. In the world of the press and publishing, it is normal to hold that the director of publishing is able to control the information that circulates due to his or her enterprise[127]. From such controlling power follows liability for the transmission of harmful information.

However, as some authors have remarked, it is doubtful whether this presumption is always verifiable on the Internet, especially in situations in which there is no "fixing prior to the communication to the public", which is the only way for a site operator to exercise any control[128].

This is a limitation on this metaphor regarding electronic environments because to ask site operators to effectively supervise the content of everything they transmit to the public supposes a considerable burden[129]. This leads to attention being removed from the intention to broadcast and placed on the intention to communicate a message *of which the site operator should have known* the harmful nature[130].

In *Stratton Oakmont Inc.* v. *Prodigy Services Co.*[131] the court concluded that the Prodigy network had assumed the role of a publisher. A subscriber to Prodigy had sent a defamatory

[125] Loftus E. Becker, Jr., "The Liability of Computer Bulletin Board Operators for Defamation Posted by Others" (Fall 1989) 22 Connecticut Law Review, 203 at 217.

[126] Timothy Arnold-Moore, "Legal Pitfalls in Cyberspace: Defamation on Computer Networks" (1994) 5(2) Journal of Law and Information Science 165 at 178. (http://www.kbs.citri.edu. au/law/defame.html).

[127] David R. Johnson and Kevin A. Marks, *supra*, note 1, at 492.

[128] X. Linant de Bellefonds and A. Hollande, *Droit de l'informatique et de la télématique*, (Paris: J. Delmas et Cie, 1990) at 131.

[129] David R. Johnson and Kevin A. Marks, *supra*, note 1, at 492. See also Edward A. Cavazos, "Computer Bulletin Board Systems and the Right of Reply: Redefining Defamation Liability for a new Technology" (Fall 1992) 12 Review of Litigation 231 at 238.

[130] Jay R. McDaniel, *supra*, note 109 at 817-818.

[131] Index No. 31063/94, N.Y. Sup. Ct., 24 May 1995.

message concerning the President of Stratton onto the network. The court held Prodigy responsible for the damage caused.

In order to decide to call Prodigy a publisher, the court examined the behaviour of the site operator with respect to information carried. In this case Prodigy exercised a degree of control over the information: it was reputed to answer for the information it transmitted because it was supposed to be aware of the content[132].

From this decision, many concluded that when a site operator claims to offer a service free of "vices", adopts a code of conduct, pays employees to ensure such a code is respected, and provides an arbitrator for cases of conflict regarding certain statements, then the site operator makes itself liable for the content carried by its services. By assuming the same control as that of a publisher, the site operator also takes on the same liability[133]. Against such a conclusion, some have argued that by declaring the service to be a "family" service, Prodigy played the role of a bookseller which chooses the type of literature it wishes to sell, but that such choice does not make it a publisher[134].

Nonetheless it remains that editorial control is recognised when a participant in electronic communications[135]:

- examines messages and exercises control over their contents before they are transmitted;

- deletes messages or actions of users which do not fulfil the criteria he or she has determined.

It is appropriate however to distinguish cases in which the site operator, in order to prevent a discussion group from overflowing out of the theme it is assigned, does not allow certain off-topic messages. The site operator is then not automatically considered to be a publisher due to the simple fact that it exercises such control since its action does not

[132] David Loundy, "Holding the Line, On-Line, Expands Liability" (8 June 1995) Chicago Daily Law Bulletin at 6.

[133] *Ibid*.

[134] Eugene Volokh, cyberia-1@listserv.cc.wm.edu, 11/07/95, 21:46, FYI, re: Stratton Oakmont v. Prodigy.

[135] Eric Schlachter, *supra*, note 6 at 135.

target editorial control over the content so much as it does a certain zoning in the network[136].

### 6.2.2 The broadcaster

When they are free to broadcast, broadcasters are generally considered to be the publishers of the statements they transmit and thus to have the same standards of liability as the latter. The written press, the radio and TV are subject to the provisions of the principles of civil liability except if the dispositions of a statutory exception suspend or modify their application.

Broadcaster liability can result from harmful statements made by members of the public acting in their own names. In this respect, the general rule governing broadcaster liability remains the same if it can be proven that all measures to prevent harmful statements had been taken[137]. In this respect, a Canadian court has refused to apply the American doctrine of the "outside speaker" which makes the broadcaster responsible for the statements of an "outside guest speaker" except in so far as evidence is established that the broadcaster was negligent[138].

The rule which applies in Québec is similar to that which is advocated by a certain current in French jurisprudence, which holds that in spite of the fact that the broadcaster's liability cannot result directly from the statements of a member of the public which are transmitted "live", it does result from the "authorisation" to speak which the broadcaster accords that person[139]. However the Paris Appeal Court asserted that a broadcaster is liable for the statements of a member of the public which are transmitted "live" only if the

[136] *Ibid.* [Since all users have the opportunity to post messages as they wish, many discussion groups can easily become invaded by "junk postings" if the "sysop" does not withdraw unrelated messages.]; Henry H. Perritt Jr., "Tort Liability, the First Amendment and Equal Access to Electronic Networks" (1992) 5 Harvard Journal of Law & Technology 65 at 140. [A network could not survive if every single individual could publish whatever he or she desired and evaluate the content of his or her messages in accordance with his or her own system of values.]; Edward A. Cavazos, "Computer Bulletin Board Systems and the Right of Reply: Redefining Defamation Liability for a New Technology" (Fall 1992) 12 Review of Litigation 231 at 239. [A discussion group which addresses itself to children should not contain messages "for adults only".]

[137] Pierre Trudel and France Abran, *Droit de la radio et de la télévision* (Montréal: Thémis, 1991) at 464.

[138] *Lawson* v. *Burns, Succamore and Jim Pattison Broadcasting Ltd*, [1976] 6 W.W.R. 362 (B.C.S.C.).

[139] *Affaire Polac*, Trib. gr. inst. de Paris, 29 January 1986, flash, no. 10.

broadcaster endorses them or if the statements are made with the broadcaster's connivance[140].

In certain circumstances, while they may be participants in the publication process, broadcasters may not be able to intervene in the content of the information broadcast. For example, press operators (for a newspaper), couriers which carry the publication and radio or television engineers have no control over content[141]. In general the secondary publisher does not know the content of the information he or she carries and is thus not able to prevent harmful statements from circulating.

The standard of liability thus applied resembles that generally attributable to a carrier, in other words, the case in which there is no liability for the harmful content of the messages transmitted[142]. Moreover, some advocate a presumption that secondary publishers are ignorant of the harmful content of the information. [143]However, the secondary publisher is liable if he or she knew or had reason to know of the defamatory nature of the message transmitted[144]. In such a case, the secondary publisher then becomes a kind of re-broadcaster and acquires the same liability as the latter[145].

### 6.2.3 Re-broadcasters

A re-broadcaster circulates material *published by others*[146]. A re-broadcaster's liability is largely determined by the existence of possibilities of verifying the content of the information broadcast.

[140] Paris, 1st Ch. Sect. A, 6 October 1987.

[141] David J. Loundy, "E-law: Legal Issues Affecting Computer Information Systems and Systems Operator Liability" Online 1995 (http"//www.leepfrog.com/E-Law/Contents.html).

[142] Robert Charles, "Computer Bulletin Boards and Defamation: Who Should be Liable? Under What Standard?" (1987) 2 J.L. & Tech. 121 at 131; David J. Loundy, *supra*, note 18.

[143] Robert Charles, "Computer Bulletin Boards and Defamation: Who Should be Liable? Under What Standard?" (1987) 2 J.L. & Tech, 421 at 131; David J. Loundy, "E-Law: Legal Issues Affecting Computer Information Systems and Systems Operator Liability" Online 1995 (http://www.leepfrog.com/E-Law/E-Law/Contents.html).

[144] *Lerman* v. *Chuckleberry Pub. Inc.*, 521 F. Supp. 228, 235 (S.D.N.Y. 1981).

[145] David J. Loundy, *supra*, note 143.

[146] Eric C. Jensen, "An Electronic Soapbox: Computer Bulletin Boards and the First Amendment" (1987) 39 Federal Communications Law Journal 217; Joseph P. Thornton, Gary G. Gerlach and Richard L. Gibson, *supra*, note 126 at 179.

In principle, individuals who re-circulate harmful information are liable in the same way they would have been if they themselves had written or published it in the first place. Thus, a radio or television station which only broadcasts the statements of a third party and a newspaper which reprints what has been said or written by others are considered to be the primary publishers of such statements and are thus liable for them[147]. A broadcaster which re-circulates defamatory statements, regardless of the source of such statements, even if it is a news agency which the journalist believed to be reliable, is liable for them: it cannot be exonerated[148]. In such situations, it is possible to check the information, or at least to be aware of its possibly harmful nature.

### 6.2.4 The librarian

The category of distributor is distinct from that of re-broadcaster. Librarians, like booksellers, are information distributors. In other words, they deliver or provide information whereas a re-broadcaster repeats it[149].

