Université de Montréal

LA TENEUR DU STANDARD DE FIABILITÉ DES MOYENS ÉLECTRONIQUES DE SIGNATURE

par

Ivan Mokanov

Centre de recherche en droit public
Faculté de droit

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade LL.M.
dans le programme de maîtrise en droit

octobre, 2002

RESUMÉ

Les institutions juridiques ont été bâties autour des réalités connues depuis des millénaires, que nous appelons de nos jours des phénomènes du monde réel. Ces phénomènes retrouvent présentement un nouveau théâtre – le cyberespace, et les règles du droit font face au défi de s'approprier ce nouvel environnement. Entre autres, les technologies du cyberespace ont mis au monde divers moyens qui nous permettent de nous identifier et de manifester notre attitude envers les actes juridiques - des finalités qui ont été assurées de longue date par la signature manuscrite. Bien que ces nouveaux moyens aient mérité un nom similaire à leur contrepartie traditionnelle - l'appellation de *signature électronique*, ils restent des phénomènes dont la proximité avec la signature manuscrite est discutable. Force est de constater que le seul point commun entre les moyens classiques et électroniques de signer réside dans les fonctions qu'ils remplissent. C'est en se basant sur ces fonctions communes que le droit a adopté une attitude identique envers les moyens d'authentification traditionnels et électroniques et a accueilli ces derniers sous l'emprise de ses institutions. Cependant, ceci ne signifie pas que ces institutions se soient avérées appropriées et qu'elles ne demandent aucun ajustement. Un des buts de notre étude sera de mettre en relief les moyens d'adaptation qu'offre le droit pour réconcilier ces deux environnements. Ainsi, pour ajuster l'institution de la signature aux phénomènes électroniques, le droit s'est tourné vers le standard de fiabilité de la signature électronique. Le standard de fiabilité est un complément de l'institution juridique de signature qui ne se rapporte qu'à la signature électronique et dont cette étude démontrera les applications. Les composantes du standard de fiabilité qui occuperont un deuxième volet de notre étude représentent un ensemble de règles techniques liées à la signature électronique. Ainsi, comme le standard de fiabilité puise sa substance dans les propriétés de l'architecture du cyberespace, l'attitude du droit envers la signature électronique s'avère tributaire de la morphologie du cyberespace. Étant donné que les possibilités qui nous sont offertes par la technologie continue à déterminer la réglementation juridique, il est légitime de conclure que l'examen des tendances dans l'évolution du cyberespace nous fournira un point de vue prospectif sur l'évolution des règles du droit.

Mots clés: preuve, sécurité informatique, système d'information, architecture du cyberespace

ABSTRACT

Legal institutions were built in order to govern realities that have been known for ages, which we regard today as real space phenomena. These phenomena have recently found a new stage - cyberspace, and accordingly, the rule of law faces the challenge to map this new environment. Diverse means pertaining to cyberspace technologies have made possible the achievement of the objectives of the handwritten signature - identification and exhibition of intent to be bound by legal consequences. Although these new means of technology were labeled with the title "electronic signature", they remain remote to the phenomenon named "traditional signature". It is obvious that the sole resemblance between traditional and electronic signatures appears to be in their ability to carry out the same functions. This resemblance grounds an identical legal position to traditional and electronic signatures, through the spread of the existing legal institutions over the new authentication means. However, legal institutions do not turn up to be automatically appropriate irrespectively of a considerable need for adjustment. Thus, the initial objective of our study will be to highlight the techniques of law to settle in the new environment. Aiming the adjustment of the legal institution to the electronic methods of authentication, the legal framework recourses to the reliability criterion for the electronic signature. The importance and the impact of the reliability criterion for the electronic signatures as part of the set of rules related to the signature, gave rise to our interest. Furthermore, we will study the components of the reliability criterion, which represent a set of technical rules governing the electronic signature. Consequently we reach a conclusion underscoring a strong dependence of legal solutions from the potential offered by cyberspace, or in other words, from its morphology. Given this assumption, the study of the tendencies in cyberspace architectural evolution places us in a better position to adopt a prospective point of view over the expectancies on the evolution of the rule of law.
Keywords: evidence, security, information system, architecture of cyberspace

Abréviations

ADE	Application Development Environment
AES	American Encrytption Standart
ANSI	The American National Standards Institute
C.c.Q.	Code civil du Québec
CEI	Commission électrotechnique internationale
CNUDCI	Commission des Nations Unies pour le droit commercial international
CRID	Centre de Recherches Informatique et Droit
DES	Digital Encrytption Standart
DLL	Dynamic Link Library
EAL	Evaluation Assurance Level
ETSI	The European Telecommunication Standardization Institute
F.R.E.	Federal Rules of Evidence
IAB	The Internet Architecture Board
IESG	The Internet Engineering Steering Group
IETF	The Internet Engineering Task Force
IPv6	Internet Protocol Version 6
IRTF	The Internet Research Task Force
ISO	Organisation internationale de normalisation
ISOC	The Internet Society
IVV	Independent Verification and Validation - Validation et vérification indépendantes
L.C.C.J.T.I.	Loi concernant le cadre juridique des technologies de l'information
NIST	The National Institute of Standards and Technology
PDA	Personal Digital Assistant - Assistants numériques personnels
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
POP	Post Office Protocol
R.C.J.B	Revue critique de jurisprudence belge
S.I.	Système d'information
SMTP	Simple Mail Transfer Protocol
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
TCP	Transmission Control Protocol
TI	Technologies de l'information
U.C.C.	Uniform Commercial Code
UDDI	Universal Description, Discovery, and Integration
UETA	Uniform Electronic Transacion Act
UIT	Union internationale des télécommunications
VSAM	Virtual Storage Access Method
W3C	The World Wide Web Consortium
XML	eXtensible Markup Language - Langage de balisage extensible

Table des matières

Table des illustrations

Introduction

« *Life was simple before World War Two,*
after that we have got systems »

Amiral Grace Murray Hopper[1]

Le droit face au numérique

[1] Dire que le droit s'est retrouvé face à un phénomène nouveau, le cyberespace, serait vrai et faux à la fois.

[2] La maîtrise technologique nous a offert un monde différent, où les notions de possible et d'impossible, se distinguent sensiblement de celles auxquelles nous étions habitués dans le monde réel. L'apparition du cyberespace a donné lieu à de nouveaux phénomènes, tels que la création de la plus vaste bibliothèque (le World Wide Web) et un réseau mondial de communications. Les notions de communautés et de frontières, de distances et de contacts entre les hommes dans le monde virtuel nous portent légitimement à croire que le cyberespace est radicalement novateur.

[3] Pour novateur qu'il soit, le cyberespace n'est qu'un autre domaine de l'exercice d'activités humaines. Facilités ou empêchés par les propriétés de la technologie, les hommes ont continué d'agir et de vivre leurs expériences dans le monde virtuel. Les gens continuent d'interagir, de discuter, de négocier et de conclure des contrats, de créer, publier et obtenir des informations dans le cyberespace. Les activités connues de la société depuis des millénaires ont trouvé un nouveau théâtre.

[1] Grace M. Hopper est un expert en informatique, devenue amiral à la marine américaine, source : http://web.mit.edu/invent/www/inventorsA-H/hopper.html , visitée en mai 2002

[4] Ce théâtre est, en premier lieu, porteur de la caractéristique « virtuel » au sens d'insaisissable, qui ne peut pas être situé précisément et manque de caractère spatio-temporel s'opposant donc au réel et au tangible.[2] Ainsi, le cyberespace est défini comme un environnement global virtuel d'ordinateurs reliés entre eux grâce à des réseaux.[3] Nous estimons pertinent de soumettre cette définition à une lecture élargie à la lumière de la vision de Laurence Lessig qui étend encore le concept de cyberespace en y incluant d'autres zones. L'auteur utilise l'exemple de l'affaire Olmstead[4], impliquant des compagnies de téléphone, pour illustrer les premiers effritements entre la Constitution américaine et le cyberespace.[5] Lessig énonce qu'avant même 1928 « much of life had moved onto the wires… those first steps into cyberspace»[6]. Dans le cadre de cet exposé, nous ne nous limiterons pas à considérer le cyberespace comme une dénomination de l'Internet. Il n'existe pas d'obstacles à envisager tous les médias véhiculant de l'information par des moyens électroniques, tels la téléphonie, le télégraphe, les réseaux fermés, les systèmes de guichets bancaires, le réseau de cartes de crédit, la télévision interactive et bien évidemment Internet et le World Wide Web, comme des zones du cyberespace ou de l'espace virtuel. L'adoption de ce point de vue large se justifie aussi par l'avenir qui se présente devant les moyens de communication de l'information. Si dans les prochaines années les ressources informationnelles sont partagées, disponibles et accessibles de tout dispositif - des machines de jeux, des postes de travail, des téléphones cellulaires, des assistants numériques personnels (Personal digital assistant ou PDA) – nonobstant la zone dans laquelle ces dispositifs se situaient jusqu'alors, ceci serait encore un argument à l'appui d'une définition large du cyberespace.

[5] Parmi les activités se déroulant sur cette nouvelle scène qu'est le cyberespace, il y a des rapports sociaux auxquels le droit continue de s'intéresser et qu'il continue de gouverner par ses institutions même si elles sont situées en dehors de leur environnement original. Ainsi, les institutions juridiques préexistantes, se sont retrouvées face à un monde nouveau.

[6] Tout de même, la rencontre entre le droit et la nouvelle architecture, ne s'est pas faite sans contrainte. Cette problématique est explicitée dans les propos de Laurence Lessig :

---

[2] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF, Sophie HEIN, *Droit du cyberespace*, Montréal, Thémis, 1997, p. 1 - 13
[3] *Id.*, p. 1 – 15
[4] 277 U.S. 438
[5] Lawrence LESSIG, « Reading the Constitution in Cyberspace », *Emory Law Journal*, 45 (1996), 869, 872
[6] *Id.*

> *« Our institutions about property, and about how best to order society, are institutions built in a particular physical world. We have learned a great deal about how best to order that world, given the physics as it were, of that particular world.*
>
> *But the physics of cyberspace is different. The character of the constraints is different. So while there may be good reason to carry structures that define real space into cyberspace, we should not assume that those structures will automatically map. »*[7]

[7] Selon l'auteur, l'architecture du cyberespace rend les institutions juridiques inappropriées et plaide pour une réglementation différente. Par conséquent, la régulation du monde virtuel provoque deux processus complémentaires - la modification des institutions du droit d'une part et la modification de l'architecture du cyberespace d'une autre.

[8] Lorsque nous parlons d'architecture, il faut tenir compte que le cyberespace est une notion large, qu'il serait plus justifié de considérer comme l'ensemble de plusieurs sphères d'activité. Comme l'énonce Lessig, le cyberespace n'est pas unifié, il englobe plusieurs endroits dont les caractéristiques ne sont pas identiques[8]. Chaque activité ou ensemble d'activités similaires peuvent être identifiés comme des espaces distincts les uns des autres chacun possèdant son propre degré de différence avec sa contrepartie du monde réel. À titre d'exemple, les domaines des droits d'auteurs, de la protection de la vie privée et de l'authentification forment en soi des sphères d'activités au sein du cyberespace. Ces sphères d'activités se distinguent aussi de leur contrepartie du monde physique. Par conséquent, la manière dont le droit appréhende le monde virtuel doit être analysée séparément pour chaque activité.

[9] Dans cet ordre de réflexions, nous nous intéresserons spécifiquement à une représentation du processus de l'adaptation du droit et de modification de l'architecture, notamment celui de l'authentification dans le cyberespace à travers la réglementation de la signature électronique.

---

[7] Laurence LESSIG, *The Future of Ideas : The Fate of the Commons in a Connected World,* New York, Random House, Incorporated, 2001, p. 104

[8] Laurence LESSIG, *Code and Other Laws of Cyberspace,* New York, Basic Books, 1999, p. 63

La modification du droit

[10] Selon plusieurs hypothèses, la réglementation juridique n'a pas su étendre l'emprise de ses institutions sur les phénomènes virtuels sans modifier ses règles, telles les institutions de la propriété intellectuelle, la protection de la vie privée pour ne citer que celles-là. Le passage du papier au numérique a révélé de nombreuses divergences, entre le monde en ligne et le monde hors ligne, requérant une adaptation en profondeur de l'institution juridique et de l'architecture virtuelle. Tel est le cas de l'institution juridique de l'authentification et les architectures d'authentification dans le cyberespace.

[11] Le besoin d'authentifier les actes auxquels le droit attache une importance est une nécessité impérieuse ressentie dans les rapports sociaux. L'identification des personnes et de leur attitude envers les actes qu'elles produisent sont indispensables à l'attribution de conséquences auxdits actes. Parmi les moyens destinés à servir ces besoins, à partir des sceaux jusqu'aux souscriptions, la signature manuscrite s'est démarquée comme étant un des plus efficaces. Ainsi, assurant de la manière la plus appropriée l'identification du signataire et la démonstration de son consentement vis-à-vis du contenu de l'acte signé, le seing manuel a connu un avènement qui a été finalement sanctionné par l'institution juridique de la signature. De nos jours, la signature prend une importance majeure dans les rapports juridiques. Selon certaines hypothèses le droit en fait une condition à la validité des actes (elle est un élément *ad solemnitatem*), dans d'autres, elle est seulement un élément probatoire indispensable devant le tribunal (la signature accomplit un rôle *ad probationem*). Cet encadrement juridique, tel que nous le connaissons aujourd'hui, résulte de l'imposition progressive de la signature manuscrite.