Normally, distributors do not control the content of the information they transmit and are not liable if it is harmful[150]. In effect it would be unthinkable for each distributor (newsstand, bookstore, library) to have the duty to check the contents of each publication distributed in order to be sure that it contains no harmful information[151].

However, when they are made aware of the harmful nature of information, distributors have the duty to withdraw it. If

[147] Joseph P. Thornton, Gary G. Gerlach and Richard L. Gibson, *supra*, note 126 at 179; *Cianci* v. *New Times Publishing Co.*, 639 F.2d 54, 61 (2d Cir.1980); *Lerman* v. *Chuckleberry Publishing Co.*, 521 F. Supp. 228, 2335 9S.D.N.Y. 1981); *Macaluso* v. *Mondadori Publishing Co.*, 527 F.Supp. 1017, 1019 (E.D.N.Y. 1981).

[148] *Chinese Cultural Centre of Vancouver* v. *Holt* (1978), 7 B.C.L.R. 81 (S.C.).

[149] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 493.

[150] Trotter Hardy, "The Proper Legal Regime for "Cyberspace" (1994) 55 University of Pittsburgh Law Review, 993 at 1003; David R. Johnson and Kevin A. Marks, *supra*, note 1 at 493.

[151] *Balabanoff* v. *Fossani*, 81 N.Y.S.2d 732, 733 (Sup. Ct. 1948). American jurisprudence even considers that a law which would impose strict liability on a distributor, for example on a librarian, for the content of the works he or she distributes would be unconstitutional because it would have the effect of indirectly restricting information transmitted to the public (since the works available would be only those inspected by the librarian). See: *Smith* v. *California*, 361 U.S. 147 (1959), reh'g denied, 361 U.S.; Trotter Hardy, *supra*, note 152 at 1003.

they do not do so, they can be held liable for the damage caused by such statements[152].

The problem with electronic environments is that the majority of site operators participate in their own systems (without, nonetheless, exercising real control over all the information circulating in it). Such participation could be interpreted, according to some authors, as implying real or presumed knowledge of the harmful nature of the information contained in the system. The site operator who has been informed of the harmful nature of the information would have the obligation to take all necessary measures to prevent the circulation of or to withdraw the information, or else he or she could be held responsible for the harm caused by such information[153]. However the site operator's liability would be tempered by the requirement of being attentive to the problematic nature of the information found in a site partially or wholly under its control.

In the *Cubby* case, an electronic message distributed in CompuServe contained unflattering remarks about a rival server (Cubby). The court concluded that CompuServe had no control over the information circulating in its system and that it could not know or have reason to know of the harmful nature of the messages. It was thus not liable. The court compared CompuServe to an electronic library. Like a library, CompuServe had the choice of circulating a work or not, but once the work was in the system it could exercise no editorial control over it. Moreover, even if CompuServe had wanted to examine each message, the extremely large number of messages would have made such action impossible[154].

According to some, the analysis performed in the Cubby case seems to imply that in order to avoid liability, all the site operator has to do is close its eyes to the information circulating in its network[155]. A site operator which knew or should have known that harmful information was being carried in its network and which exercised no control over such information would then become a kind of re-broadcaster and

[152] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 493; David J. Loundy, *supra*, note 143.

[153] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 494.

[154] *Cubby* v. *CompuServe Inc.*, 776 F.Supp. 135 (S.D.N.Y. 1991) at 140.

[155] Edward A. Cavazos, "Computer Bulletin Board Systems and the Right of Reply: Redefining Defamation Liability for a New Technology" (Fall 1992) 12 Review of Litigation 231 at 242.

acquire the same liability as the latter[156]. This would require, however, the participation of users who would have to inform the system operator of the existence of information they consider potentially harmful.

Some claim however that, even if they are considered to be like libraries, "sysops" operating less busy systems would have the duty to examine messages since there is the possibility, in an electronic environment, of performing an automatic computer search of words or expressions likely to be harmful (whereas a library in the real world would have to perform such a search manually)[157].

In electronic environments, information storage is not necessarily done by large, easily identifiable storefront publishing companies. Presently, the fact that a librarian or bookseller is not liable for what he or she distributes has little effect on the victim since he or she will attack the publisher of the document directly. In electronic environments, what would happen if the system operator was not liable and the publisher was unknown or insolvent?[158]

Yet, the system operator often lacks a legitimate motive to intervene in order to suppress potentially harmful information. In the name of what and in virtue of what authority must a system operator decide whether a given piece of information is actionable or not? In virtue of what authority should it assume the role of a tribunal charged with determining is the content is harmless or harmful?

### 6.2.5 The retransmitter

Programming distributed by broadcasting distribution companies does not originate with those companies. It is received and then transmitted. Thus, direct satellite-to-home broadcasting systems are considered to be like broadcasting distribution companies when the operator acts as a re-transmitter of existing signals. The operator does not produce or order programs and does not modify the content of the programs on any of the signals distributed. Such programs can be distributed either coded or uncoded. Multipoint distribution systems are also included in the category of broadcasting distribution companies insofar as the operator

[156] David J. Loundy, *supra*, note 143.

[157] Trotter Hardy, *supra*, note 152 at 1003 (Trotter Hardy agrees however that it is almost impossible to determine "harmful words".)

[158] Trotter Hardy, *supra*, note 152 at 1005.

neither produces nor orders programs and does not modify the content of the programs on any of the signals distributed[159].

In such situations, re-transmitters cannot be assigned liability for the content thus re-transmitted.

### 6.2.6 The owner of a space

Some have argued that electronic communications sometimes require the use of an individual's property[160]. This leads to the consideration that certain participants sometimes find that presumably harmful information is located in a space they own.

Owners are rarely held liable for acts committed on their property. Timothy C. May compares some system operators to hotels that rent rooms (electronic spaces) to users and which have no obligation, or right, to supervise what the latter do there. They thus have no liability if illegal activities occur there.

This line of argument corresponds to the rule established in Québec jurisprudence that states that a landlord is not necessarily responsible for the misdeeds of his or her tenants[161]. Obviously, a hotel which, with complete awareness, makes itself the centre of illegal activities is liable for damages, as would be a site owner who endorsed defamatory messages transmitted by users[162].

Moreover, it is recognised that an owner who is informed of the presence of harmful statements on the walls of his or her property and who does nothing to remove them, is considered to be a re-broadcaster of those statements and is liable for them to the same extent as the author of the message[163]. Likewise, site operators would always have the duty

[159] CRTC, Public Notice 1987-254 (26 November 1987), Politique de réglementation des systèmes de radiodiffusion directe (SRD) du satellite au foyer, des systèmes de distribution multipoint (SDM) et des entreprises de télévision par abonnement (TPA).

[160] Timothy C. May, "Who is Responsible on the Net" law.listserv.cyberia-l, (Subject: Cyberspace is more like property, lease space, rent, etc.) 7 February 1995 12:31:21.

[161] *Bissonnette* v. *Corriveau* [1992] A.Q. 2005; *Bissonnette* v. *Boulet* [1992] A.Q. 2004.

[162] Timothy C. May, *supra*, note 37.

[163] *Hellar* v. *Bianco* 11 Cal. App. 2d 424, 244 P.2d 757, 28 ALR2d 451 (1952); *Scott* v. *Hull*, 22 Ohio App.2d 141, 259 N.E.2d 160, (1970); *Tackett* v. *General Motors Corporation*, 836 F.2d 1042 (7th Cir. 1987); *Woodling* v. *Knickerbocker*, 17 N.W. 387 (Minn. 1883).

to withdraw information they know to be harmful if they do not want to be assigned liability as re-broadcasters[164]. According to this metaphor, the prerequisite to liability would be the knowledge of the presence of harmful information in a site[165].

### 6.2.7 The Carrier

Like a carrier, an electronic communications system sometimes acts only as a channel for transporting information from one site to another[166]. Carriers are in principle freed of liability for the content of statements they carry for their users[167]. Contrary to publishers and distributors, carriers have the obligation to carry any message and may discriminate neither against the content of the message nor against the person who sends it[168].

Nonetheless a carrier, like a telecommunications company, can be held liable for the content it carries if it is itself the author of the statements: its situation would be that of a publisher. Generally, it acquires no responsibility for content which originates with third parties and circulates on its lines since it is then simply a channel[169]. The Ontario Supreme Court judged that in effect it would be unthinkable for each employee of a telegraph company to be responsible for checking each message and for deciding if the content is harmful or not[170].

However, common law recognises that carriers must provide evidence of reasonable diligence in the transmission of messages. Among carriers, telegraph companies are the most likely to be held liable for the content of the messages they transmit. This results from their common law obligation to

[164] Eric Schlachter, *supra*, note 6 at 118.

[165] Jay R. McDaniel, *supra*, note 109 at 825.

[166] David J. Loundy, *supra*, note 143.

[167] Michael H. Ryan, *supra*, note 13 at 416; Lynn Becker, "Electronic Publishing; First Amendment Issues in the Twenty-First Century" (1984-85) 13 Fordham Urban Law Journal, 801 at 857.

[168] David R. Johnson and Kevin A, Marks, *supra*, note 1 at 495; Terri A. Cutrera, *supra*, note 144 at 555; *Chastain* v. *British Columbia Hydro & Power Authority* [1973] 2 W.W.R. 481; *Telecommunications Act*, S.C. 1993, c. 38, s.36: "Except where the Commission approves otherwise, a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public."

[169] Floyd Abrams and Dean Ringel, "Content Regulation (Symposium: Legal Issues in Electronic Publishing" (Sept. 1984) 36 Federal Communications Law Journal 153.

[170] *Kahn* v. *Great Northwestern Telegraph Co. of Canada* (1930) 39 O.W.N. 143 (C.A.).

transmit messages with reasonable diligence[171], but its origin lies primarily in the fact that since the message must go through the hands of an employee of the company before being transmitted, the control over the content is greater than when, for example, a message is transmitted using a telephone.

The Supreme Court of Canada distinguishes between messages intended to be published (for example, letters and news for newspapers) from purely personal messages. The Court holds telegraph companies liable for the content of messages intended to be published since in such cases it considers the telegraph company to be like a publisher[172]. Others go so far as to believe that there is a presumption that the defamatory statements contained in a telegraph were published through their transmission[173]. According to this reasoning, the telegraph company would be presumed at all times to be playing the role of a publisher and, unless there is proof to the contrary, would be liable for damages. Against this line of thought, some hold that the transmission of messages by carriers never amounts to a publication of the statements and that carriers never have more than a right to limited control over messages[174].

Unlike telegraph companies, telephone companies have never been held responsible for the content of the messages they carry since according to some they do not "transmit" messages[175]. The person speaking is the one who truly transmits the message and he or she is liable for the content[176].

The situation is however different for messages which are recorded and then transmitted by a telephone company (voice Mail). In the U.S., the court states that even if a telephone company could be held responsible for having "published" such messages, such a company should be granted a privilege and be relieved of its liability[177]. American jurisprudence thus grants extensive immunity to telephone companies[178].

[171] Jay R. McDaniel, *supra*, note 109 at 789.

[172] *Dominion Telegraph Co.* v. *Silver* (1882) 10 S.C.R. 238.

[173] *Pavlovic* v. *Knutson* (30 June 1982) Doc. No. 137/1981 (Sask. Q.B.).

[174] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 495.

[175] Michael H. Ryan, *supra*, note 13 at 416; Bell Canada's Terms of Service, s. 16 (approved by the CRTC) states: "Bell n'est pas responsable pour la diffamation [...] transmise ou reçue par le biais de ses services".

[176] *Electric Despath Co.* v. *Bell Telephone Co.* (1891) 20 S.C.R. 83.

[177] *Anderson* v. *New York Telephone Company*, 320 N.E.2d 647 (N.Y. Ct. App. 1973).

[178] Jay R. McDaniel, *supra*, note 109 at 822.

Some believe[179] that comparing electronic environments to actual carriers is not appropriate because of the carriers' obligation to transmit information without discrimination. In *Cubby* v. *CompuServe*[180], the CompuServe network was sued as a co-defendant in a defamation case. This recourse resulted from information published in an electronic news letter entitled: "Rumorville USA". This news letter was published by a network subscriber who had no other link with CompuServe. Leisure J. exonerated CompuServe, noting that in this case CompuServe did not have the possibility of becoming aware of the information broadcast. The company received no fees for providing public access to the incriminated electronic site, just as it paid no fees to broadcast that site to its subscribers.

In so far as CompuServe could not be aware of the harmful nature of the information transmitted, it assumed no liability in that respect.

From this analysis one might infer that it is incumbent on the network to do whatever is necessary to withdraw information when it becomes aware of its harmful nature. Such an approach tends to lead to the conclusion that the degree of responsibility of the network administrator is closely linked to the degree of control it exercises or is supposed to exercise over the information transmitted or otherwise available on its network.

This demonstrates the crucial importance of qualifying the role played by information providers. Thus, in *Stratton Oakmont* v. *Prodigy*[181], an investment firm sued Prodigy following defamatory statements transmitted on an electronic site broadcast by Prodigy. The court decided that Prodigy exercised some degree of control over the content and ruled in consequence.

In order to define the liability assumed by electronic sites, we must ask what degree of control the site operator has over the information found in the site. If we refer back to the criteria stated in the *Cubby* decision, the level of control or supervision exercised by the electronic bulletin board operator would be determining. In truth, it is

[179] Edward A. Cavazos, *supra*, note 157 at 239.

[180] *Cubby* v. *CompuServe Inc.* (1991) 776 F. Supp., 135; See also: Anthony J. Sassan, "Comparing Apples to Oranges: The Need for a New Media Classification (Case Note) *Cubby* v. *CompuServe Inc.* 776 F. Supp. 135 (S.D.N.Y. 1991)" (1992) 5 Software Law Journal 821.

[181] http://www.eff.org/pub/Legal/Cases/Stratton_Oakmont_Porush _v_Prodigy/stratton-oakmont_porush_v_prodigy_et_al.decision

difficult to exclude the liability of the site operator when it has deciding power over the posting of messages. This scale allows us to determine the level of liability incumbent on those responsible for sites open to the general public and sites reserved for closed groups. Their liability is closely related to the degree of control they exercise over the posting or making available of information.

### 6.3 Relations between liability and control exercised over information

In order to determine the liability of an actor who transmits the same information to many users at the same time, we must examine the relation such an actor has with the content of the message transmitted[182].

The goal and the scope of the rights and responsibilities of the various actors in electronic communications do not depend so much on the official roles of such actors as they do on the degree of control such actors exercise, or are supposed to exercise, over the information and communications found in open networks or in the part of such networks over which they have some control. The assignment of liability to an entity presupposes the possibility of identifying the actors who control the information in the various spaces within such a virtual environment[183].

Perritt notes that the criterion of control over information plays a major role in the assignment of liability:

> *In all three categories of tort liability (defamation, copyright infringement and invasion of privacy), the requisite fault cannot be proven without showing either that the actor and potential tort feasor exercised some actual control over content or that it was feasible for it to control content and that it could foresee the possibility of harm if it did not control content.*[184]

Regarding this, Eric Schlachter writes:

> *There is a sliding scale of control in relation to forced access. At one end of the scale are primary publishers,*

[182] Jay R. McDaniel, *supra*, note 109 at 823.

[183] See Pierre Trudel, "La protection des droits et des valeurs dans la gestion des réseaux ouverts" in CRDP, *Les autoroutes électroniques: usages, droit et promesses* (Montréal: Éditions Yvon Blais, 1995) at 324-325.

[184] Henry H. Perritt Jr., *supra*, note 138 at 110-111.

> *who have virtually unrestrained discretion over what they print or to whom they give access to disseminate information. Also on this end are owners of private property, who are similarly protected from mandatory or forced access. [...] At the other end of the sliding scale from primary publishers are common carriers who by definition must be available to all comers and cannot refuse to provide service in a discriminatory fashion.*[185]

This sliding scale concerns not only rights to access to electronic environments: it fully applies in the domain of liability. Schlacter points out that "Those entities with more editorial control generally also have greater exposure to tort liability for the statements or actions of others."[186] Thus, it is possible to determine the degree of liability from the degree of control a person effectively exercises over information in a given situation.

Editorial discretion, which is exercised Mainly in traditional areas by an editor or broadcaster, guarantees freedom of editorial choices and that of the selection of information to be published[187].

Editorial liability does not take into account the intention to communicate a damaging message. What counts is the intention to communicate a message, the harmful nature of which should have been known by the editor[188]. Thus the editor is generally considered to be able to control the set of information which circulates in his or her enterprise[189], and such an editor answers for damages, whether the actionable statements come from an employee, an open letter to the editor, or advertising[190]. This power of control is what entails liability for the transmission of possibly illegal or harmful information[191]. The corollary is that those who play only a subordinate or minor role in the process leading up to

[185] Eric Schlacter, *supra*, note 6 at 113 ff.

[186] Ibid.

[187] Susan D. Charkes, "Editorial Discretion of State Public Broadcasting Licensees" (1982) 82 Columbia L. Rev. 1161, 1172.

[188] Jay R. McDaniel, *supra*, note 109 at 817-818.

[189] Raymond E. Brown, *The Law of Defamation in Canada*, Second Edition (Toronto: Carswell, 1994) at 1219; David R. Johnson and Kevin A. Marks, *supra*, note 1 at 492; Robert Beall, "Notes: Developing a Coherent Approach to the Regulation of Computer Bulletin Boards" (1987) 7 Computer/Law Journal, 499 at 505.

[190] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 492.

[191] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 492.

publication incur liability only if their negligence is clearly demonstrated[192].

The exercise of editorial discretion and its consequences on the level of assignment of liability were discussed in *Cubby*. An electronic message distributed on CompuServe contained unflattering remarks about a rival (Cubby). The court ruled that "Compuserve has *no more control* over such a publication than does a library, book store or newsstand"[193]: the information, established by an independent third party, was entered directly into the system to provide immediate access to users. For this reason, and because the extremely elevated number of messages in the system made it impossible to examine them[194], the court concluded that CompuServe could not know, or have a reason to know, of the harmful nature of the messages. CompuServe was thus not liable for them.