[12] Le cyberespace est venu bousculer le monopole de la signature manuscrite en offrant d'autres moyens d'identification des personnes ou de révélation de leur consentement par rapport à leurs actes, englobés sous la notion de signature électronique.

[13] S'appuyant sur les fonctionnalités de la signature manuscrite, le droit a étendu son emprise sur ces nouveaux moyens d'authentification virtuels. Cette affirmation trouve confirmation dans les cadres législatifs civilistes et de *common law*. Nous nous sommes penchés sur la position de la tradition du droit civil, en faisant le choix d'analyser deux modèles de réglementation de la signature électronique. Celui proposé par la Directive

européenne[9] d'une part et le modèle québécois, d'autre part, exprimé dans le nouveau Code civil de 1994 et dans la *Loi concernant le cadre juridique des technologies de l'information*[10]. Pour ce qui est de l'approche fonctionnelle au sein de la tradition de *common law*, nous trouvons nos exemples dans la jurisprudence ainsi que dans le cadre réglementaire aux États-Unis - le *Uniform Commercial Code* et le *Uniform Electronic Transaction Act*.

[14] Ainsi, dans les cadres juridiques étudiés, sans modification substantielle des institutions, la réglementation juridique, se penchant sur les fonctions traditionnelles de la signature classique, a adopté une attitude similaire envers les moyens informatiques. Elle considère que tout moyen de signature peut être digne de reconnaissance légale, pourvu qu'il assure l'identification du signataire et son adhésion au contenu du document signé, remédiant ainsi à l'insécurité juridique. Il faut dire encore qu'une la définition large de cyberespace ayant été mise de l'avant, la signature électronique, comme phénomène technologique, doit elle aussi, obéir à cette vision étendue. Dans ce cadre, les moyens de réalisation de la signature électronique sont offerts par le cyberespace et une signature électronique peut donc être réalisée dans de différentes zones du cyberespace, la téléphonie, la téléphonie mobile, Internet, un réseau de guichets bancaires, un réseau de cartes de crédit. L'institution juridique s'étend désormais à une grande variété de formes autres que les signatures classiques.

[15] Cependant, l'étude de cette libéralisation du droit ne devrait pas perdre de vue des propriétés importantes de l'institution juridique de signature. L'imposition de la signature manuscrite accompagnée de la construction de l'institution juridique est un processus qui possède une autre facette. L'institution juridique de signature, en sanctionnant une forme de signature particulière, est demeurée profondément empreinte des caractéristiques et des spécificités du mode de signature traditionnel, le seing manuel. Par conséquent, en raison des grandes divergences entre les moyens de signature classiques et modernes, certaines règles du droit s'avèrent forcément inadaptées aux moyens fournis par l'architecture du cyberespace. Pour pallier cette inadaptation, le cadre juridique s'est doté d'un nouveau

---

[9]Directive 1999/93/ce du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, L13/12, JOCE, 19 janvier 2000 (ci-après citée Directive européenne)

[10] Loi concernant le cadre juridique des technologies de l'information, L.Q. 2001, c.32 (ci-après citée L.C.C.J.T.I.)

paradigme, dit *standard de fiabilité*. Il réfère à une règle de droit, faisant appel à la fiabilité des moyens électroniques de signature. Cette règle s'ajoute à l'ensemble de celles formant l'institution juridique de signature dans le contexte probatoire. Les règles de droit concernant les capacités probatoires de la signature électronique s'appliquent compte tenu des réponses aux interrogations sur la fiabilité du procédé de sa réalisation.

[16] Au plan probatoire, la signature est censée fournir des informations sur l'identité du signataire, sur son attitude envers l'acte signé, de même que sur le lien entre la personne déterminée et l'acte précis. Selon que les informations que porte la signature soient fidèles ou non, la signature sera authentique ou non. En tant que données porteuses d'informations, tant les signatures manuscrites que les signatures informatiques sont produites grâce à la mise en place de certains moyens et au cours d'un processus. C'est à ce propos que le droit de la preuve adopte une attitude différenciée par rapport aux signatures électroniques interrogeant la fiabilité des procédés de leur conception. Les cadres juridiques ne sont pas, et d'ailleurs ne peuvent pas, être discriminatoires par rapport aux signatures en tant que données, la signature électronique, tout comme sa contrepartie classique, ne pouvant être que vraie ou fausse. Le droit adopte cependant une attitude différenciée en matière de signature électronique par la prise en considération du procédé de réalisation de la signature. D'importantes conséquences juridiques concernant ses capacités probatoires sont donc liées à la fiabilité de ses moyens de réalisation.

[17] La fiabilité est définie par le Petit Robert comme l'« [a]ptitude d'un système, d'un matériel, à fonctionner sans incidents… ». L'adjectif « fiable » se dit, selon le dictionnaire, d'un matériel dans lequel on peut avoir confiance. La fiabilité a toujours trait à des fonctions requises, des spécifications habituelles. Dans ce contexte, la fiabilité du procédé informatique d'authentification réfère à la capacité du moyen de servir à la production d'une signature renfermant des garanties d'authenticité. Ce nouveau paradigme juridique représente une modification de la réglementation afin d'ajuster ses institutions à l'architecture du cyberespace.

[18] En effet l'institution juridique est complétée par des règles techniques liées à la signature. Le standard juridique de fiabilité est ensuite rempli de contenu par les paramètres techniques de l'architecture du cyberespace.

La modification de l'architecture

[19] La fiabilité des procédés électroniques d'authentification à laquelle le droit attache des conséquences pour le statut probatoire des signatures est un standard essentiellement liée à l'architecture et aux particularités du cyberespace.

[20] Le processus de réalisation de signatures électroniques peut être situé dans la structure et la hiérarchie de l'architecture du monde virtuel. Le milieu dans lequel ce processus a lieu est le *système d'information*, la composante de base du cyberespace. Cette composante représente une île d'information et de fonctionnalité. Le système d'information réfère à un ensemble d'unités structurantes – des intervenants, des données, des processus, des interfaces et des communications – mises en place pour assurer l'accomplissement de certaines fonctionnalités. La bibliothèque, le système de connexions téléphoniques, le système de communication par courrier électronique, une infrastructure à clés publiques sont tous des exemples de systèmes d'information. Le système d'information ne fait pas nécessairement partie du cyberespace, un grand nombre de systèmes d'information existent dans le monde physique. En revanche, lorsqu'il est situé dans le cyberespace et en forme le noyau, le système d'information repose sur les strates formant la hiérarchie du cyberespace, le milieu physique (la substructure), le milieu logique (la strate intermédiaire) et le contenu (la strate supérieure).

[21] Dans la grande variété de formes susceptibles de constituer une signature électronique il est difficile de trouver un point commun, une caractéristique essentielle de tous les moyens de signature que le cyberespace peut nous offrir. Des messages électroniques portant les initiales de l'émetteur, aux procédés reposant sur l'image de la rétine ou d'autres caractéristiques biométriques, en passant par le chiffrement mathématique de la cryptographie asymétrique, les techniques sont toutes différentes. Néanmoins un dénominateur commun les unit. La réalisation de signatures électroniques est une fonctionnalité du système d'information résultant d'un processus complexe impliquant les unités structurantes du système dont les caractéristiques influencent le procédé lui-même. Ainsi, la fiabilité du moyen virtuel de signer est conditionnée par les propriétés de l'environnement qui l'héberge. Les certitudes et les incertitudes concernant les capacités du moyen électronique d'établir un lien fiable entre la signature et son auteur, de même

qu'entre la signature et l'acte auquel elle se rapporte sont déterminées par les propriétés de l'environnement où le processus se déroule. Par conséquent, les interrogations du droit sur la fiabilité des procédés électroniques de signature trouvent leurs réponses essentiellement et uniquement dans les propriétés de l'architecture du cyberespace.

[22] Selon cette analyse, l'utilisation du recours au standard de fiabilité implique donc une modification de l'architecture. Les processus de création de signatures sont conçus au sein d'infrastructures à clés publiques, des constructions qui se veulent des environnements obéissant à leurs propres règles qui, au fond, modifient l'architecture du cyberespace l'illustre parfaitement.

[23] Le recours du droit à la fiabilité des moyens de signature, entraîne une convergence de l'ordre juridique et de l'architecture. Il est alors justifié d'énoncer, que l'ajustement du droit en matière de signature électronique est tributaire de la morphologie du cyberespace.

[24] Il convient s'intéresser dans une première partie à la consécration du nouveau paradigme juridique qu'est la fiabilité des moyens de signature. En effet, l'inadaptation du droit au monde virtuel (Chapitre I) implique le recours au standard de fiabilité du processus de réalisation de signature, qui introduit un ensemble de règles techniques associées à l'institution juridique de signature (Chapitre II). La deuxième partie s'attache au contenu des règles techniques liées à l'institution juridique de signature – la substance du standard de fiabilité (Chapitre I) et aux façons de répondre aux interrogations sur ledit contenu (Chapitre II).

[25] Il appartient aussi de nous pencher sur les tendances les orientations de l'évolution de l'espace virtuel comme un facteur intervenant dans la difficile imbrication du cadre juridique et l'architecture cybernétique.

[26] L'architecture du jeune Internet peut être un point de départ illustratif de la transformation de la morphologie cybernétique. Internet était basé sur des protocoles simples, tel TCP/IP. Les possibilités d'identification de ce protocole étaient très faibles, les possibilités de contrôles minimales. Selon Lessig, ce minimalisme était recherché et reflétait le choix politique de désactiver le contrôle d'une part et le choix technologique d'optimiser le design du réseau d'une autre.[11]

[11] L. LESSIG, *op. cit.,* note 8, p. 32-33

[27] Il est incontestable que ce cyberespace change. Comme l'exprime Lessig: *« How it looks, what you can do there, how you are connected there – all this has changed. »*[12] L'architecture du cyberespace se transforme et les possibilités offertes se modifient. Dans ce processus, il faut accorder la place méritée à la poussée générale vers une architecture favorisant l'identification.

[28] L'aspiration à une architecture « plus favorable au contrôle » est un fait persistant dans le développement du cyberespace. L'Internet original n'a pas survécu et son architecture a connu des transformations majeures orientées vers la construction d'un système de contrôle. Cette tendance est générale. Elle est caractéristique pour toutes les activités hébergées par le cyberespace et elle se manifeste, par exemple, par le renforcement du concept de propriété en dépit du « libre » et du « commun » en matière d'innovation et de prospérité.[13] Cette pulsion générale vers le contrôle prend la forme d'une aspiration vers une architecture d'identification, ce qui influencera la réglementation juridique en matière de signature électronique.

[29] Les architectures facilitant l'identification sont multiples. Au fil de l'innovation, l'authentification dans le cyberespace a été facilitée par les cookies, les certificats numériques, les infrastructures à clés asymétriques, les techniques biométriques. Nous pouvons estimer ces procédés de contrôle comme des solutions isolées. Elles peuvent cependant être vues comme autant de marches vers une architecture globale de confiance. Les architectures de contrôle peuvent favorisées par diverses incitations[14], afin de bâtir une architecture robuste d'identification. Si nous imaginons que les certificats numériques peuvent relater des faits liés à l'identité mais aussi chaque fait concevable et envisageable, ceci représenterait sans doute une plate-forme architecturale de confiance et de sécurité. Par conséquent, la position juridique envers la signature électronique y serait entièrement différente de celle qui reflète l'état de l'art du cyberespace d'aujourd'hui.

[30] Dans les pages qui suivent le but de notre analyse n'est pas de présager l'état du droit de la signature dans le contexte d'une architecture robuste d'identification. Cependant la bonne compréhension du rôle et de la nature du standard de fiabilité des moyens informatiques de signature, comme un nouveau paradigme en droit, nous permettra

---

[12] *Id.*, p. 64

[13] L. LESSIG, *op. cit.,* note 7, p. 238

[14] Lessig cite des exemples à l'appui de l'allégation que le droit et le marché, en tant que régulateurs, peuvent stimuler le passage à un « *ID enabled world* », L. LESSIG, *op. cit.,* note 7, p. 49-60

d’exposer l’interdépendance entre le cadre juridique et la morphologie architecturale du cyberespace et d’adopter une approche prospective.

Partie I - LA FIABILITÉ DES MOYENS ÉLECTRONIQUES DE SIGNATURE – LE NOUVEAU PARADIGME DU DROIT FACE AU CYBERESPACE

CHAPITRE I - LA SIGNATURE EN DROIT – DES VOIES TRADITIONNELLES ET MODERNES

Section I - LA SIGNATURE MANUSCRITE – LA SANCTION LÉGALE D'UNE DONNÉE COUTUMIÈRE RELEVANT DE L'INCONSCIENT COLLECTIF

[31] L'avènement de la signature manuscrite comme phénomène social et réalité juridique a été la réponse aux besoins impérieux des rapports juridiques. Il existe dans les relations juridiques une nécessité d'identifier les auteurs des actes, de même que de s'assurer de leur attitude par rapport aux dits actes, bien que cette nécessité n'ait pas toujours été aussi clairement définie. Parmi les moyens dont la communauté a fait usage pour atteindre ces finalités, c'est la signature manuscrite qui s'est imposée grâce à ses caractéristiques. Le choix collectif de la signature manuscrite a induit la création de l'institution de signature en droit. La réalité juridique qu'est la signature de nos jours est le fruit de l'attitude du droit envers la signature manuscrite, justement nommée traditionnelle.