According to Eric Schlacter, it is important to interpret the law in a manner which takes into account new information technologies. To this end, a relation between the degree of editorial control and liability can be recognised.

A system operator or any other actor can, depending on innumerable possible circumstances, have different degrees of control over information[195].

### 6.3.1 Effective physical control and information longevity

Effective physical control is exercised by a person who, knowing that he or she is participating in the broadcast of a potentially damaging message, has the possibility of withdrawing such a message and ending its circulation not by exercising editorial control over the content, but by withdrawing the material support of the content or the entire "work"[196]. That such a factor should be considered when liability is to be assigned is simply common sense: "on ne peut imputer à un individu la responsabilité d'un acte imprévisible et inévitable sur lequel il n'avait aucun pouvoir

[192] Raymond E. Brown, *supra*, note 197 at 1220; *Weldon* v. *"The Times" Book Co.* (1911) 28 T.L.R. 143 (C.A.).

[193] *Cubby Inc.* v. *CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991) at 140.

[194] *Cubby Inc.* v. *CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991) at 140.

[195] Eric Schlacter, "Electronic Networks and Computer Bulletin Boards: Developing a Legal Regime to Fit the Technology", http://www.seamless.com/eric/eric-1.html.

[196] Here "work" refers to the complete set of information considered as a whole.

d'intervention."[197] In contrast, the courts demonstrate a natural tendency to assign liability to those who were reasonably capable of acting to prevent the damage.

Many examples taken from traditional communications contexts (press, radio, television, printed publication) show that the possibility of exercising effective control over the medium used to circulate information can be one of the factors in assigning liability if the actor in question did not take the precautions available to remedy the damage after its initial publication or broadcast.

One such example can be found in the regime applied to secondary publishers. Secondary publishers are persons who participate in the publication process, but in a limited manner. A secondary publisher is liable if it knows or had a reason to know of the defamatory nature of the message transmitted[198]. Likewise, jurisprudence considers that a printer cannot be held responsible for the defamatory content of works written by its clients since it does not have the duty to revise the content of the works it prints and it is presumed to not know their content[199].

A similar regime is applied to the re-broadcaster, in other words some one who circulates or sells material *published by others*[200]. The status which best illustrates the possibility of performing this sort of control is that of an information distributor. A librarian, like a bookseller, distributes information. In other words, he or she delivers or circulates information - while a re-broadcaster repeats it[201]. Normally, a distributor does not control the content of the information it transmits and thus has no liability if it is damaging[202]. It would in effect be unthinkable for each distributor (newspaper vendor, bookstore, library) to have the duty to verify the content of each publication it distributes in order to ensure that it contains no harmful information[203].

[197] Nicole Vallières and Florian Sauvageau, *supra*, note 73 at 25-26.

[198] *Lerman* v. *Chuckleberry Pub. Inc.*, 521 F. Supp. 228, 235 (S.D.N.Y. 1981); David J. Loundy, *supra*, note 143.

[199] *Mainard* v. *Port Publications Inc.*, 297 N.W.2d 500 (Wis 1980).

[200] Eric C. Jensen, *supra*, note 148; Joseph P. Thornton, Gary G. Gerlach and Richard L. Gibson, *supra*, note 26 at 179.

[201] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 493.

[202] Trotter Hardy, *supra*, note 152 at 1003; David R. Johnson and Kevin A. Marks, *supra*, note 1 at 493.

[203] *Balabanoff* v. *Fossani*, 81 N.Y.S.2d 732, 733 (Sup. Ct. 1948).

However, since the distributor has physical control over the material published, it has the duty to make reasonable inquiries into the accuracy of statements when it is informed that they are potentially harmful[204]. If such inquiries lead it to the conclusion that the statements in question could indeed by harmful, it has the obligation to withdraw them from circulation. While the distributor does not have an editor's control over the content of a book, it always retains the ability to remove a book from the book store shelves. If the distributor fails to do so, it may be held liable for the damages caused by the statements[205].

In the *Cubby* decision, the judge applied the standard of distributor to CompuServe: it was held liable if it "knew or should have known":

> *the inconsistent application of a lower standard of liability to an electronic distributor such as CompuServe, than that which is applied to a public library, book store or newsstand, would impose an undue burden on the free flow of information.*[206]

Because of the speed of information transmission, and the great number of transmissions, CompuServe could exercise no physical control except at the level of the complete work. While CompuServe has the choice whether to circulate a work, once a work is in its system, it can exercise no editorial control over it[207]. Since it was not established whether CompuServe "knew or should have known" that the publication in question contained harmful information, no liability was assigned to it.

The longevity of the information, like the effective control of it, has a direct influence on the possibility of exercising control. In effect, liability will not be evaluated in the same way when the information is stable and when it continually varies. Variable information changes regularly, sometimes every few seconds (for example, financial data), and

[204] Henry H. Perritt Jr., *supra*, note 38 at 106.

[205] David R. Johnson and Kevin A. Marks, *supra*, note 1 at 493; David J. Loundy, *supra*, note 143.

[206] *Cubby Inc.* v. *CompuServe Inc.*, 776 F.Supp. 135 (S.D.N.Y. 1991) at 140.

[207] "While CompuServe may decline to carry a given publication altogether, in reality, once it does decide to carry a publication, it will have little or no editorial control over that publication's contents. This is especially so when CompuServe carried the publication as part of a forum that is managed by a company unrelated to CompuServe": *Cubby Inc.* v. *CompuServe Inc.*, 776 /f.Supp. 135 (S.D.N.Y. 1991) at 140.

thus it is not only virtually impossible to revise its content as it is transmitted for use, or to provide remedies if such information is false or inaccurate[208], there is greater difficulty in stopping its circulation before damage is suffered.

In contrast, information that remains relatively stable is much more amenable to control. Moreover, the user is much more justified in relying on such information because its stability implies that the provider has taken the trouble to confirm its accuracy[209].

Perritt nonetheless emphasises that the possibility of exercising such physical control does not result uniquely from technological factors:

> *The victim would prefer a rule that would allow a defendant to avoid tort liability only in situations in which content control is technologically infeasible. Unfeasibility, however, is a concept with an economic dimension. Determining what is feasible requires balancing of risks and benefits.*[210]

This is why we necessarily find ourselves back at the issue of knowledge of the harmful nature of the information.

### 6.3.2 Relations between liability and knowledge of information

Knowledge of the harmful nature of a piece of information is strictly linked to many factors in the assignment of liability. This is why they are dealt with, in certain instances, concurrently. The knowledge issue does not usually come up in editorial contexts in which knowledge of the harmful nature of the information is accompanied by a presumption of knowledge inherent to the exercise of editorial discretion: faith in editorial decisions in no way tempers the entailed liability[211]. To publish is to communicate information to third parties knowing that such information will be read, seen or heard. As a result of the exercise of editorial

[208] Joseph J. Tiano Jr., "The Liability of Computerized Information Providers: A Look Back and A Proposed Analysis for the Future" (1995) 56 University of Pittsburg Law Review 655, 684.

[209] *Ibid.*, at 685.

[210] Henry H. Perritt Jr., *supra*, note 138 at 110-111.

[211] Jean-Louis Baudouin, "La responsabilité causée par les moyens d'information de masse", (1973) R.J.T. 201, 203.

freedom, publication supposes first-hand knowledge of the existence of the information transmitted[212].

While editorial discretion entails a presumption of knowledge of the harmful nature of the information transmitted, in the absence of editorial power, knowledge must be established for liability to be assigned. Knowledge can be assigned under many circumstances:

> *Knowledge, or the imputation of knowledge, can be established if the intermediary exercised content control over the messages on the network (e.g.: moderator of a bulletin board conference who screens messages before posting them) or if special circumstances were present, such as the fact that the operator knew of the user's repeated transmission of defamatory messages and had knowledge that a recent message may be defamatory. This special circumstance may arise even if an intermediary that otherwise does not exercise content control receives complaints about an originator of messages.*[213]

Yet how is it possible to impose a duty to prevent damages following the broadcast of information the harmful or illegal nature of which is likely to be determined only by a court decision? The same question arises following the emphasis of the harmful nature of a piece of information: what credibility must be granted to external sources of knowledge? What re-evaluation of this information must then take place?

These questions were asked in *Religious Technology Center* v. *Netcom Online Communication Services Inc.*[214] in an intellectual property context, which is however applicable to more global contexts. An anonymous user made available, through the intermediary of a discussion group, material copyrighted by the Church of Scientology. As soon as the latter was made aware of the infringement, it asked the system operator to remove the material. The system operator refused to act until it had obtained supplementary evidence. The judge ruled that Netcom was made liable through its failure to act, which amounted to substantial participation in the illegal distribution of material.

[212] Loftus E. Becker Jr., *supra*, note 127 at 217.

[213] Henry H. Perritt Jr., *supra*, note 138 at 107.

[214] 907 F. Supp. 1361 (N.D. Cal. 1995).