[32] Dans cette section nous étudions le processus d'imposition de la signature traditionnelle dans les rapports sociaux et juridiques, soutenant que l'élaboration de l'institution de signature en droit a été d'une part inspirée par les caractéristiques de la marque manuscrite et, d'une autre part, a reflété ces caractéristiques. Les particularités de la marque manuscrite qui se sont imposées au législateur font l'objet du deuxième volet de notre analyse.

§ 1. De la marque manuscrite à l'institution juridique de signature

a. Historique

[33] Dans les rapports sociaux dont l'importance a suscité l'intérêt du droit, les actes des personnes sont un élément clé lorsqu'il s'agit de créer, modifier ou éteindre des droits et des obligations. Deux informations se sont avérées indispensables – l'obtention d'une

certitude en ce qui concerne les auteurs des actes et une assurance de leur attitude vis-à-vis du contenu dudit acte. Ces exigences d'information constituent des besoins impérieux des rapports juridiques. Sans qu'ils soient définis avec la précision et la clarté de la doctrine moderne s'intéressant à la signature, ces besoins ont été ressentis et la recherche de moyens pour y répondre a une longue histoire.

[34] Parmi les premières tentatives nous remarquons le signe gravé sur le chaton d'un anneau sigillaire porté au doigt dont les peuples de l'antiquité faisait usage il y a 3000 ans avant J.C.[15] Les bagues-scarabées égyptiennes servant de sceaux, les cachets des crétois et les marques de texte en relief imprimées dans l'argile fraîche des coroplates en Asie mineure sont parmi les premiers moyens auxquels la société a recouru pour authentifier les actes. Vers 740 avant J.C. les romains imprimaient des camées en relief sur la cire en guise de sceau.[16] Plus tard, au bout de quelques siècles, l'*annulus signatorius* (l'anneau à signer) s'est répandu dans l'Empire Romain. Dans la Rome Antique, l'empreinte produite par la gravure du chaton était nommée *signum* (signa, seing). Tous les citoyens romains possédaient des anneaux portant leurs propres signes. La technique d'authentification pouvait changer et le résultat de l'apposition de la marque pouvait être une empreinte en relief (la trace laissée par les sceaux) ou une trace humide pour laquelle l'outil était trempé dans l'encre (le cas des timbres). Les distinctions que les signes d'authentification portaient variaient de monogrammes et de patronymes jusqu'à des devises, des maximes, des personnages allégoriques.[17]

[35] Chronologiquement, les sceaux ont été suivis du *subscriptio* – l'apposition d'un signe représentant la souscription autographe. Cette méthode a été adoptée à partir de l'an 63 avant J.C. à partir de l'exigence pour le testament d'être accompagné du signe du testateur et des témoins, tracé de leur propre main, faisant état de leurs noms, de leurs qualités et du rôle joué dans l'acte. Initialement appliquée uniquement aux testaments, la souscription s'est étendue ensuite à tous les actes privés ou publics. L'expansion que la souscription a connue s'est déroulée pendant les règnes de Tibère et de Néron quand elle a été appelée *signum manuale* (seing manuel) pour la distinguer du seing apposé à l'aide du sceau. Malgré son apparition précoce, l'usage du seing manuel n'a été étendu que plus tard, lors

---

[15] Alain BUQUET, *La signature du sceau à la clé numérique, histoire, expertise, interprétation*, Paris, Édition Service Gutenberg XXIème siècle, 2000, p. 11

[16] *Id.*, p. 11

[17] *Id.*, p.12

de sa renaissance en France au début du 13ème siècle. Il en a alors été fait usage par les clercs de notaire, les médecins, les magistrats, sans tout de même réussir à remplacer complètement l'usage des sceaux.[18] Le seing du nom ou le petit seing, par opposition au grand seing ou seing ordinaire, fait aussi son apparition dans certaines chartes de la deuxième moitié du 13ème siècle. Le petit seing a été officiellement introduit dans la grande chancellerie royale de Philippe IV (Le Bel). L'usage de la signature a continué de se généraliser au cours du 14ème siècle, mais cette marque n'arrive pas encore à se substituer au sceau parmi les moyens d'authentification des actes. L'essor de la signature est incontestable à partir de Jean Le Bon et Charles V (Le Sage), mais son utilisation demeure facultative.[19]

[36] L'usage du seing manuel n'est devenu une formalité obligatoire dans les actes authentiques qu'à partir des ordonnances de Henri II, François II et Henri III, pendant la deuxième moitié du 16ème siècle. L'imposition de la signature manuelle comme moyen de servir aux besoins impérieux des rapports juridiques, accompagnée de l'évolution de l'institution juridique de signature débouchent sur l'adoption par le droit de la signature manuscrite comme la seule à être légalement valable à partir du 18ème siècle.[20]

[37] La place que le droit réserve à la signature, telle que nous la connaissons aujourd'hui, a été le fruit de deux processus historiques parallèles. L'imposition de la signature parmi les tentatives d'élaboration d'un moyen de répondre aux besoins des rapports juridiques d'une part – l'identification des auteurs, des actes et l'expression de leur volonté - et, d'autre part, de l'évolution de l'institution juridique de signature, telle que développée dans les systèmes juridiques modernes.

b. La création de l'institution juridique de signature – la réponse du droit

[38] Les multiples usages que le droit fait de la signature forment l'institution juridique de signature. Notons cependant que l'attitude du droit envers la marque manuelle, l'importance qu'il lui attribue, a subi une évolution avant de prendre ses dimensions modernes. Avant d'ériger la signature en partie du *negotium* et de l'*instrumentum*, telle que

[18] *Id.*, p. 13
[19] *Id.*, p. 14
[20] *Id.*, p. 14

nous sommes habitués à la considérer aujourd'hui, le droit a vécu une évolution qui mérite notre attention.

i. L'évolution du droit s'articulant autour de l'imposition de la signature traditionnelle

[39] De la phrase d'Érasme « verba volant, scripta manent »[21] jusqu'au rôle de l'écrit comme formalité préalable à la validité de certains actes d'une part et de moyen de preuve prééminent de l'autre, le droit a certes connu un développement. Tout au long de cette évolution, de toutes les marques d'identité apposées sur un acte, la signature s'est vue reconnaître un impact particulier[22] qui n'a cessé de se confirmer au fil du temps.

[40] Par l'Ordonnance de Villers-Cotterêts de 1493, François Ier a introduit l'exigence de rédiger les contrats en français. Cette ordonnance a été suivie de celle de Fontainebleau de 1554 qui a exigé que les notaires fassent signer aux parties leurs conventions. Cette règle s'avère être le fondement textuel de l'exigence de la signature dans le support des actes juridiques.[23] L'Ordonnance d'Orléans de 1560 transforme ensuite cette exigence en condition de validité des contrats, l'absence de signature manuscrite est sanctionnée par la nullité. Le développement légal se poursuit avec un acte de 1566, l'Ordonnance de Moulins, qui apporte une nouvelle extension du rôle de l'écrit en obligeant de passer devant notaires les contrats de valeur excédant cent livres et en interdisant le recours à des témoins contre et outre l'acte écrit. Ainsi, la suprématie de l'écrit sur le plan probatoire, a-t-elle été affirmée. Les exigences de forme des actes notariés et des actes sous seing privé étant établies en 1667, nous nous rapprochons des fondements de la réglementation moderne sur la place et l'importance de l'écrit.

[41] Ce bref parcours historique fait, nous constatons que l'attention actuelle que le droit accorde à la signature est le résultat d'un développement historique qui a abouti aux dispositions du *Statute of Fraudes* de 1677 et celles du Code Napoléon de 1804. Ce développement, il paraît légitime de l'énoncer encore ici, a d'une part été induit et inspiré par l'imposition de la signature comme moyen efficace de répondre aux besoins impérieux du droit. D'autre part, les particularités du seing manuel ont influencé profondément l'évolution juridique.

---

[21] John GLISSEN, « Le preuve en Europe (XVI – XIXe siècles) », *Recueils de la Société Jean Bodin*, p. 813
[22] Delphine MAJDANSKI, *La signature et les mentions manuscrites dans les contrats*, Bordeaux, 2000, p. 30
[23] *Id.*, p. 29

ii. Le paysage juridique actuel – le contenu de l'institution juridique de signature

[42] Il apparaît pertinent d'examiner les fruits de l'évolution historique de l'institution de la signature - l'état actuel du droit concernant la signature afin d'en révéler les caractéristiques et les principes généraux. C'est dans ce paysage juridique que le droit contemporain ambitionne d'intégrer de nouveaux phénomènes de signature.

[43] Sous réserve des différences entre les systèmes de *common law* et de droit civil vis-à-vis de la signature traditionnelle, sa place en droit peut généralement s'exprimer sur deux plans, à savoir le rôle que la signature se voit attribuer comme étant une partie du *negotium* ou un élément de son *instrumentum*. Certains contrats n'existent que par le respect d'un formalisme particulier, ces actes étant les contrats solennels pour la validité desquels l'établissement d'un acte sous seing privé ou un acte notarié est indispensable. Lorsque la signature est exigée à cet effet, elle représente une véritable règle de forme qui conditionne la validité du contrat et fait partie intégrante du *negotium*.[24] Des exemples de telles exigences formelles sont connus tant des systèmes de la tradition civiliste que de ceux s'inscrivant dans la tradition de la *common law*. Cependant, la présence de la signature comme condition de la validité d'un acte juridique s'inscrit dans le cadre des exceptions au principe général du consensualisme en matière d'obligations.

[44] Le plus souvent, l'exigence de signature est instaurée *ad probationem*, en vue d'établir l'existence de l'acte juridique invoqué.[25] Dans de pareilles circonstances, les défauts de l'*instrumentum*, découlant de l'absence de signature, vont désavantager le plaideur sur le plan probatoire, sans que la validité de l'acte même ne soit remise en cause.[26] Sur le plan probatoire en droit civil, la signature se voit attribuer une signification majeure, parce qu'elle est la seule exigence que le législateur impose à l'acte sous seing privé.[27] En droit civil, la portée du document signé se traduit par la force probante qui y est attachée. Le document s'impose alors au juge et sa mise en cause exige des procédures spéciales. Dans les pays faisant partie de la tradition de la *common law*, la signature

---

[24] *Id.*, p.12

[25] Marc VAN QUICKENBORNE, « Quelques réflexions sur la signature des actes sous seing privé », *R.C.J.B.*, 1985, 68

[26] Étienne DAVIO, « Questions de certification, signature et cryptographie », dans Cahiers du CRID, Namur, CRID, *Internet face au droit*, 1997, 69

[27] Serge PARISIEN, Pierre TRUDEL, *L'identification et la certification dans le commerce électronique*, Cowansville, Yvon Blais, 1996, p. 26

apposée sur un acte invoqué devant le juge, intervient d'abord au stade de l'admissibilité du document en preuve, l'exigence d'authentification de la preuve étant un préalable à sa recevabilité.[28] Avouons tout de même que la signature en *common law* est un moyen parmi d'autres d'authentifier l'acte et ne bénéficie pas en soi de la force probante que les traditions civilistes lui confèrent.

[45] Le bref exposé de l'ensemble de règles juridiques cernant le rôle que le droit attribue au seing manuel circonscrit le contenu du concept d*'institution juridique de signature*. Cet état actuel du droit fut le produit d'un développement historique de plus de 6 siècles. Ce développement a été aiguillé par l'avènement de la place de la signature manuscrite qui s'est avéré être le meilleur moyen pour satisfaire aux besoins impérieux des rapports juridiques – la nécessité d'identifier les auteurs des actes et d'extérioriser leur volonté. Tout en étant motivé par l'efficacité de la signature traditionnelle, le droit n'a pu tenir compte dans son évolution que des particularités du seing manuel comme étant l'unique moyen d'authentification envisageable. Par conséquent, il est possible de soutenir que les caractéristiques de la signature manuscrite prennent une importance majeure sur deux plans : elles sont le facteur de l'essor du seing manuel et ont profondément influencé l'institution juridique de signature.

§ 2. Nature de la signature traditionnelle

[46] Il faut maintenant examiner les particularités de la signature traditionnelle en les envisageant du point de vue des caractéristiques de la marque manuscrite comme telle, de même que sous l'angle de l'essence de la signature, c'est-à-dire, des fonctions qu'elle remplit grâce à ses caractéristiques.

[28] *Id.*, p. 45

a. Caractéristiques de la marque manuscrite

i. La signature manuscrite – tentative de définition

[47] Le besoin n'a pas été éprouvé par le législateur ni par le juge de donner une définition de la signature traditionnelle. Ceci s'explique par le fait que la signature est une notion fort certaine, faisant partie de l'inconscient collectif que la plupart des gens vivent plutôt que ne la pensent. [29] Selon Lamèthe, la signature est essentiellement une notion coutumière.[30] Si nous nous tournons vers son étymologie, le terme signature provient du nom latin *« signum »*, qui réfère au signe, à la marque, à l'empreinte, de même qu'au sceau et au cachet, une signification multiple qui recoupe l'évolution historique connue par la signature.[31] Les tentatives doctrinales de fournir une définition de la signature sont abondantes, mais ne présentent pas une grande diversité, la plupart d'entre elles s'articulant autour des finalités poursuivies par la signature.

[48] Soutenant que la signature est un résultat de la coutume, nous ne pouvons faire référence qu'à des catégories coutumières. Ceci dit, nous remarquons que traditionnellement, trois éléments sont susceptibles de constituer une signature, à savoir le nom, le prénom ou les initiales du signataire. Tout aussi traditionnellement, la signature comme signe représente un graphisme apposé par la main du signataire. Les particularités de la signature en tant que graphisme méritent d'être étudiées parce qu'elles permettent d'assurer les fonctions que la signature remplit.

ii. Particularités du signe

[49] La signature est avant tout un trait. Ce trait se caractérise par des paramètres physiques comme la largeur, la forme et la qualité qui en est l'aspect visuel.[32] Comme le

---

[29] D. MAJDANSKI, *op. cit.,* note 22, p.43
[30] Didier LAMÈTHE, *La signature dans les actes sous seing privé*, Th. Paris II, 1975, p. 2
[31] D. MAJDANSKI, *op. cit.,* note 22, p.44
[32] A. BUQUET, *op. cit.*, note 15, p. 65

trait résulte d'un certain dynamisme, il porte aussi une conduite spécifique, une pression et une tension.

[50] Parmi les plus importantes caractéristiques du seing, il faudrait sans doute mentionner son caractère personnel. Tel que l'écrit le professeur Quickenborne[33], la signature implique « *un graphisme personnel, essentiellement propre au signataire*.» Comme signe personnel, la signature indique des caractéristiques d'un individu faisant en sorte qu'on puisse le reconnaître.[34] Cette qualité de la signature a donné lieu à un débat doctrinal. Selon certains auteurs[35], l'élément personnel de la signature signifierait : « provenant d'une personne déterminée ». Cette perception du caractère personnel vient s'opposer à celle : « provenant d'une caractéristique unique et physique de la personne ou correspondant à cette caractéristique ». Selon cette vision que Syx traite de « dogmatique »,[36] le caractère personnel de la signature est assuré par la combinaison de son contenu traditionnel (le patronyme) et une caractéristique biométrique de la personne, qu'est son écriture.[37] Il existe la croyance empiriquement vérifiée, mais sans fondement théorique, que l'écriture est un paramètre strictement personnel et que deux individus ont nécessairement des écritures différentes.[38] Cependant, notons encore ici, que le caractère personnel de la signature n'est pas une donnée absolue et c'est pour cela que nous adhérons à la vision moins sévère du caractère personnel de la signature - une idée sur laquelle nous reviendrons lors de l'analyse des incertitudes reliées au seing manuel.

[51] Une autre particularité de la signature manuscrite est son caractère inchangeable. Comme l'exprime Davio,[39] la signature « classique » affiche une « belle stabilité ». Fruit de la coutume et datant de longue date, le seing manuel possède la qualité d'être inchangeable, c'est-à-dire, d'avoir toujours les mêmes contenu et technique de réalisation qui en font une donnée « innée ».

[52] Tout en offrant une stabilité particulière quant à son contenu et mode d'exécution, la signature d'une personne déterminée fait preuve d'une variabilité qui en est une caractéristique inhérente. La signature, tout comme l'écriture, varie au cours de la vie en

---

[33] M. VAN QUICKENBORNE, *loc. cit.,* note 25, 81
[34] É. DAVIO, *loc. cit.,* note 26, 67
[35] Dirk SYX, « Vers de nouvelles formes de signature? », (1986) 3 *Droit de l'informatique*, 133, 135
[36] *Id.*, 135
[37] Arnaud-F. FAUSSE, *La signature électronique*, Paris, Dunod, 2001, p. 348
[38] *Id.*, p. 347
[39] É. DAVIO, *loc. cit.,* note 26, 84

fonction des différentes phases d'existence, de même qu'en fonction de l'état du signataire.[40] Étant un acte physique, elle subit les influences des états physiques et psychiques, ainsi que de tout autre facteur de nature humaine.

[53] D'autres capacités propres à la signature traditionnelle sont sa durée illimitée dans le temps et son indépendance par rapport au texte. Même apposée sur un acte ayant une durée de validité, la signature qui en fournit l'authenticité n'est pas en elle-même limitée dans le temps, mais s'appuie sur le contenu du texte pour en déterminer la portée temporelle.[41] La signature est aussi indépendante du texte en terme sémantique.[42] Elle demeure inchangée par rapport au contexte de son utilisation et diffère de la souscription, telle qu'utilisée au Moyen Âge qui elle répètait les conditions d'établissement ou d'acceptation de l'écrit.

[54] Une caractéristique fort importante de la signature classique est sa simplicité. Selon Syx, elle représente un avantage essentiel.[43] La technologie nécessaire à son apposition fait appel à « *la main de quelqu'un qui puisse écrire avec une plume ou quelque chose de similaire* ».[44] La signature peut être aisément utilisée dans les circonstances et les activités les plus diverses. Elle est aussi matériellement un procédé purement visuel, tant au moment de sa création qu'au moment de sa vérification. Grâce à sa nature, elle est aussi vérifiable visuellement ce qui contribue à sa simplicité et représente une autre particularité inhérente au seing manuel.

iii. La maîtrise de l'environnement – une particularité externe

[55] Outre les caractéristiques propres au signe comme tel, nous nous pencherons sur une particularité de la signature qui lui est externe et réfère au contexte de son utilisation, mais qui se trouve en lien immédiat avec la place que le seing privé tient dans la société et en droit. Il s'agit de la maîtrise de l'environnement dans lequel la signature est utilisée. Tel que l'énonce Davio,[45] ce à quoi la signature doit en partie sa place sur le plan probatoire,

---

[40] A. BUQUET, *op. cit.*, note 15, p. 111
[41] A.-F. FAUSSE, *op. cit.,* note 37, p. 349
[42] *Id.*, p. 350
[43] D. SYX, *loc. cit.* note 35, 137
[44] *Id.*
[45] É. DAVIO, *loc. cit.,* note 26, 77

est le fait de la maîtrise préalable de son environnement. Selon Masse,[46] dans le cadre contractuel, la signature n'est pas l'élément déterminant dans l'identification du cocontractant. Dans les rapports contractuels traditionnels des parties, la signature est assistée dans le processus de l'établissement de l'identité du signataire par un ensemble de facteurs dont nous ne saurions sous-estimer l'importance. Parmi ces facteurs il serait pertinent de citer la connaissance physique que les parties ont l'une de l'autre, composée du sexe, de la physionomie et des autres caractéristiques physiques de la personne, y compris la voix, la renommée de la personne et son introduction par des personnes ou sur la base de documents émis par des autorités fiables. La maîtrise préalable de l'environnement est un facteur dont le droit a tenu compte lors de l'élaboration de son attitude vis-à-vis de la signature manuscrite. Quoiqu'une caractéristique étrangère au signe manuscrit comme tel, la maîtrise de son environnement s'avère en liaison importante avec la place que la signature classique a méritée sur le plan juridique.

iv. Les incertitudes liées à la signature traditionnelle

[56] La place que la signature traditionnelle occupe en droit a été déterminée aussi bien par les capacités du signe manuscrit que par les incertitudes qu'il crée. Il serait injustifié d'attribuer à la signature une fiabilité absolue. En revanche, il est légitime de souligner que les incertitudes tout comme les caractéristiques du seing personnel se reflètent dans sa réglementation juridique.

[57] Le caractère personnel physique de la signature, comme nous l'avons énoncé, n'est pas assimilable au caractère physique unique. Selon Syx, il ne fait aucun doute que la signature suppose un acte physique émanant de la personne qui l'effectue[47] sans que ceci associe indubitablement l'auteur au signe. L'examen graphologique ne peut que présumer de l'identité du signataire qui se cache derrière la signature et il ne s'agit ici que d'une probabilité sans qu'il soit question d'un lien absolu entre la signature et le signataire. De surcroît, l'on ne saurait contester la possibilité qu'une personne change de signature ou utilise plusieurs signatures à la fois. Après un examen des caractéristiques de la signature,

[46] David G. MASSE, « L'autoroute de l'information : convergence du droit et de la technologie », Colloque *Faire des affaires en toute sécurité sur les autoroutes de l'information*, 10 novembre 1995
[47] D. SYX, *loc. cit.* note 35, 135

l'observateur ne peut que constater la relativité de la crédibilité de cette donnée. Cette relativité se manifeste aussi sur le plan de la vérification de son authenticité. Syx exprime l'avis qu' « *à moins d'avoir vu de ses propres yeux (et encore) quelqu'un apposer sa signature sur un document écrit bien précis, la signature repose toujours sur une présomption réfutable d'authenticité et de confirmation*. »[48]

[58] Le législateur, conscient de l'impossibilité de la signature d'atteindre une sécurité absolue, s'est abstenu de lui accorder une valeur sacrée. Même en droit civil, où la signature occupe une place probatoire très forte, le législateur a toujours considéré la signature comme un moyen à la crédibilité relative. Rappelons que malgré la force probante attachée à l'acte sous seing privé la contestation de l'acte demeure toujours ouverte. Un autre indice de la certitude relative du droit par rapport au seing privé est l'insuffisance de la signature seule dans certaines circonstances. En effet, le droit exige dans certains cas que la signature soit vérifiée ou confirmée par un notaire ou un autre officier public. Les procédures de légalisation ou de validation des signatures dans les actes de droit international privé fournissent d'autres exemples de cette réserve.

[59] Nous reprenons l'opinion énoncée par Fausse, selon laquelle la fiabilité de la signature manuscrite est scientifiquement faible, mais que l'utilisation que le droit en fait est adaptée à cette faiblesse.[49] En effet le droit, dans sa réglementation de la signature apparaît conscient de ses caractéristiques, que ce soit les atouts de la marque manuscrite qui en ont provoqué l'avènement et l'imposition dans les rapports juridiques ou les faiblesses qui lui sont aussi inhérentes.

b. Les fonctions de la signature traditionnelle

[60] Un aspect important de la nature de la signature tient aux fonctions qu'elle remplit. En effet, il serait logique d'énoncer que les fonctions de la signature traditionnelle sont de répondre aux nécessités des rapports juridiques. Le droit, plutôt indifférent à une définition du signe de la signature comme tel, a, en revanche, démontré un grand intérêt envers les fonctions de la signature et l'a définie selon les finalités qu'elle assure. Pour ce qui est des

---

[48] *Id.*, 137

[49] A.-F. FAUSSE, *op. cit.,* note 37, p. 349

fonctions de la signature, un consensus a été atteint, nonobstant les aspects spécifiques des démarches des pays du droit civil et ceux de la *common law*. Dans le cadre des traditions civilistes, des arrêts des jurisprudences belge et française[50], de même que la définition légale du Code Civil du Québec[51] confirment la position commune sur la question des fonctions de la signature. Aux États-Unis, une abondante jurisprudence, provoquée le plus souvent par l'introduction d'innovations technologiques, met en relief les mêmes finalités.[52]

i. L'identification

[61] Selon le consensus des systèmes juridiques que nous venons de mentionner, la première fonction de la signature est celle d'identification. L'identification permet d'établir juridiquement un lien entre le contenu signé et la personne qui a réalisé le signe.[53] En remplissant sa fonction d'identification, la signature permet d'établir l'origine et la source d'un acte et par-là, de l'attribuer au signataire prétendu ou présumé. L'identification est un impératif indispensable des rapports juridiques car c'est grâce à elle que l'on obtient l'information sur l'auteur d'un acte précis pour ensuite utiliser cette information afin de diriger les conséquences que le droit associe à la réalisation de l'acte. La fonction d'identification de la signature a été, dans certains cas, sous-estimée par les tribunaux américains, les juges prétendant que le lien entre la signature et la personne physique l'ayant apposée n'est pas un préalable à la validité du seing.[54] D'autres insistent sur ce lien stipulant que : « *...a signature's traceability to the signatory [is] very important.* »[55]

---

[50] La chambre commerciale de la Cour de Cassation française adopte résolument une interprétation fonctionnelle de ce concept, Cass. fr. (com.), 2 déc. 1997. Selon la jurisprudence belge formulée au sujet des testaments olographes : « la signature… est la marque manuscrite par laquelle le testateur révèle habituellement sa personnalité aux tiers », Cass., 7 janv. 1955, *Pas*., 1955, I, p. 456.

[51] L.Q. 1991, c. 64, article 2827, (ci-après cité C.c.Q.)

[52] Les fonctions de la signature sont identifiées eu égard aux problèmes invoqués par l'utilisation du télégraphe - *Yaggy v. B.V.D. Co.*, 173 S.E. 2d 496 (N.C. Ct. App. 1970), le télex – *Joseph Denunzio Fruit Co. v. Crane*, 79 F. Supp. 117 (S.D. Cal. 1948), le télécopieur – *Parma Tile Mosaic & marble Co. v. Estate of Short*, 590 N.Y.S. 2d 1019 (Sup. Ct. 1992)

[53] D. SYX, *loc. cit.* note 35, 134

[54] *Hassentaler v. Farzin*, 388 Pa. Super. 37, 564 A. 2d 990 (1989)

[55] Voir Benjamin WRIGHT, *The Law of Electronic Commerce, EDI, Fax, and E-mail: Technology, Proof, and Liability*, Boston, Little, Brown & Co., 1991, p. 293

ii. L'extériorisation du consentement

[62] La deuxième fonction de la signature est la manifestation de la volonté du signataire d'adhérer au contenu de l'acte signé. La démonstration du consentement est désignée intention de signer[56] en common law mais il ne s'agit là que de facettes différentes de la même réalité. Selon Syx[57], la fonction de manifestation de la volonté du signataire se décompose en trois aspects dont la présence est indispensable pour conclure à l'accomplissement de la fonction en question. L'auteur soutient que la signature doit d'abord refléter une manifestation de la volonté. Ce premier élément implique une participation physique du signataire qui par son geste manifeste une volonté personnelle. Cette manifestation doit traduire ou exprimer une appropriation ou un consentement du signataire. C'est dans ce deuxième élément qu'est renfermé *l'animus signandi* – le moment intentionnel qui témoigne de l'attitude du signataire vis-à-vis de l'acte juridique. Troisièmement, ce consentement doit avoir pour objet le contenu de l'acte portant la signature, l'intention doit s'y rapporter et ne concerner que l'essence de l'acte signé.