While it does allow us to focus on certain specific issues[215], this judgement does not provide any precise guidelines. In this case in particular, evidence revealed that Netcom had done nothing to stop the distribution of *potentially* illegal material and that it had even refused to look at the material in question. Still, what weight must a notification have to create a duty for a system operator, or any other intermediary which could prevent damage by stopping the circulation of the material, when the policy of the latter is to exercise no editorial control over the content it helps to circulate?[216]

While the safest solution would be to take action on each notification, such a practice would be incompatible with the freedom and openness to debate that exists on the Internet[217].

Another possible solution would be to protect the intermediaries from any liability until a judgement has been passed on the harmful, illegal or infringing nature of certain information, which could be removed from distribution. However Perritt demonstrates the weakness of such an approach, in particular in the case of broadcast of content infringing on intellectual property rights:

> *...that approach would not adequately protect the interests of copyright holders. It takes a long time to get a judgement on the merits in most jurisdictions and continued availability of infringing materials while the litigation process proceeds could result in substantial irreparable harm to the copyright holders.*[218]

The notion of knowledge will also be shaped by the damage likely to be caused. For example, defamation results by definition in a negative perception held by third parties, a criterion evaluated in function of the perceptions of an

[215] "Does the notice of violation identify which materials are at issue? Does it provide specific evidence of copyright ownership or just a vague claim?": "The Scientology Lawsuits and Lawyer Letters: The Problem Faced by On-line Services Who Get Notice of Users' Alleged Violations", Legal Bytes, Spring 1996, Vol. 4, No. 1, http://www.gdf.com/1b4-1.htm.

[216] "The Scientology Lawsuits and Lawyer Letters: The Problem Faced by On-line Services Who Get Notice of Users' Alleged Violations", Legal Bytes, Spring 1996, Vol. 4, No. 1, http://www.gdf.com/1b4-1.htm.

[217] *Ibid.*

[218] Henry H. Perritt Jr., "Computer Crimes and Torts in the Global Information Infrastructure: Intermediaries and Jurisdiction", (12 October 1995), http://www.law.vill.edu/chron/articles/oslo/oslo12.htm.

ordinary person[219]. As soon as it is presumed that the exercise of editorial freedom leads to contact between the editor and all content published, it is taken for granted that the editor, as a reasonable person, knew that the statements with which he or she had been in contact could harm the reputation of the person they targeted, but that he or she nonetheless published them.

In the case of certain types of information, it is often impossible for intermediaries, which were in no way responsible for the establishment of such information, to know if it is inaccurate and thus capable of causing harm. In such cases, presumed knowledge will thus be necessary for the assignment of liability:

> *It may well be argued that the producer will be liable if he publishes or fails to correct inaccurate data after he discovers it is unreliable, at least if he is aware of their potentially damaging nature. [...] On the other hand, liability may be limited because the defendant knew, or at least should have been aware, that the data were not reliable.*[220]

However the question is whether a regime of presumed knowledge will not have the practical consequence of transforming network operators into editors.

### 6.3.3 Relations between Liability and the Role Assumed in Information Dissemination

There are certain links between the role assumed in the dissemination of information and the liability following from that role. These links are entailed by principles applicable to the liability of intermediaries.

The new information technologies have stimulated analyses oriented toward a reformulation of the rules under which intermediaries in the information chain are held responsible for harmful information created by some one else[221]. What are the foundations of the attribution of liability to intermediaries in the information chain?

[219] N. Vallières, *supra*, note 37 at 20.

[220] Jaap H. Spoor, "Database Liability: Some General Remarks", (April 1989) 3 International Computer Law Adviser 4, 6.

[221] Henry H. Perritt Jr., *supra*, note 227.

While civil liability law in common law is built around duties of diligence[222], civil law approaches liability from the point of view of the prejudice suffered, and not the obligation which may have preceded it: the extent of liability is greater because any one who causes a loss or prejudice following unreasonable conduct is liable to provide compensation for the damages suffered[223].

Intermediary responsibility can result from the jurisdictional or practical impossibility of holding the true author of the tort liable. This concern is particularly relevant in the context of electronic communications:

> *Tort liability imposed on an intermediary is a kind of default rule or safety net, recognising that there may be instances in which the person with fault - the originator of the harmful message or file - would be unavailable, beyond the jurisdiction of any tribunal available to the victim, or judgment proof. Thus, the policy question for intermediary liability is whether the victim should bear the loss when the originator cannot be found, or conversely when the intermediary should bear the loss.*[224]

The question of intermediary liability is not entirely separate from issues of national jurisdiction. Since information highway communication technologies allow a person situated at one point on the globe to inflict prejudice on another person elsewhere simply by sending an electronic message, the difficulties in identifying the actor and obtaining compensation from him or her naturally moves attention from the victim of the damages to the intermediaries, which are likely to be more easily identified, subject to the jurisdiction of traditional legal institutions, and financially able to provide compensation for the prejudice.[225]

Another foundation of intermediary liability is the role as a contributor to and amplifier of the damage. Intermediaries would be subject to greater liability than that

[222] "First one has to ask whether as between the alleged wrong-doer and the person who has suffered damage there is a sufficient relationship of proximity or neighbourhood such that, in the reasonable contemplation of the former, carelessness on his part may be likely to cause damage to the latter in which case a prima facie duty of care arises": *Anns* v. *London Borough of Merton*, [1977] 2 All. E.R. 492 (H.L.).

[223] J. Huet, *supra*, note 92 at 107.

[224] Henry H. Perritt, *supra*, note 227.

[225] *Ibid*.

of the creators of the harmful communication because the intermediary's channel increases both the possibility and the severity of such a tort[226]. However, we must not underestimate the consequences of the imposition of an excessively strict standard of liability regarding intermediaries in the information chain.

## 7. Conflict in cyberspace

Several types of conflict can occur in cyberspace. Such conflict can be related to the infrastructure or the circulation of information, or it can result from difficulties in communication and exchanges:

**1.- Infrastructure:** Conflicts concerning transmission fall under this heading. For example, issues concerning access to a network belong to this category, as do conflicts involving access refused for discriminatory reasons, licensing and fee issues, disputes between Internet access providers and their clients, and quarrels about domain names.

**2.- Circulation of information:** This category covers disputes concerning the type of information circulating in cyberspace and how it is used. Thus the following issues belong here: privacy, honour and reputation, pornography, hate propaganda, fraud, dangerous or false information, intellectual property, copyright, etc.

**3.- Communication and exchanges:** This category essentially concerns the various aspects of electronic commerce. Contract and consumer disputes, as well as those involving advertising, belong to this category.

Of course, a priori, the state law of each country is intended to cover cyberspace conflict just like any other conflict. With respect to issue of public order, it is certain that state law, reinforced by international cooperation mechanisms, remains the principal vector of rulemaking.

However, in commercial matters cyberspace has features that require additional methods for dealing with conflicts. It is not so much a question of replacing the mechanisms of state law, but of providing supplementary mechanisms to attenuate the problems in resorting to the mechanisms of state laws to resolve conflicts in cyberspace.

Cyberspace is made up of environments that ignore state boundaries, and this exacerbates the difficulties generated by the structural differences between various state laws. Finally, relations in cyberspace tend to demand conflict resolution mechanisms that are in greater harmony with an environment involving continuous and discontinuous relations occurring over short periods.

[226] Henry H. Perritt Jr., *supra*, note 227.

### 7.1 Which law applies when there is a conflict?

Conflicts between jurisdictions and between laws are seen as two distinct mechanisms and the results do not always point to the same legal order. When there is a legal situation with a foreign feature, the first step is to determine which rules of conflict apply. Next we must identify the tribunal with jurisdiction to hear the dispute and then the applicable law.

The rules concerning the determination of a tribunal's competency with respect to a case can be called upon to play an important role in electronic environments. At the European level, the determination of competent jurisdiction is facilitated by the rules of the Brussels Convention, September 27, 1968, concerning judicial competence and execution of civil and commercial decisions[227].

The competence of courts used to be established only with respect to situations occurring on the territory under their jurisdiction, but the rule has become increasingly flexible to allow courts to extend their jurisdiction to defendants who, by establishing themselves abroad, compromise the application of legislation. Thus, in American law, the *long-arm statutes* recognise the competence of courts with respect to defendants who are not domiciled and have no residence in the court's jurisdiction, so long as such defendants have established "*minimal contact with the forum such that maintenance of the action is not contrary to the traditional notions of equity and substantial justice"*[228]. Henry Perritt has referred to the application of these principles in electronic environments:

> *An electronic publisher should be subject to personal jurisdiction in any place to which the electronic publisher intentionally sends its publication. Thus, subscription-based commercial systems like Compuserve or America Online should be subject to personal jurisdiction in places where significant numbers of their subscribers reside. The residence of subscribers is known to these services, they derive revenue from those subscriptions, and there is little reason to distinguish between the electronic subscriber and the print subscriber. If an electronic publisher (including an individual poster) publishes a statement intended to injure someone, the publisher should be subject to personal jurisdiction in the place where the injured party is located.*[229]

However, wanting to classify the activities of individuals in electronic environments according to their physical location is not always appropriate. It may sometimes even prove impossible. There are a number of situations involving certain activities taking place in electronic environments in which the participants will not be able to situate those activities in space. This delocalisation phenomenon is accentuated by the suggestion, proposed by several authors, that electronic environments constitute a distinct, autonomous geopolitical space.