[63] La signature assure donc la réalisation de ces finalités et, par la suite, elles lui sont assignées comme en étant les fonctions. L'identification des parties et la manifestation de leur volonté sont les besoins des rapports juridiques auxquels la signature a répondu de la manière la plus efficace. Son importance pour l'accomplissement de ces finalités peut être attribué à ses caractéristiques spécifiques. Ce sont donc les particularités de la signature traditionnelle qui l'ont érigée en moyen efficace de satisfaire les nécessités des rapports juridiques et en ont justifié l'avènement.

[64] Une autre caractéristique de la signature classique qui mérite l'attention, est le fait que dans le développement de l'attitude du droit vers la signature, celui-ci s'est inspiré des particularités du signe manuscrit. L'institution de signature, telle que le juriste la connaît aujourd'hui, reflète les capacités de la signature traditionnelle, de même que ses faiblesses. Il ne pouvait en être autrement, vu que le droit a été bâti autour du principal moyen envisageable d'identification et d'extériorisation du consentement qu'était la signature classique. C'est à la fin de cette chaîne logique que viennent les fonctions de la signature que le droit lui a assignées et a définies a posteriori. C'est aussi sur les finalités que la

---

[56] *Id.*, p. 282, *Interstate United Corp. v. White*, 388 F. 2d 5 (10th Cir 1967)
[57] D. SYX, *loc. cit.,* note 35, 134

signature manuscrite assure que le droit s'est basé pour étendre son emprise sur des moyens nouveaux de signature, qui tout en ne possédant aucune analogie même lointaine avec la signature classique, remplissent les mêmes fonctions de manière convaincante et pour cela méritent une place égale à celle du seing privé.

Section II - LA SIGNATURE ÉLECTRONIQUE – LE MOYEN DU MONDE VIRTUEL D'ATTEINDRE LES FINALITÉS DE LA SIGNATURE TRADITIONNELLE

[65] Le développement des moyens modernes de communication et l'expansion du cyberespace posent le problème de l'applicabilité du droit dans des rapports se déroulant dans ce nouvel espace. Ce phénomène a aussi et surtout affecté le processus d'engagement dans le monde virtuel en créant une très sérieuse insécurité juridique quant aux moyens virtuels de conclure et de prouver l'existence des actes juridiques, y compris la signature. Pour remédier à l'incapacité des moyens du monde virtuel à bénéficier du statut juridique du monde papier, le droit a étendu l'emprise de ses institutions à des phénomènes non-traditionnels que la réalité virtuelle avait mis au monde. La signature n'a pas fait exception. Les systèmes législatifs sur lesquels nous nous pencherons ont reconnu la capacité de certaines méthodes produites dans la réalité virtuelle à bénéficier des conséquences juridiques accompagnant la signature traditionnelle, pourvu qu'elles remplissent les fonctions classiques de celle-ci. Ainsi, le droit a-t-il abrité sous l'institution juridique de signature divers nouveaux phénomènes, tout à fait différents de la signature manuscrite. Ces nouveaux phénomènes juridiques ne possèdent qu'une ressemblance avec la signature manuscrite : leur capacité à en assurer les finalités. Pour ce qui est du reste, ces moyens demeurent profondément empreints du monde duquel ils relèvent, le cyberespace.

[66] Dans cette section, nous chercherons à trouver les défis de l'intégration des moyens de signature virtuels dans les systèmes juridiques bâtis autour des réalités du monde physique.

§1. Les fonctions de la signature en droit – le justificatif de la reconnaissance de conséquences juridiques à la signature électronique

a. Accueillir le nouveau phénomène en droit - la voie législative

[67] Il existe quatre voies pour le droit de reconnaître aux techniques modernes d'authentification une valeur juridique comparable à la signature manuscrite, et de se

prémunir ainsi contre l'insécurité menaçant l'engagement en ligne[58]. La première démarche est l'approche interprétative, selon laquelle, se basant sur une analyse fonctionnelle de la signature, il peut être soutenu que même en l'absence de législation expresse, les tribunaux devraient reconnaître aux procédés du cyberespace une valeur égale à la signature manuscrite. Selon la deuxième approche, nommée contractuelle, la valeur juridique peut être octroyée aux moyens virtuels selon le principe de la liberté contractuelle par le consentement des parties. La voie des exceptions a aussi été l'objet du discours juridique.[59] Selon elle, les moyens d'authentification électroniques seraient introduits en droit par le principe des exceptions à la prééminence de leurs contreparties du monde réel. La quatrième voie est la voie législative selon laquelle le droit prend le soin de définir la signature électronique et d'en fixer la valeur. Les réglementations québécoise, européenne et américaine ont préféré cette approche pour exprimer leur position envers la signature électronique. Il faudrait cependant noter que les quatre voies susmentionnées ne sont pas systématiquement des solutions alternatives. La preuve en étant que les législations examinées réfèrent dans leurs définitions de la signature électronique aux fonctions assignées à la signature traditionnelle.

[68] La voie législative peut prendre deux orientations : celle d'une définition large du concept de signature de façon à pouvoir y inclure les formes électroniques ou celle d'une définition spécifique de ce que l'on entend par signature électronique.[60]

i. Définition large de la signature

[69] Un exemple de législation adoptant une définition large de la signature, susceptible d'englober les formes modernes est fourni par le C.c.Q. Selon son article 2827 « [*l*]*a signature consiste dans l'apposition qu'une personne fait à un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante, pour manifester son consentement.* » Cette définition libérale prend en considération les fonctions essentielles de la signature, notamment l'identification et la manifestation de la volonté. Par cette

[58] É. DAVIO, *loc. cit.,* note 26, 72
[59] Yarick COOL, « Signature électronique et signature manuscrite : sœurs ennemies ou sœurs jumelles? », dans Cahiers du CRID, Namur, CRID, *Droit des technologies de l'information,* 1999, 71, 74
[60] É. DAVIO, *loc. cit.,* note 26, 73

définition, le législateur élargit les formes de signature au-delà de la simple transcription du nom.[61] Dans cette rédaction du texte rien ne laisse supposer que seule la signature manuscrite soit exigée. Le libellé de la définition ne s'oppose aucunement à ce qu'une signature aux termes de l'article 2827 C.c.Q. se présente sous une forme électronique dans un environnement informatisé[62], au même titre que d'autres formes de signature moins traditionnelles, telles les initiales, les griffes et les paraphes dans le monde classique. Les auteurs ne trouvaient aucune justification valable d'exclure les signatures informatiques de la définition encore même lorsque l'article du Code apparaissait dans son ancienne version qui référait à une marque apposée sur un acte[63]. Le texte a été encore plus libéralisé et tout doute sur la validité des signatures électroniques dissipé, lorsque l'usage de l'expression *« l'apposition qu'une personne fait sur un acte »* a été remplacée par *« l'apposition qu'une personne fait à un acte »*.[64] Selon la législation en vigueur au Québec, tout moyen est susceptible de bénéficier de la définition légale de signature, y compris ceux du monde virtuel qui remplissent les fonctions inhérentes à la signature.

ii. Définition spécifique de la signature électronique

[70] L'autre voie législative est celle d'une définition expresse de la signature électronique. C'est l'approche de la Directive européenne sur la signature électronique[65] et de l'*Uniform Electronic Transaction Act*[66]. Selon la Directive, la signature électronique est définie de manière très générale et fait appel à une donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification.[67] Les fonctions traditionnelles de la signature peuvent être repérées dans cette définition et il

---

[61] Pierre TRUDEL, Guy LEFEBVRE, Serge PARISIEN, *La preuve et la signature dans l'échange de documents informatisés au Québec*, Québec, Publications du Québec, 1993, p. 65
[62] S. PARISIEN, P. TRUDEL, *op. cit.,* note 27, p. 33
[63] P. TRUDEL, G. LEFEBVRE, S. PARISIEN, *op. cit.,* note 61, p. 83
[64] Précitée, note 10
[65] Précitée, note 9
[66] Uniform Electronic Transaction Act, Approuvé et recommandé à l'adoption par la Conférence Nationale des commissaires du droit étatique uniforme, Conférence Annuelle Denver, Colorado, Juillet 1999, (ci-après citée UETA)
[67] Directive européenne, article 2 (1), précitée, note 9

en découle que les moyens du cyberespace qui possèdent les capacités à les remplir se retrouvent dans le champ de la définition.

[71] L'UETA consacre aussi les fonctions fondamentales de la signature dans sa définition de signature électronique. Selon le texte de l'article 2 (8), la signature électronique peut être un son, un symbole ou un processus électronique qui est attaché ou logiquement associé à un enregistrement et qui est exécuté ou adopté par une personne pour en manifester l'intention de signer. L'élément d'identification, comme dans l'exemple du C.c.Q., peut être déduit de l'exigence que la signature porte un caractère personnel. Pour ce qui est du consentement, cet aspect est expressément explicité par la définition dans sa partie concernant l'intention de signer. Le commentaire officiel accompagnant l'UETA explique que la définition se veut une garantie que la signature peut être réalisée par des moyens électroniques pour autant qu'ils répondent aux exigences contenues dans la norme de l'article 2 (8).

b. Les conséquences juridiques d'une méthode procédurale

[72] Par la suite des modifications normatives dans les cadres législatifs étudiés, les moyens du monde virtuel se voient octroyer la capacité à réaliser des signatures légalement valides. Au niveau de la définition de la signature électronique, nous pouvons aisément remarquer un consensus pour ce qui est de l'approche méthodologique. Il est à noter que le C.c.Q., la Directive européenne et l'UETA ne prévoient pas de changement substantiel du droit régissant et entourant la signature. Pour cette raison leurs approches peuvent être qualifiées de procédurales, car elles étendent la notion de signature au-delà des transcriptions manuscrites sans modifier la substance des normes formant l'institution juridique de signature. En d'autres mots, la signature comme phénomène du droit demeure inchangée, seuls les moyens de la réaliser se modifient.

[73] Nous pouvons facilement imaginer que selon les définitions libérales étudiées, d'innombrables moyens peuvent constituer une signature. Pourvu qu'ils identifient leurs auteurs et manifestent leur consentement par rapport à l'acte signé, les méthodes

satisfaisant aux définitions peuvent varier de combinaisons *cartes et codes*, enregistrements vocaux faits par téléphone[68], et d'initiales apposées au bas d'un message électronique aux processus reposant sur la cryptographie asymétrique réalisés au sein des infrastructures à clés publiques. Ainsi l'institution de la signature s'ouvre à la diversité des moyens du monde virtuel qui ne ressemblent à la signature manuscrite que par le fait qu'ils servent aux mêmes finalités que le droit lui a assignées.

[74] Le droit a évolué et a été bâti pendant des siècles sur la base de la signature manuscrite, tout en reflétant les caractéristiques et les faiblesses du seing manuel et que les formes nouvelles de signature ont été introduites dans un système qui leur est étranger et dont le développement se fondait sur des réalités différentes, relevant d'un monde différent du milieu de réalisation des marques informatiques. Alors, est-il justifié de soutenir qu'intégrer un phénomène nouveau dans une catégorie existante voudrait aussi dire adapter cette catégorie à la nouveauté du phénomène? Selon nous les différences entre les moyens nouveaux de signature et les réalités sur lesquelles le droit a construit ses catégories sont trop profondes pour considérer qu'il existe une équivalence entre le fait d'intégrer les nouvelles méthodes d'authentification en droit d'une part et adapter le droit de la signature aux réalités virtuelles d'une autre.

[75] Dans les pages qui suivent, nous nous pencherons sur les différences entre les signatures traditionnelle et modernes pour analyser les problèmes que ces différences posent et le besoin d'adaptation qui émerge.

[68] UETA, Commentaires, précitée, note 66

§ 2. Prise en considération des variétés des moyens de signature électronique

a. Le fondement des divergences entre les deux types de signatures - les différences entre le monde réel et le monde virtuel

i . Les moyens modernes de signature – produits du cyberespace

[76] Étant donné que le droit s'est tourné vers les fonctions de la signature au lieu de rester attaché à une conception dogmatique faisant appel à la forme, il est évident que de nombreux moyens du monde informatique peuvent valablement prétendre occuper une place dans la définition de signature. Une des caractéristiques de la signature électronique est l'énorme variété de formes sous lesquelles elle peut se présenter. Il est extrêmement difficile d'englober toutes les signatures électroniques possibles dans une seule catégorie qui en révèlerait toutes les particularités. Dans la recherche des différences entre les deux types de marques nous avons d'un côté une donnée relativement stable et, de l'autre, une variété non circonscrite de formes. Tout de même, il est opportun d'énoncer que tous les moyens d'authentification nouvellement créés, et à l'être, portent une caractéristique qui leur reste toujours commune, nonobstant leurs différences. Cette caractéristique réfère à leur provenance du monde virtuel - le cyberespace, c'est la seule caractéristique commune de nature formelle qu'elles possèdent susceptible de servir d'appui dans la comparaison entre la catégorie des signatures électroniques et celle de la signature manuscrite.