[227] Tanguy VAN OVERSTRAETEN, "Droit applicable et juridiction compétente sur Internet", (1998) 5 *Revue de droit des affaires internationales*.

[228] Voir *International Shoe Co.* v. *Washington, Office of Unemployment Compensation & Placement*, (1945) 326 U.S. 310.

[229] Henry H. PERRITT Jr., *Law and the Information Superhighway*, New York, Wiley Law Publications, 1996, pp. 513-514.

The problem of identifying a competent forum in private law is however attenuated by the ability individuals have, in their contractual relations, to determine that forum in advance through an "election of forum" clause. Such clauses, as we will see later, could become one of the principal solutions to jurisdiction problems encountered in electronic environments.

When the competence of the tribunal is established, that tribunal does not necessarily apply the substantive rules in effect in its territory. The competence of tribunals is not necessarily established in accordance with the same criteria of relation as those that apply to the substance of disputes: a case duly referred to a court could have the substantive rules of law of another state applied to it. The criteria of relation are essential spatial: the applicable law will be that of the place where a person, legal act or event can be situated.

Moreover, the recognition and execution abroad of court decisions is the ultimate instrument developed by international private law. Such measures allow states to ensure reciprocal enforcement of decisions rendered by the courts without restrictions as to the territory or persons under their jurisdiction.

In cyberspace all these rules have major importance because a number of foreseeable conflicts could be situated at the level of determining the applicable rule or body of rules.

### 7.2 Dealing with conflict in cyberspace: experiments with cybercourts

As early as 1992, Henry Perritt wrote that the use of new information technologies could be an appropriate means to optimise the operation of adjudicative authorities[230]. In 1993 he considered the idea of an electronic mechanism for resolving conflicts occurring in cyberspace[231]. For him, there is no doubt that the electronic application of a pre-existing rule[232] is no more complex than rulemaking[233]. In simple terms, he confirmed that it is perfectly possible to envisage the electronic resolution of conflicts arising in cyberspace:

> *Adjudication is no more difficult to implement electronically than rulemaking. There needs to be a particular kind of message and a specified manner of "serving" it and a way for the pleading, discovery and trial functions to be performed. Pleading is easy because it simply envisions the exchange of electronic documents setting out the facts*

[230] Perritt refers in this respect to the concepts of "adjudication" and "rulemaking", which he defines as follows: *"Adjudication involves the application of a pre-existing rule to a particular case. Rulemaking involves the formulation of new standards for application in later adjudications as pre-existing rules. There is a loose correspondence between the categories of adjudication and rulemaking in administrative law, and the categories of contract administration and contract formation in contract law. Rulemaking and contract formation define a relationship, establishing standards for the first time. Contract administration, like adjudication, applies the standards to particular conduct"*. Henry H. PERRITT Jr., "The Electronic Agency and the Traditional Paradigms of Administrative Law", (1992) 44 *Administrative Law Review* 79.

[231] Henry H. PERRITT Jr., "Dispute Resolution in Electronic Network Communities", (1993) 38 *Villanova Law Review* 349.

[232] La fonction d'"adjudication" pour Perritt.

[233] Le "rulemaking" pour Perritt.

> *and legal theories supporting a claim and the response. Discovery, at least in the form of interrogatories, similarly is simple to accomplish through an electronic network.* [234]

It is important to note that technology does not yet provide all the answers when a face-to-face meeting is inevitable:

> *The trial function envisions an adversarial presentation before a neutral decisionmaker who has some formal way of signifying his decision. Modern litigation is becoming more focused on discrete issues decided largely on paper submissions, with the single-event, face to face trial playing less of a role. This trend and single-issue decisions based on written submissions can be accommodated nicely in an electronic network environment.*
>
> *The face-to-face portions are more difficult. As multimedia becomes common, recorded audio and video testimony within the adjudication database is conceivable. Until then, the most that can be done in a purely networked environment is interactive argument and presentation through a "chat" feature. It is far from clear, however, that this mode of electronic dispute resolution would be efficient because people type more slowly than they talk.*[235]

Moreover in the majority of cases complementary methods, unlike legal proceedings, do not really require face-to-face interaction and can very well take place entirely in writing, thus using electronic means.

David R. Johnson also wondered whether the networks themselves should not promote a conflict resolution system. Beginning with the idea that electronic conflicts have features that are theirs alone, in particular their instantaneousness, delocalisation, transnationality and interactivity, he argues that the networks could be an ideal place to establish flexible mechanisms better adapted to the needs of cybernetic communities:

> *Disputes that have arisen over networks are, demonstrably, different in character, as well as in subject matter, from more traditional fights. Like everything else electronic, they happen more quickly than their terrestrial counterparts. More people tend to be involved. There are fewer facial cues - and less chance for a physical fist-fight. They may involve people located in many different territorial jurisdictions. And they are more interactive in character - more rapidly evolving from one state to another. These characteristics compound the difficulties faced by traditional authorities in offering adequate dispute resolution mechanisms.*[236]

Considering the possibility of the emergence of a specific legal regime respecting the fundamental characteristics of cyberspace, Johnson suggests that the best way to contribute to

[234] Henry H. PERRITT Jr., "Dispute Resolution in Electronic Network Communities", (1993) 38 *Villanova Law Review* 349, 394.

[235] Henry H. PERRITT Jr., "Dispute Resolution in Electronic Network Communities", (1993) 38 *Villanova Law Review* 349, 394.

[236] David R. JOHNSON, "Dispute Resolution in Cyberspace", (1994) 136 *N.J.L.J.* 10, 21.

the development of a body of rules is to provide users experiencing conflicts with an effective procedure for resolving them.

Claudine Schweber reviews the first attempts to use technology for these purposes. With respect to the latest developments, she writes:

> *So far, there are only a few examples of attempts to use technology entirely. Yeend developed and successfully implemented a three-step electronic dispute management system involving structured negotiation, conciliation, and binding arbitration that was used for several years by the client corporation (Yeend). Helie participated in a multi-party, multi-issue on-line mediation in which he created an electronic conference with structured topics and some restricted access; however, the electronic mediation was halted due to conflicts and was eventually settled by telephone; the electronic medium remained for document sharing (Helie); Macduff was involved in an international electronic mediation sitting at his computer in New Zealand (Macduff); a private non-profit business organisation experimented with telephone and fax mediation (Schweber). Some others use technology in addition to the face-to-face process : consensus building with an overhead monitor connected to a computer (Helie), the transmission, on disk, of changing positions and last-best-offers in arbitration (Denenberg), negotiating rules at the Occupational Health and Safety Administration (OSHA) using computers to send messages and shuttle documents among negotiators (Skrzycki), electronically completing portions of an international negotiation which requires finesse in wording after the substance has been agreed to (Macduff). Indications are that plans to further test the limits of the electronic medium are under way; one firm has a software tool (CM/1) and a decisionmaking method which has been presented to conflict resolution groups (de Matteo), another has extensively and successfully tested an interactive computer assisted negotiation (ICANS) prototype for multi-party, multi-issue problems (Thiessen), others are talking about expanding use of the medium for governmental regulatory negotiations (Perritt, GSA/Action Plan, Helie) or in the international arena (Macduff).*[237]

In addition to the projects Schweber mentions, we should note the various enterprises offering mediation or arbitration services over the Internet[238]. In the majority of cases, however, such services do not specialise in the resolution of conflicts arising in cyberspace. Moreover, these enterprises do not provide conflict resolution by electronic means: they simply use the medium to offer their services.

However, the Global Arbitration Mediation Association Inc. (GAMA)[239]" does offer arbitration and mediation services using electronic means. The technique is simple: the parties

[237] Claudine SCHWEBER, "The Use of Technology in Conflict Resolution", http://www.batnet.com/oikoumene/arbtadr.html. On Yeend's project referred by by Schweber, see the short text by Nancy Neal YEEND, "Electronic Alternative Dispute Resolution System Design", (Hiver 1993) 11(2) *Mediation Quaterly* 193.

[238] In particular, see the following sites: http://www.adr.com/portfolio/index.html; http://www.gama.com/; http://www.cbbb.org/cbbb/adr.html#top; http://www.cba.uh.edu/center/aawdri.html; http://www.adr.org/overview.html.

[239] Available on the Internet at: http://www.gama.com/.

have to complete an application form for arbitration that they then transmit by electronic mail. However this enterprise does not specialise in resolving conflicts arising in cyberspace.

Mechanisms for resolving disputes over domain names are certainly the first to have adopted a cyberjustice approach.

Many policies on domain name management refer to the benefits of using alternative mechanisms to deal with disputes and to the need to resolve conflicts by taking advantage of the possibilities offered in cyberspace itself. Thus, the World Intellectual Property Organisation has established an arbitration service intended to deal with both disputes over domain names and other conflicts based over intellectual property.

Indeed, it seems natural to suppose that conflicts arising in cyberspace will increasingly be dealt with, or even resolved, in that same environment. With respect to the experimentation undertaken in the framework of projects such as CyberTribunal and Virtual Magistrate, the operations developed must be designed so as to facilitate the resolution of conflicts such as those over domain names.

### 7.2.1 Virtual Magistrate

On March 4, 1996, the Cyberspace Law Institute (CLI)[240] and the National Center for Automated Information Research (NCAIR) jointly launched the Virtual Magistrate Project (VM), an entirely electronic arbitration service[241] with the following general goal:

> *The Virtual Magistrate Project will offer arbitration for rapid, interim resolution of disputes involving (1) users of online systems, (2) those who claim to be harmed by wrongful messages, postings, or files and (3) system operators (to the extent that complaints or demands for remedies are directed at system operators). Arbitration services will be available for computer networks anywhere in the world as long as relevant parties agree to participate.*[242]

The specific goals of this pilot project are to:

*1. Establish the feasibility of using online dispute resolution for disputes that originate online.*

*2. Provide system operators with informed and neutral judgements on appropriate responses to complaints about allegedly wrongful postings.*

*3. Provide users and others with a rapid, low-cost, and readily accessible remedy for complaints about online postings.*

[240] It is interesting to note that Perritt and Johnson are both members of the CLI. In fact, Johnson is the Co-director of it.

[241] At present, the cases requiring mediation or conciliation must instead be redirected to other organisations.

[242] “The Virtual Magistrate Project”, Concept Paper, 26 February 1996, http://vmag.vcilp.org/docs/ vmpaper.html

> *4. Lay the groundwork for a self-sustaining, online dispute resolution system as a feature of contracts between system operators and users and content suppliers (and others concerned about wrongful postings).*
>
> *5. Help to define the reasonable duties of a system operator confronted with a complaint.*
>
> *6. Explore the possibility of using the Virtual Magistrate Project to resolve other disputes related to computer networks.*
>
> *7. Develop a formal governing structure for an ongoing Virtual Magistrate operation.*[243]

The Virtual Magistrate Project arbitration tribunal is made up of three arbitrators selected from a list of qualified arbitrators. This list is public and so can be consulted by cybernauts. This list is determined by members of a sub-committee of the CLI, jointly with representatives from the American Arbitration Association (AAA). The arbitrators, who are not exclusively lawyers, must have extensive knowledge of electronic environments[244]. A code of conduct has also been developed to provide a framework for their activities[245].

Arbitration takes place essentially using electronic mail. The injured party refers the dispute to the adjudicative authority by answering a set of questions on, in particular, the date of the incident, the parties involved and the field of activites concerned and by describing the incident and the solution desired[246]. Virtual Magistrate commits itself to rendering, in so far as it is possible, a written award to the parties within 72 hours after receiving the complaint. A fee of $10 is billed to the complainant to discourage frivolous cases.

In reality, the technical procedure takes place as follows:

> *A listserver/newsgroup ("grist") will be established for each case, and participants will be directed to post messages to the grist. Messages posted to the grist will automatically be sent to all participants. The address will be included in the initial notification letter. Participants will be provided with password access to the grist, allowing all messages to be reviewed. Each decision will be posted to the grist so that all participants will receive a copy.*
>
> *The Magistrate will conduct fair and appropriate proceedings to reach a decision in the time available. The Magistrate may ask the complainant for additional information and may permit the complainant to amend the complaint. The Magistrate may contact the parties, conduct proceedings, ask questions, collect information, solicit arguments,*

[243] "The Virtual Magistrate Project", Concept Paper, 26 February 1996, http://vmag.vcilp.org/docs/ vmpaper.html, section titled "Pilot Project Goals".

[244] "The Virtual Magistrate Project", Concept Paper, 26 February 1996, http://vmag.law.vill.edu:8080/docs/ vmpaper.html, section titled "Appointment of Virtual Magistrates".

[245] See the "Virtual Magistrate Hanbook", http://vmag.law.vill.edu:8080/magis/vmhdbook.html.

[246] See: http://vmag.law.vill.edu:8080/forms/dispute.form.html.

> *or take any other steps that the Magistrate deems appropriate and fair. When practical, the Magistrate will keep participating parties informed of these activities and will share with participating parties information received.*
>
> *Participants will also be given a private email address for the magistrate in case that there is a need for private communications. It will be up to the magistrate to determine if private communications will be accepted. At the discretion of the Magistrate, submissions from persons who are not participants to a proceeding may be accepted and considered.*
>
> *The Magistrate will maintain a copy of all records, correspondence, evidence, and other materials relevant to the case. All materials will be forwarded at the completion of the case to the Villanova Center for Information Law and Policy.*[247]

Obviously, as in the case of non-electronic environments, the process is voluntary and so based on the parties' agreement to submit the conflict to arbitration[248]. A system operator could thus agree to insert a clause in its user contract providing for recourse to VM in the case of conflicts or require the consent of users so that complaints would be directed to that service. The system operator could also promise in the user contract to base its conduct on the awards determined by Virtual Magistrate[249]. The limitations of this solution must, however, be noted.

Presently, the field of Virtual Magistrate's activities is limited to conflicts arising out of messages and files with illegal content, for example, royalty or trademark infringement, illegal appropriation of commercial secrets, libel, fraud, unfair business practices, inappropriate material (obscene material or hate propaganda) and infringement of privacy.

Thus the adjudicative authority decides whether it is reasonable for a system operator to destroy, mask or restrict access to a specific message, file or transmission. It is possible to believe that the authority could be called upon to determine an award on the disclosure of the identity of an individual to a person other than the government. In extreme cases, Virtual Magistrate can decide on whether it is appropriate for a system operator to deny a given person access to an electronic environment. Thus issues concerning invoicing and financial obligations are not examined in the framework of this project. However, with the parties' agreement, the adjudicative authority could possibly extend the scope of its decisions[250].

To determine awards, the arbitrators must consider the information available, code of the network in question, applicable contracts and appropriate substantive law. This said, they

[247] See the "Basic Rules", http://vmag.law.vill.edu:8080a/docs/vmrules.html.

[248] Obviously, since at present use of an arbitration clause has not yet become a contractual practice, there is a certain risk that one of the parties will not consent to arbitration. However this risk seems to us to be attenuated, in most cases, by the parties' desire to preserve their business relations and their corporate image.

[249] "The Virtual Magistrate Project", Concept Paper, 26 February 1996, http://vmag.law.vill.edu:8080/docs/vmpaper.html, section titled "Effects of Decisions".

[250] "The Virtual Magistrate Project", Concept Paper, 26 February 1996, http://vmag.law.vill.edu:8080/docs/vmpaper.html, section titled "What will the Virtual Magistrate decide?".

are not bound to automatically apply the law of a given jurisdiction. Rather, they must take into consideration the circumstances of each case, the parties' views on the applicable legal principles and remedies, as well as the potential effects of the dispute if it were to be transferred to the courts or an executory conflict resolution mechanism[251].

Virtual Magistrate decisions are generally made public on the World Wide Web, more specifically through the Villanova Center for Information Law and Policy server[252]. The process itself remains confidential until the award is rendered.

### 7.2.2 Online Ombuds Office

Online Ombuds Office is a project established by the Center for Information Technology and Dispute Resolution at the University of Massachusetts. Since 1996, this service has been offering mediation services for the resolution of conflicts arising in certain Internet contexts. The disputes covered by this service include conflicts between members of news groups and discussion lists, respecting domain names, between competitors, between Internet access providers and subscribers, and relating to intellectual property. The goal of the project is to develop methods based on the advantages of cyberspace to improve the way that conflicts are dealt with. In particular, research has been undertaken on the use of text and even graphs to assist resolution. Agreement proposals are sent to the parties using graphs and other computer tools to help them determine their respective levels of dissatisfaction and what they require from each other.

### 7.3.3 Cybertribunal

Cybertribunal is an experimental project undertaken by the University of Montréal in September 1996. Its goal is to identify the feasibility conditions for light, effective conflict prevention and resolution mechanisms for the various actors taking part in cyberspace transactions. The project has established an innovative service for the prevention and resolution of conflicts arising in cyberspace.

CyberTribunal originates in an institution located in a country with mixed law, bringing together jurists used to legal biculturalism. The dual influence of civil and common law is clearly important in a field greatly inclined to comparison and globalisation. These two features are not without importance if geographical borders are to be replaced by cultural frontiers.

CyberTribunal's field of application is much greater, though it is limited to disputes arising on the Internet or analogous electronic environments. CyberTribunal does not rule on cases of a public nature. Services are offered in French, English and, in the future, Spanish.

[251] "The Virtual Magistrate Project", Concept Paper, 26 February 1996, http://vmag.law.vill.edu:8080/docs/vmpaper.html, section titled "Standards for Decisions".

[252] See the following Internet site: http://vmag.law.vill.edu:8080/.