[77] Les particularités du cyberespace préoccupent la pensée juridique lorsque le monde virtuel soulève à nouveau des questions que le droit a déjà eu le souci de régler dans le monde réel. La signature ne fait pas exception. L'adaptation du droit aux moyens nouveaux de signature fait donc partie de la question plus fondamentale de l'adaptation du droit au cyberespace ou, en d'autres mots, de la problématique de la régulation du cyberespace.

ii. Le rôle et la cause des différences entre le monde réel et le cyberespace

[78] Tout comme la signature électronique, d'autres institutions juridiques ont été mises à l'épreuve par les caractéristiques du monde virtuel. Prenons, à titre d'exemple, le droit d'auteur, les institutions juridiques relatives à la liberté d'expression, la diffamation, le droit international privé, la divulgation et la cueillette d'informations, etc. Dans tous ces cas, soit au stade de la recherche d'une réglementation appropriée, soit dans la résolution d'un litige, les juristes se sont penchés sur la question des particularités du cyberespace sans hésiter à en reconnaître l'importance majeure en droit.

[79] Dans une des premières affaires concernant Internet aux États-Unis[69], les avocats et les juges ont ciblé leur attention sur la nature du cyberespace pour y puiser leurs affirmations. Le Solliciteur Général Adjoint Waxman, au nom du Gouvernement, a énoncé l'opinion selon laquelle Internet se rapprochait du concept d'une bibliothèque. Waxman a exprimé cet avis en relation avec la question de l'application du *Communications Decency Act*. Selon le juge Breyer, Internet ressemblait plus aux communications téléphoniques, alors que pour les juges O'Connor et Kennedy le réseau s'identifiait surtout comme un « coin de rue » ou un parc.[70] Ce jugement n'est pas le seul exemple des tentatives de circonscrire la nature et les particularités du cyberespace et il démontre l'intérêt particulier dont les juristes ont fait preuve pour les caractéristiques du monde virtuel lorsqu'il s'avérait le théâtre d'activités sur lesquelles le droit avait déjà statué. Les particularités du cyberespace se sont vues reconnaître la place d'une des réalités les plus importantes dans la résolution des questions juridiques.

[80] Comme l'explique Stuart Biegel[71], « *it is virtually impossible for anyone to view today's Internet as anything other than « different » »*. L'auteur fournit une argumentation abondante à l'appui de cette affirmation et conclut en désignant la source des différences entre le monde réel et le cyberespace. Selon Biegel, Internet doit sa nature unique à son architecture, aux particularités des activités en ligne, de même qu'aux changements dans les modes de vie qui en découlent.

---

[69] *Reno v. ACLU*, 521 U.S. 844 (1997)

[70] Stuart BIEGEL, *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace*, Cambridge, MIT Press, 2001, p. 27

[71] *Id.*, p. 31

[81] Cependant, même si un consensus auquel nous adhérons sans hésitation, a été atteint quant à l'existence de différences et de leur importance majeure pour le droit, un débat juridique demeure quant à la nature et la profondeur desdites différences. Soucieux de caractériser les différences entre les signatures traditionnelle et électroniques, nous présenterons les principaux courants de ce discours portant sur la profondeur des disparités entre les mondes réel et virtuel. La profondeur des différences illustrera le degré d'inadaptation du droit qui nous intéresse ici.

iii. La nature et la profondeur des différences

[82] Le premier courant est celui en faveur de la vision traditionaliste du cyberespace. Selon cette conception Internet n'est pas un endroit autre que le monde réel, mais fait bien partie de la réalité physique. Eugene Volokh[72], un des représentants de ce courant d'idées, s'oppose à l'affirmation que les ordinateurs vont changer profondément la façon dont nous pensons le droit, nous l'appliquons ainsi que son rôle dans la société.[73] Les traditionalistes reconnaissent l'importance significative des nouvelles technologies, mais ils ne voient comme résultat qu'un changement modeste dans la réglementation. Au sujet des droits d'auteur, Volokh rejette l'idée que la réglementation de la propriété intellectuelle soit inappropriée aux rapports survenus avec l'apparition d'Internet[74], soutenant que l'existant en droit est également applicable aux environnements statiques (ceux du monde réel) et aux environnements dynamiques (que sont les nouveaux médias). Au sujet du commerce électronique, ces commentateurs soulignent qu'il ne diffère pas au point de nécessiter une nouvelle réglementation de sa contrepartie ancienne[75]. Ils cherchent même à trouver des analogues entre les transactions en ligne et des exemples connus au monde réel, telles les ventes par catalogues.

[83] Une deuxième vision du cyberespace est la position *modérée* adoptée par plusieurs auteurs. Ils considèrent les différences que l'environnement virtuel renferme, mais ne vont

---

[72] Eugene VOLOKH, « Technology and the Future of Law », *Stanford Law Review*, 47 (1995), 1375
[73] *Id.*
[74] *Id.*
[75] Jane Kaufmann WINN, « Open Systems, Free Markets, and Regulation of Internet Commerce », *Tulane Law Review* 72 (1998), 1177

pas jusqu'à définir le cyberespace comme une zone temporellement et physiquement différente (la troisième conception du cyberespace). Selon la vision modérée, au moins certains aspects du cyberespace diffèrent résolument à cause des particularités de l'architecture, du design et du type d'activités que cet univers abrite. Ces différences sont causées par la combinaison de caractéristiques uniques qui marquent les réseaux virtuels. Les disparités entre le monde réel et l'espace virtuel peuvent s'exprimer par des différences conceptuelles, des différences légales ou des différences physiques. Des exemples de la conscience de ces réalités peuvent être retrouvés dans l'affaire *Digital Equipment Corporation v. Alta Vista Technology*[76], dans laquelle la juge Gertner a exprimé l'opinion que l'analyse juridique des nouvelles questions peut nécessiter de nouveaux paradigmes. Dans cette affaire le concept de *territoire* était mis à l'épreuve, alors que dans l'affaire *Thomas*[77], le concept à réviser était celui de communauté et de standards communautaires.

[84] Lawrence Lessig adhère à cette vision modérée des caractéristiques du cyberespace, le considérant comme un endroit distinct et similaire en même temps. Il soutient que le monde virtuel existait déjà en 1920, un argument pour le considérer plutôt comme un endroit faisant partie du monde réel.[78] Lessig avoue cependant qu'à l'heure actuelle les gens vivent de nombreuses expériences dans le cyberespace.[79] Il accorde une importance régulatrice déterminante à son architecture[80]. Toujours au sein du courant *modéré*, David Post met l'accent plus sur la composante « espace » du cyberespace.[81] Il souligne le caractère séparé et autonome de cet environnement.

[85] Tout en reconnaissant les spécificités de l'environnement électronique, les supporteurs de la conception *modérée* se distinguent du troisième courant dans le discours concernant la profondeur des différences du cyberespace. Ce troisième courant admet la position que les environnements modernes représentent une zone séparée tant temporellement que géographiquement. Leur conception provoque une réaction de rejet de toute tentative de

---

[76] *Digital Equipment Corporation v. Alta Vista Technology Inc.*, 960 F. Supp. 456 (1997)
[77] *U.S. v. Thomas*, 74 F. 3d. 701 (6th cir. 1996)
[78] L. LESSIG, *loc.cit.,* note 5, 872
[79] Lawrence LESSIG, « Surveying Law and Borders : the Zones of Cyberspace », *Stanford Law Review* 48 (1996), 1367
[80] L. LESSIG, *op. cit.,* note 8
[81] David R. JOHNSON, et David G. POST, « Law and Borders: The rise of Law in Cyberspace », *Stanford Law Review* 48, (1996), 1403, 1407

réglementation des activités se déroulant sur Internet.[82] Assez caractéristique à cet effet est l'expression de Barlow: *« Cyberspace does not lie within your borders…you do not know our culture, our ethics…We are forming our Social Contract*. »[83]

[86] Les trois courants circonscrivent les différences entre le monde réel et l'environnement virtuel et les enjeux en découlant pour le droit. Ce débat est intéressant, parce que la question des différences entre la signature manuscrite et les signatures électroniques fait écho à la question plus large que les auteurs se sont posée. Ainsi, le débat général peut être concrétisé et ciblé sur des aspects du problème de la signature électronique. Dans les pages qui suivent nous nous pencherons sur la question des similitudes ou des différences entre les moyens traditionnels et modernes de signer et sur leur importance pour l'institution juridique de signature.

b. Différence de la signature électronique avec sa contrepartie traditionnelle

[87] Les trois positions vis-à-vis de la nature et de la profondeur des différences entre l'espace réel et le cyberespace peuvent être identifiées lorsqu'il s'agit du monde virtuel pris dans son ensemble. Tout de même, comme l'explicite Biegel[84], si nous examinons les phénomènes différents, les activités individuelles se déroulant dans le cyberespace, le débat général peut s'avérer inutile. L'auteur soutient que les trois positions trouvent une application selon les particularités concrètes de l'architecture et de l'activité sur une base individuelle, au cas par cas. Par exemple, en déterminant les règles sur la propriété intellectuelle dans le cyberespace, il doit être tenu compte de l'aisance avec laquelle les objets de la protection peuvent être copiés dans le monde en ligne et celui hors ligne. Il en va de même pour la protection de la vie privée, la liberté d'expression, etc. Selon cette approche, il peut apparaître que certains phénomènes dans le cyberespace ne sont pas totalement différents de leurs contreparties du monde physique et les conclusions des traditionalistes apparaissent plus appropriées. Dans d'autres cas, on peut constater de telles

---

[82] S. BIEGEL, *op. cit.,* note 70, p. 38

[83] John Perry BARLOW, « A Declaration of the Independence of Cyberspace », *Electronic Frontier Foundation*, source http://www.eff.org/~barlow/Declaration-Final.html, visitée en mai 2002

[84] S. BIEGEL, *op. cit.,* note 70, p. 39

différences qu'elles appellent la démarche du courant *modéré*. Il n'est pas exclu que les spécificités de certaines activités soient à ce point différentes que le phénomène puisse constituer une réalité virtuelle séparée. Dans ce cas, les idées de Barlow trouveraient un fondement juste.

[88] L'idée de Biegel d'envisager le cyberespace comme un ensemble d'environnements d'activités plutôt que comme un tout, nous paraît justifiée lorsqu'il s'agit d'identifier les particularités et les différences qui intéressent le droit. Le problème des différences entre la signature traditionnelle et les signatures électroniques doit être examiné sous cet angle. Les spécificités de la signature électronique ne devraient pas être envisagées sous l'angle d'une différentiation généralisée entre le monde en ligne et celui hors ligne, mais méritent l'analyse individualisée d'un environnement autonome au sein du concept de cyberespace. Par conséquent, même si aucun des trois courants susmentionnés ne s'applique de façon générale, ils peuvent prétendre, tous les trois, à une pertinence dans le domaine des signatures électroniques.

[89] En appliquant les idées des trois conceptions au phénomène de la signature électronique trois conclusions sont possibles. D'abord, on peut croire qu'entre les deux types de signatures il n'existe que des différences insignifiantes qui autorisent une approche régulatrice identique et inchangée, ce qui représenterait une position traditionaliste. Cependant si l'existence de différences est constatée au plan conceptuel, légal et substantiel, le phénomène nécessiterait une réglementation sous l'angle de la vision modérée. La troisième solution serait de considérer les moyens d'authentification comme une réalité totalement différente, comme un phénomène n'ayant aucun point commun avec le phénomène du monde réel auquel on tente de l'assimiler.

[90] Dans ce premier chapitre nous avons identifié les fonctions que la signature manuscrite remplit. Il a aussi été vu que la signature électronique sert les mêmes finalités. Dans ce contexte force est de constater l'identité des résultats auxquels l'apposition d'une signature traditionnelle et l'application d'une méthode électronique nous mènent. Dans les deux cas, l'identification du signataire et la démonstration de sa volonté de s'approprier le contenu de l'acte seront assurées. Cette ressemblance est d'une importance majeure, mais notons tout de même qu'elle est aussi la seule. À part cela, l'architecture et la nature de l'activité (les deux aspects qui ont préoccupé les auteurs lors de la résolution des questions des différences entre le monde réel et le monde virtuel) qui nous mènent à

l'accomplissement de ces finalités sont totalement différentes. Dans cette optique, il semble qu'en matière d'authentification le cyberespace et le monde réel font preuve de disparités considérables. La différence des moyens appelle sans doute à être prise en compte dans la position que le droit adopte vis-à-vis du phénomène des signatures électroniques, une des activités qui, ensemble, bâtissent le cyberespace.

c. Les conséquences – l'inadaptation du droit et le besoin d'un correctif

[91] L'identité entre les fonctions que la signature traditionnelle et son équivalent électronique remplissent a donné lieu à des définitions légales de signature électronique. Moyennant ces définitions, les méthodes du monde virtuel se sont vues reconnaître les capacités de la signature manuscrite de produire des effets juridiques. Dès lors, on peut validement apposer une signature par les moyens qu'offre le cyberespace, l'utiliser pour former un contrat valide et l'invoquer dans un litige. Les problèmes de la validité et de la recevabilité en preuve sont ainsi résolus et l'insécurité juridique a été surmontée. Ce sont les résultats atteints par le biais des définitions de signature en l'absence de modification substantielle du droit, plus particulièrement de l'institution juridique de signature.

[92] En d'autres termes, la signature électronique a été accueillie sous l'empire de l'institution juridique de signature. Notons cependant la différence décisive entre l'acte d' « accueillir » un phénomène en droit et celui d' « adapter » le droit audit phénomène. Nous avançons trois arguments à l'appui de l'inadaptation du droit à la signature moderne.