In spite of its name, CyberTribunal does not claim to play the role of a judge. Rather its purpose is to facilitate dialogue between the parties to a dispute (mediation) and, if necessary, act as a legal institution called in to help those parties (arbitration). The mediators and arbitrators working together in CyberTribunal are jurists and non-jurists, professors, and lawyers from a number of countries specialized in the fields of commercial mediation and new information technologies.

*Modes of operation*

Each of the parties must clearly express its agreement, before or after the conflict arises, to submit the dispute in which it is involved to CyberTribunal.

CyberTribunal has the appropriate computer equipment to ensure the confidentiality of those using its services. Thus the information relating to each case is accessible only by the parties concerned.

CyberTribunal fosters a cooperative attitude by promoting mediation over any adjudicative procedure. Even if the parties have signed an arbitration agreement, the procedure allows them to resort, by joint agreement, to prior mediation. In many cases the dispute is resolved through mediation and does not make it to the arbitration stage.

CyberTribunal's electronic site is made up of a reception module, a mediation module, an arbitration module and a module for the secretariat.

The reception module includes general information on CyberTribunal and the appropriate electronic forms for opening a file. When a person refers a case to CyberTribunal, he or she fills out an electronic form that includes that person's addresses and those of the other party. The person states the claim in his or her own words and explains the reasons supporting the application. This electronic form is encrypted and then sent to the CyberTribunal Secretariat, which then assigns a mediator (who could be located anywhere in the world) to take charge of the case. The mediator contacts the defendant, explains the claim and asks the defendant to participate in the process. Obviously the mediator's task is easier when the parties have made a prior agreement, by contract, to submit to mediation or arbitration.

The mediation module receives parties who accept to submit to mediation. The mediator contacts the parties and a secure site is assigned to them in accordance with the conditions and methods defined by the mediator assigned to the case.

The arbitration module operates in an environment with characteristics similar to those of the mediation module but more formal rules of procedure guide the process. The rules of procedure are modelled on those generally used in the field of commercial arbitration. However simplicity, friendliness, speed and fairness have been targeted, and arbitration can be accelerated if the parties consent. These rules of procedure have guided the team in designing the arbitration module. The goal is to allow parties to have recourse to arbitration without having to refer to the rules of procedure. In order to do this, certain processes have been automated and all relevant information is accessible in the computer environment. The parties can write and send electronic documents from their reserved site. The exchange of information is performed with all necessary security guarantees.

The CyberTribunal Secretariat module defines how information is processed when the Secretariat must take action.

## Conclusion

The features of cyberspace have various consequences on how it is regulated. These consequences are important because they help to identify the directions state policy must take in information highway development. Among the most important consequences are the facts that cyberspace regulation is necessarily international, increasingly conveyed by contractual tools and strongly motivated by the concern to share the responsibility among the parties. Furthermore, the guarantee of effective rules increasingly lies in mechanisms external to the state, such as in self-regulatory and certification mechanisms.

Little more is needed to infer from these new conditions that national policies still have a role to play if they converge with other national legal frameworks, providing their evolution is monitored and they are complemented by other regulatory tools. Such policies must foster the emergence of electronic spaces offering optimal guarantees of security, integrity and trustworthiness. National policies must target, above all, the establishment of regulatory tools complementing state law in order to influence the development of practices and promote values considered fundamental.

### Naturally international regulation

The regulation of cyberspace naturally goes beyond borders. The international nature of a number of interactions taking place in cyberspace raises problems that cannot be completely resolved by contracts concluded between parties or by the law of a single state. Depending on the jurisdiction in which one happens to be, different rules can apply to contract interpretation. This is why we must consider the perspective of an increase in the movement already begun toward achieving global uniformity in the rules governing international commercial transactions and, more generally, the circulation of information.

It is not inconceivable that we will see the emergence of a set of international rules of conduct stating and making explicit the principles to follow in regulating exchanges occurring in electronic environments. There are already a number of international forums where states can discuss which strategies would be best to adopt and the steps to take to coordinate them. In particular, discussions have taken place with in the G-7, OECD, ITU, ISO, OMC and WIPO. A number of governments have perceived the global dimension of this problem and recognise the need to cooperate in order to identify, in various fields, the major principles that will guide the development of rules to provide a framework for the many activities that can take place in cyberspace. However, such approaches must be followed while keeping a certain distance from the strictly positivist paradigms such authorities so often adopt.

There are many who wish for a true law of cyberspace, a body of laws separate from national legislation that would be based on the practices of those acting in this space. The challenge facing all countries and the various communities is to be sure to take part in both processes contributing to the emergence of a global legal framework for cyberspace because there are advantages in harmonising the international legal framework for electronic environments, and even the possibility of a true body of generally applicable rules. Given the possibilities of such an a-national body of rules, it is vital to establish and reinforce the tools for open, effective access within such non-governmental processes.

### The importance of contracts

The consensual nature of electronic communication invests contracts with a major role to play in the regulation of cyberspace. Contractual practices developing there are often the main source of rules effectively applying to relations between parties. In order to ensure equity in contractual relations, we must have mechanisms for complying with practices and establishing technical and legal security systems able to guarantee equity in relations occurring between partners of necessarily unequal strength.

### The division of responsibilities

Even in cyberspace we do not escape the obligation to determine who must answer for harmful information. The fundamental issue in cyberspace law remains that of the best ways to divide responsibilities between the various participants. A state's legislation covering responsibility is thus a major component in its information highway policy. Rules that are too restrictive or too permissive will have the consequence of attracting or discouraging the establishment of sites and of influencing the propensity of the parties to subject themselves to a state's legal principles and so possibly determine their respective shares in responsibility.

### Plural regulation

State regulation, in the sense in which it is usually understood – that which results from laws and regulations – is no longer sufficient to provide the balance desired in the many activities now taking place in cyberspace. Regulation rests more on technical standards than on techniques. For example, the regulation of legal uses of personal information depends only in part on legislation: increasingly, it originates in technical standards integrated directly into systems design. In this respect, the Model Code for the Protection of Personal Information of the Canadian Standards Association uses certain generally accepted principles.

The effectiveness of the regulation of activities taking place in cyberspace hangs on the ability to influence the content of the standards and practices that will inevitably emerge in various areas of activity. With respect to the protection of personal information, it must be noted that the principles of Québec law have inspired the development of standards such as those of the Canadian Standards Association. Thus, when there is an advance in legal research it becomes possible to establish regulatory tools more quickly and with greater chances of influencing practices in electronic environments. Here, as elsewhere in the field of information technology, research is a major strategic advantage.

The guarantee of the effectiveness of the rules is increasingly assured by mechanisms external to the state, such as self-regulation, certification, mediation and arbitration. The regulation of cyberspace is conveyed in a number of, often innovative, ways (legislation, regulations, standards, contracts, practices, techniques). While they are necessary, civil and penal sanctions are no longer sufficient to ensure the effectiveness of the rules. The challenge is to ensure that this regulation is sufficiently effective when it can no longer rely uniquely on state sanctions.

Since users make choices, regulatory mechanisms are increasingly based on the provision of information about the qualifications of sites and their compliance with certain standards of quality and trustworthiness. For example, an informed consumer wishing to perform transactions in cyberspace will look for sites with reputations for security and honesty. The availability of information on compliance with certain standards of good conduct then appears as an essential vehicle for a policy regulating electronic environments.

Thus we can predict that certification processes will be established to guarantee that sites wishing to post the appropriate label respect set rules. People or enterprises wishing to announce that they comply with a standard could undergo an audit and receive authorisation to say that they comply with a given code or standard. People who believe the enterprise does not comply with the standard would have access to a complaint mechanism. Loss of certification would be the ultimate sanction for failure to respect the standard. Thus the central guarantee of regulatory effectiveness would no longer be a penal or civil sanction, but rather the perspective of loss of distinctive signs informing users about promised trustworthiness.

**The role of state measures**

When faced with the features of cyberspace, there is a strong temptation to conclude that states can do nothing to promote respect for the balances inherent to all life in society. When national policies are implemented, state measures always have a role to play. However, they must converge with other national legal frameworks, be monitored and be complemented by other regulatory tools. In spite of the manifest limitations on its effective application, in certain cases state law can continue to apply to a large number of legal situations occurring in cyberspace, in particular those that suppose relations between parties in the same national jurisdiction. Yet the effectiveness of state measures is limited when they try to govern relations that cross borders. Among other things, given the relative ease with which activities can be delocalised in cyberspace, it is easy to conclude that these measures can be made virtually inoperative. In contrast, the proliferation of convergent state measures curbing the most universally condemned abuses will at least have the result of confining those who traffic in abusive or illicit information to territorial spaces that are easier to identify.

National policies must target the establishment of regulatory tools that complement state law in order to influence the development of practices and so increase the chances of promoting specific values.

In an environment dedicated exclusively to broadcasting, it is possible to implement restrictive regulation. For example, the regulation of radio and television is based almost exclusively on rules imposed on transmitting companies. However, in a network environment, there is no clearly identifiable transmitter or receivers. All the parties alternately or simultaneously play these roles to communication. Regulation must therefore be conceived as a set of solutions to the problems experienced by users.