[93] Premièrement, rappelons l'absence de modification substantielle de l'institution juridique de signature. L'ensemble des normes qui circonscrivent l'importance juridique de la signature a été étendu pour couvrir les nouveaux moyens d'authentification sans être substantiellement modifié. Les dispositions qui déterminent les conséquences que le droit lie à l'utilisation de la signature demeurent inchangées que ce soit vis-à-vis des signatures traditionnelles ou informatiques.

[94] Deuxièmement, l'institution juridique de signature a été développée et a évolué compte tenu de la seule forme de signature envisageable qu'était la signature manuscrite. Vu que le seing privé est souvent appelé « signature traditionnelle » ou « classique », ces deux qualifications méritent l'attention car elles désignent une caractéristique importante de

la signature. Comme nous l'avons démontré dans ce premier chapitre, le droit a reflété l'ensemble des caractéristiques spécifiques du seing manuel, prenant en considération tous ses aspects de même que les certitudes et les incertitudes que la signature manuscrite crée.

[95] Troisièmement, il faudrait certes rappeler la profondeur et la nature des différences entre les deux phénomènes, découlant des différences des architectures et de la nature des activités.

[96] Dans ce contexte, le besoin émerge de trouver un moyen par lequel le droit s'ajustera à la nouvelle réalité qu'il a accueillie sous son empire. Le droit a donc créé un nouveau paradigme. L'institution juridique de signature recourt à un nouveau concept qu'est *la fiabilité* de la signature électronique. Ce concept, dont le droit se désintéressait par rapport à la signature manuscrite, intervient pour servir de correctif à l'intégration de la signature électronique dans un environnement juridique qui lui est, on peut le dire, étranger. La création de ce nouveau paradigme, la référence au standard de fiabilité, représente le moyen de réconcilier le paysage juridique et la réalité nouvelle. Le standard de fiabilité traduit parfaitement les particularités de l'architecture et de l'activité propres à la signature électronique et permet de les prendre en considération lors de la résolution des questions soulevées en droit.

[97] Dans le prochain chapitre nous examinerons la manière dont ce correctif intervient en droit en situant le standard de fiabilité dans la réglementation des capacités probatoires de la signature électronique.

CHAPITRE II – L'AJUSTEMENT DU RÉGIME DE LA PREUVE - LES RECOURS DU DROIT AU STANDARD DE FIABILITÉ DES PROCÉDÉS ÉLECTRONIQUES DE SIGNATURE

[98] Nous avons adhéré à l'opinion de Biegel[85] selon laquelle le droit doit appréhender sous différents angles les activités survenant dans le cyberespace plutôt que de considérer le monde virtuel de manière généralisée. Nous pouvons aller encore plus loin et soutenir que la différentiation doit être aussi de rigueur au sein même d'une seule activité. Ainsi, la signature en tant qu'institution juridique est un ensemble de normes qui consacre les règles se rapportant aux nombreux usages du seing manuel. Dans ce contexte, il serait hasardeux de soutenir que toutes ses utilisations dans le cyberespace aboutissent au même degré d'inadaptation du droit. Lorsque l'on s'interroge sur la validité du seing en tant que prérequis à la validité de l'acte juridique, le simple recours aux fonctions traditionnelles de la signature – l'identification du signataire et la démonstration de son adhésion à l'acte - suffit à l'inclusion des technologies du cyberespace dans le paysage juridique. Cependant, dans le cas de la détermination de la valeur probante d'une signature, lorsque sa capacité à établir un lien entre le seing et son auteur ou entre la signature et l'acte auquel elle se rapporte, y compris sa capacité à maintenir l'intégrité de cet acte, est mise à l'épreuve, les moyens qu'offre le cyberespace diffèrent sensiblement de ceux du procédé traditionnel auquel la réglementation se conformait jusqu'alors. Dans ce cas, c'est la capacité probatoire de la signature électronique qui requiert un ajustement de l'institution juridique.

[99] En cas de litige, après être déclarée recevable[86], la signature est prise en considération par le juge pour lui fournir des informations sur l'identité des parties et leur adhésion au contenu du document[87]. Elle n'influencera pas forcément la décision du juge, l'obligation de celui-ci ne consistant à ce stade qu'à étudier l'élément en question.

---

[85] *Id.*
[86] Y. COOL, *loc. cit.,* note 59
[87] Chris REED, « What is a Signature? », *The Journal of Information, Law and Technology* (3), 2000, source: http://elj.warwick.ac.uk/jilt/00-3/reed.html, visitée en mai 2002

[100] Différents systèmes juridiques et de différentes hypothèses à l'intérieur de ces systèmes, se distinguent selon l'influence qu'a la signature sur l'opinion du juge. Dans un premier groupe d'approches, la signature s'impose au juge pour ce qui est de l'existence des faits qu'elle est censée étayer, tandis que dans d'autres, l'évaluation de sa valeur probante lui est tout simplement confiée.

[101] Le droit recours au standard de fiabilité des procédés d'authentification virtuels afin d'intégrer la signature électronique dans le juridique. L'appel au standard de fiabilité du procédé de signature constituera le moyen pour le droit d'ajuster l'institution de la preuve à l'usage des signatures modernes. Il remplit les fonctions de correctif entre le juridique et les nouveaux phénomènes.

Section I – LE STANDARD DE FIABILITÉ COMME RÈGLE DE DROIT, L'INTRODUCTION DU STANDARD DE FIABILITÉ DANS LA RÉGLEMENTATION DE LA SIGNATURE ÉLECTRONIQUE PAR LES LOIS-TYPE DE LA CNUDCI

[102] Le concept de standard juridique, selon le sens que notre étude lui attribue, fait appel à une règle de droit. Ainsi, le standard est une disposition qui fait partie de l'ensemble normatif régissant un phénomène ou un groupe de rapports. Lorsque nous référons au standard de fiabilité en matière des moyens électroniques de signature, nous envisageons une règle de droit faisant partie de l'encadrement juridique de la signature électronique. Si les règles du droit formant l'institution de signature déterminent les conséquences juridiques associées à l'usage de la signature, le standard de fiabilité précise l'application de ladite institution aux moyens électroniques de signature. Il serait justifié de dire que l'application même du droit de la signature en matière de signature électronique s'effectue à la lumière d'une règle de droit, mettant en avant la fiabilité des moyens de signature électroniques, que nous appelons standard de fiabilité. Vincent Gautrais réfère à ce standard

comme à un ensemble d'éléments techniques attachés à la signature[88]. Nous adhérons à une telle affirmation, parce que le standard de fiabilité est de par sa nature une règle juridique qui possède cependant un contenu essentiellement technique.

[103] L'intervention du standard de fiabilité se remarque dans les dispositions concernant la signature électronique résultant des travaux de la CNUDCI, notamment la *Loi type sur le commerce électronique*[89]*, la Loi type sur les signatures électroniques*[90], ainsi que *L'avant-projet de convention sur les contrats électroniques*[91]. L'article 7, alinéa 1 (b) de la Loi type sur le commerce électronique dispose :

> *« 1. Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données :*
>
> *a) Si une méthode est utilisée pour identifier la personne en question et pour indiquer qu'elle approuve l'information contenue dans le message de données; et*
>
> *b) Si la fiabilité de cette méthode est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris de tout accord en la matière. »*

[104] La disposition est reprise littéralement dans l'article 6, alinéa 1 de la *Loi type sur les signatures électroniques* et l'article 13, alinéa 3 (b) de *l'Avant-projet de convention*. Les règles démontrent la présence du standard de fiabilité dans l'application des normes de l'institution de signature aux moyens électroniques.

[105] Après s'être attaché aux deux fonctions essentielles d'une signature, à savoir l'identification de l'auteur d'un document et la confirmation que l'auteur approuve la teneur dudit document (alinéa 1 (a)), la Loi type sur le commerce électronique impose une exigence de fiabilité du moyen électronique de signature. Aux termes de l'alinéa 1 (b) la méthode utilisée en vertu de l'alinéa 1 (a) devrait être aussi fiable que cela est approprié au vu de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de

---

[88] Vincent GAUTRAIS, «Le contrat électronique au regard de la Loi concernant le cadre juridique des technologies de l'information», dans Vincent GAUTRAIS (dir.), *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002, 43

[89] Adoptée par la Commission des Nations Unies pour le droit commercial international en 1996 (ci-après citée Loi type sur le commerce électronique)

[90] Adopté par la Commission des Nations Unies pour le droit commercial international le 5 juillet 2001 (ci-après citée Loi type sur les signatures électroniques)

[91] A/CN.9/WG.IV/WP.95, Trente-neuvième session New York, 11-15 mars 2002 (ci-après cité Avant-projet de convention)

toutes les circonstances, y compris tout accord entre l'expéditeur et le destinataire du message de données.

[106] En effet, l'exigence de fiabilité instaurée par l'alinéa 1 (b) porte sur la manière dont les moyens de signature électronique garantissent la capacité de la signature d'accomplir ses fonctions, objets de l'alinéa 1 (a). L'application de l'institution de signature aux signatures électroniques s'avère donc dépendante de deux conditions: l'exigence que la signature électronique remplisse les fonctions inhérentes à la signature traditionnelle d'une part, et le besoin que ces fonctions soient accomplies de manière fiable. La deuxième de ces règles conditionnant l'application du droit de la signature en matière de signature électronique introduit le standard juridique de fiabilité.

[107] Pour ce qui est de l'identification du standard, le paragraphe 58 du Guide d'application de la loi type énonce trois groupes de facteurs à prendre en considération. Ces groupes contiennent plusieurs paramètres permettant de juger de la fiabilité et d'appliquer le standard. Pour déterminer si la méthode utilisée en vertu de l'alinéa 1 est appropriée, des facteurs juridiques, techniques et commerciaux doivent être pris en considération. Le guide cite parmi les critères techniques le degré de perfectionnement du matériel utilisé par chacune des parties, la capacité des systèmes de communication, les procédures d'authentification proposées par les opérateurs des systèmes de communication, la série de procédures d'authentification communiquée par un intermédiaire. Dans la catégorie des facteurs de nature commerciale, la loi s'intéresse à la nature de l'activité commerciale, la fréquence avec laquelle s'effectuent les opérations commerciales, la nature et l'ampleur de l'opération, l'observation des coutumes et pratiques, l'existence de mécanismes d'assurance contre les messages non autorisés, l'importance et la valeur de l'information contenue dans le message de données, etc. Finalement au plan des facteurs juridiques le statut et la fonction de la signature dans un régime législatif et réglementaire donné doivent être pris en compte.

[108] Il est certain que lorsqu'il s'agit de mesurer les capacités des moyens électroniques de produire des signatures fiables (tel que le standard de fiabilité institué dans l'article 7, alinéa 1 (b) l'exige), se sont les critères d'ordre technique qui détermineront la substance du standard de fiabilité. En revanche, les facteurs juridiques et commerciaux indiqueront la rigueur que l'application du standard nécessite.

[109] Ainsi, à l'intersection du droit de la signature et ces moyens électroniques de signature intervient le standard de fiabilité des moyens de signature électronique. Ce standard représente un complément de règles techniques lié à l'encadrement normatif de la signature électronique. L'approche de la CNUDCI peut être retrouvée dans plusieurs cadres législatifs concernant la convergence du droit et des technologies en matière d'authentification. Le standard de fiabilité demeure toujours présent malgré les différences dans ses manifestations et rôles qu'il joue.

Section II – L'EXIGENCE DE FIABILITÉ DANS LA RÉGLEMENTATION DE LA FORCE PROBANTE DE LA SIGNATURE ÉLECTRONIQUE

[110] Dans la majorité des cas, les systèmes de droit civil accordent à la signature manuscrite une force probante, notion sous laquelle il faudrait plutôt entendre la force probante de l'acte sous seing privé.[92] Selon ces systèmes, la signature manuscrite jouit d'une capacité prédéterminée à servir de preuve des révélations qu'elle prétend établir. Cette capacité qui est préalablement consacrée par les dispositions légales, s'impose à la conviction du juge[93]. Ce statut de la signature implique aussi une procédure spéciale de mise en cause de sa capacité probante. La prééminence de l'écrit est expliquée dans la doctrine par la haute valeur sécuritaire de l'écrit, caractérisé par sa permanence et une signature dans laquelle l'auteur se reconnaît.[94]

[111] Les cadres législatifs reconnaissent aux signatures informatiques la possibilité de s'intégrer dans ce contexte juridique et, par-là, de bénéficier de plein droit de la force probante accordée à la signature traditionnelle. Cependant, un critère supplémentaire est

---

[92] Etienne WÉRY, Thibault VERBIEST, *Le droit de l'Internet et de la société de l'information: droits européen, belge et français*, Bruxelles, Larcier, 2001, p. 343

[93] Aux termes du Code civil français l'acte sous seing privé a entre ceux qui l'ont souscrit et entre leurs héritiers, la même foi que l'acte authentique – article 1322. Le Code civil du Québec dans son article 2828 énonce que l'acte sous seing privé opposé à celui qui paraît l'avoir signé ou à ses héritiers est tenu pour reconnu s'il n'est pas contesté. La norme de l'article suivant dispose que l'acte sous seing privé fait preuve, à l'égard de ceux contre qui il est prouvé, de l'acte juridique qu'il renferme et des déclarations des parties qui s'y rapportent directement. Les dispositions du Code civil belge sont similaires – article 1322.

[94] E. WÉRY, T. VERBIEST, *op. cit.,* note 92, p. 333

ajouté dans la réglementation de la force probante de la signature électronique, la prise en considération de la fiabilité de son procédé de création. Il s'agit d'une notion inconnue à l'institution de la force probante des signatures manuscrites. Les législateurs font usage du standard de fiabilité pour adapter le régime civiliste du statut probatoire des signatures manuscrites aux nouveaux phénomènes du cyberespace.

§ 1. L'attribution d'une force probante aux technologies de signatures électroniques fiables

a. L'exigence de fiabilité des signatures non-traditionnelles selon le C.c.Q.

[112] Dans la définition de l'article 2827 du C.c.Q. les fonctions traditionnelles de la signature sont exposées. Selon les dispositions du code, un document signé électroniquement sera recevable en preuve dans l'hypothèse où un écrit signé manuscritement était jusqu'alors exigé. Cependant, pour bénéficier de la valeur probante accordée à l'acte sous seing privé, il faudra, au cas par cas, faire la preuve que le mécanisme utilisé constitue une marque personnelle qui permet d'identifier le signataire avec une certitude raisonnable ainsi que la manifestation de son consentement, la charge de la preuve incombant à celui qui invoque l'acte signé[95]. Pour ce faire, l'on cherchera à prouver la fiabilité du mécanisme de signature et l'authenticité de la signature litigieuse. Cette affirmation de Montéro trouve ses fondements dans le commentaire que font les professeurs Trudel, Parisien et Lefebvre de la norme de l'article 2827. Selon eux, « *la recherche de l'intention manifeste du législateur nous porte à croire que l'expression « une marque personnelle qu'elle utilise de façon courante » suppose, que cette marque soit susceptible de permettre l'identification d'une personne. Par conséquent, on doit sans*

[95]Didier GOBERT, Étienne MONTERO, « La signature dans les contrats et les paiements électroniques: l'approche fonctionnelle »**,** dans Cahiers du CRID, Namur, CRID, *Commerce électronique*, 2000, 17, 19

doute considérer comme répondant aux critères de l'article 2827, une marque qui permet d'identifier une personne avec une raisonnable certitude »[96].

[113] L'exigence d'« une raisonnable certitude » avec laquelle la signature doit remplir ses fonctions nous paraît justifiée. Elle est à notre avis une manifestation du standard de fiabilité. Nous soutenons aussi que cette exigence ne s'applique qu'aux signatures non-traditionnelles. Cette affirmation se justifie par la réglementation antérieure au C.c.Q. Selon la jurisprudence et la doctrine québécoises d'avant l'adoption du C.c.Q., qui reprennent d'ailleurs le discours du droit français, la signature doit être manuscrite.[97] Cette exigence d'une forme particulière ne cohabitait pas avec une condition supplémentaire de « raisonnable certitude » ou quelque autre émanation du standard de fiabilité, la forme manuscrite étant suffisante. Dans ce contexte il faut noter que l'article 2827 du C.c.Q. n'a pas été adopté dans le but de remettre en cause les capacités de la signature manuscrite, mais afin de libéraliser la définition de signature en l'élargissant. Si le standard de fiabilité n'est intervenu qu'au moment de l'adoption de la nouvelle définition de signature, cela montre que cette intervention a été provoquée par l'innovation que la nouvelle définition apporte, notamment l'autorisation de formes de signature autres que le seing manuel. Par conséquent, nous pouvons légitimement conclure que la fiabilité de la signature s'est dégagée comme condition dans le texte de l'article 2827 C.c.Q. à cause de l'élargissement de la définition de signature à des formes non-traditionnelles et ne concerne que ces formes. Si nous appliquons cet argument dans le sens inverse, une autre conclusion s'impose. La réglementation antérieure au *Code civil* ne s'est pas tournée vers une exigence de fiabilité de la signature manuscrite non pas parce qu'elle s'en désintéressait, mais parce qu'elle trouvait des garanties de cette fiabilité dans la forme même de la signature.

[114] Rappelons aussi que le C.c.Q. a choisi de définir largement la signature pour autoriser les signatures non-traditionnelles au lieu de les définir séparément. Dans ce contexte le législateur ne pouvait pas instaurer un critère supplémentaire de fiabilité se rapportant uniquement aux signatures nouvelles. Tout de même, il est certain que l'exigence de « raisonnable certitude » n'interviendra que lors de l'appréciation de la force probante des signatures autres que traditionnelles. C'est dans la catégorie des signatures

---

[96] P. TRUDEL, G. LEFEBVRE, S. PARISIEN, *op. cit.,* note 61, p. 92
[97] *Id.*, p. 64

électroniques que ce critère supplémentaire se rajoute et prend le rôle de préalable à l'octroi d'une force probante équivalente à celle de la signature manuscrite.

[115] L'interprétation doctrinale de l'article 2827 du CCQ à laquelle nous adhérons sans a été réaffirmée par la disposition de l'article 39, al. 2 de la Loi sur le cadre juridique des technologies de l'information. Le texte ajoute des critères pour que la signature apposée à un document technologique soit opposable à son auteur : l'intégrité du document doit être assurée; et le lien entre la signature et le document doit être maintenu. Ces critères ne s'appliquent qu'aux seuls documents technologiques qui, évidemment, ne peuvent porter que des signatures électroniques. Par conséquent, la signature électronique renfermant une certitude raisonnable pour ce qui est de l'accomplissement de ses fonctions et répondant aux impératifs d'opposabilité de l'article 39, al. 2 de la Loi bénéficiera, sur un pied d'égalité avec son analogue traditionnel, de la capacité d'attribuer à l'acte, auquel elle est apposée la qualité d'acte sous seing privé et à lui conférer une force probante. Encore, pour intégrer de plein droit les moyens informatiques d'authentification au sein de la réglementation de la preuve, le droit fait référence à des conditions supplémentaires inconnues à l'usage de la signature traditionnelle, qui représentent des manifestations du concept plus large de fiabilité des procédés de signature électronique.

[116] L'exigence de fiabilité du procédé de signature électronique se profile de la même manière dans le Code civil belge.[98] L'article 1322, complété par un nouvel alinéa, requiert que la signature électronique puisse être imputée à une personne déterminée et établisse le maintien de l'intégrité du contenu de l'acte. Sous ces conditions, le moyen d'authentification informatique se voit accorder le statut de l'article 1322, c'est-à-dire la capacité supérieure probatoire dont la signature traditionnelle bénéficie.

[98] Tel que modifié par la Loi introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, Moniteur belge, 20 Octobre 2000

b. La condition de fiabilité imposée par le législateur français

[117] Le recours à la fiabilité du moyen de signature électronique au plan de la preuve est encore plus explicite en droit français. Le Code civil[99] prend le soin de régir les signatures informatiques dans une disposition séparée. La définition de signature est contenue dans la nouvelle rédaction du premier alinéa de l'article 1316-4 du Code civil français. Selon cette définition la signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations de cet acte. Le second alinéa de l'article définit la signature électronique comme suit :

> *«Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.»*

[118] L'ajout de l'exigence supplémentaire de fiabilité est clairement destiné aux seules signatures électroniques. Les fonctions que les signatures doivent remplir sont définies dans le premier alinéa et concernent les moyens tant traditionnels que nouveaux. Il ne fait aucun doute que pour servir à la perfection d'un acte, c'est-à-dire pour lui attribuer le statut d'acte sous seing privé, la signature manuscrite ne doit se conformer qu'aux exigences du 1er alinéa de l'article 1316-4. Ceci ne change d'ailleurs aucunement la position qu'occupe la signature traditionnelle dans le régime de la preuve. En revanche, il en est autrement dans le cas de la signature électronique. Tout en se voyant allouer les mêmes effets par la suite des fonctions qu'elle remplit, elle doit se conformer à des exigences supplémentaires. Pour servir à la perfection d'un acte, la signature électronique doit être réalisée à l'aide d'une méthode garantissant une identification fiable du signataire et un lien fiable entre la signature et l'acte auquel elle se rapporte. L'exigence de fiabilité est déterminante pour que les procédés électroniques obtiennent la force probante des seings manuscrits.

[119] Lue dans le contexte du titre de la loi, l'exigence de fiabilité des procédés de signature électronique s'avère un nouveau paradigme auquel le droit français a eu recours

---

[99] La France a adopté le projet de Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, J.O. Numéro 62 du 14 Mars 2000, page 3968, qui modifie le Code civil.

pour ajuster l'institution juridique de signature aux particularités des nouvelles méthodes d'authentification.

§ 2. Les présomptions de fiabilité de certaines technologies

a. La codification du standard de fiabilité par les clauses d'assimilation de la Directive européenne

[120] Même avant l'adoption de la Directive[100], le besoin d'une présomption de fiabilité faisant en sorte que le juge confère une force probante aux signatures électroniques et qu'il les considère, grâce à la garantie de leur fiabilité, comme des équivalents de la signature manuscrite, a été ressenti.[101] La Directive introduit cette présomption en adoptant une double approche vis-à-vis de la signature électronique. Tout en préconisant dans ses clauses de non-discrimination, une définition large et technologiquement neutre de la signature électronique, l'acte européen introduit également le concept de « *signature électronique avancée* »[102] qui se trouve à la base des clauses d'assimilation. Selon cette clause, une force probante, comparable à celle des signatures traditionnelles, est allouée aux signatures électroniques avancées qui satisfont à certains impératifs. Pour qu'elle réponde aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite y répond sur papier, la signature électronique avancée doit, aux termes de l'article 2 (5), reposer sur un certificat qualifié et doit être réalisée par un dispositif sécurisé de signature, dont la description détaillée fait l'objet de l'Annexe III de la Directive. Les dispositions qui mettent en fonction la clause d'assimilation sont des garanties de fiabilité du moyen de la signature électronique assimilée. Ainsi, pourrions nous conclure que les clauses d'assimilation de la Directive représentent une présomption de

---

[100] Précitée, note 9

[101] E. WÉRY, T. VERBIEST, *op. cit.,* note 92, p. 339, D. GOBERT, É. MONTERO., *loc. cit.,* note 95, Y. COOL, *loc. cit.,* note 59

[102]La signature électronique avancée est décrite par l'article 2 (2) de la Directive comme répondant aux exigences suivantes : a) être liée uniquement au signataire; b) permettre d'identifier le signataire; c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

fiabilité de certaines techniques, suite à laquelle la signature résultante se voit accorder une force probante équivalente à celle de la signature traditionnelle.

[121] Trois types de garanties, développés en détails, doivent entourer la signature électronique avancée pour qu'elle puisse bénéficier de la présomption : des assurances de fiabilité du certificat[103] sur lequel elle repose, des garanties de fiabilité du prestataire de services de certification (ci-après PSC) qui l'émet[104], de même que des indices de fiabilité du dispositif de création de signature[105]. Chacune de ces garanties est assurée par un ensemble d'exigences détaillées. La fiabilité du certificat, par exemple, suppose l'identification précise du titulaire et la description des moyens de vérification et de réalisation de la signature[106], ainsi que le maintien de cette précision au cours du cycle de vie du certificat[107]. La fiabilité du PSC implique, selon la Directive, la fiabilité de l'entreprise comme telle[108], sa fiabilité financière[109], la fiabilité des ressources humaines[110], la fiabilité de la gestion des certificats[111], etc. Les dispositifs de création de signature sont aussi entourés d'impératifs, exposés dans l'Annexe III de la Directive afin d'en assurer le fonctionnement infaillible.

[122] Il n'est pas nécessaire d'exposer les détails des annexes de la Directive pour conclure que ses conditions d'assimilations s'articulent de manière indéniable autour du concept général de fiabilité de la technologie de signature électronique. La fiabilité est incontestablement la condition supplémentaire de l'attribution aux signatures modernes du statut probatoire renforcé de leurs contreparties traditionnelles. Ainsi, le droit de la preuve s'applique à la signature électronique sous réserve d'une exigence additionnelle, d'un correctif qui est législativement instauré pour en ajuster les dispositions aux nouveaux phénomènes du monde virtuel. Le nouveau paradigme en matière de preuve écrite adaptée à la réalité virtuelle qu'est la signature électronique, est un recours au standard de fiabilité de sa technique de réalisation. Grâce à la référence à la fiabilité, les normes du droit de la

---

[103] Directive européenne, Annexe I, précitée, note 9
[104] *Id.,* Annexe II
[105] *Id.,* Annexe III
[106] *Id.,* Annexe I (e), (g), (h)
[107] *Id.,* Annexe I (f)
[108] *Id.,* Annexe II (a)
[109] *Id.,* Annexe II (h)
[110] *Id.,* Annexe II (e)
[111] *Id.,* Annexe II (b), (c), (d), (g), (i)

preuve, peuvent trouver une pleine application dans le domaine de la signature électronique.

b. La présomption de fiabilité en droit français

[123] Comme nous l'avons vu, en droit français, la question de la valeur probante de la signature électronique se résout à l'angle de la fiabilité. À cet effet la loi française instaure, elle-aussi, une présomption. Aux termes du dernier alinéa de l'article 1316-4, « *...La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décrets pris en Conseil d'État* ».

[124] Le Décret[112] qui vient cerner les manifestations du concept de fiabilité, prévoit dans son deuxième article que la fiabilité de la signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en oeuvre une signature électronique sécurisée[113], établie grâce à un dispositif sécurisé de création de signature électronique[114] et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié.[115] Les conditions qui rendent la signature fiable sont identiques à celles dont fait état la Directive européenne. Le Décret prévoit aussi une possibilité de reconnaissance de la conformité des prestataires de services de certification avec les exigences énoncées à leur sujet. L'article 7 dispose que les prestataires de services de certification électronique qui satisfont aux exigences fixées à l'article 6, peuvent demander à être reconnus comme qualifiés et que cette qualification vaut présomption de conformité aux dites exigences. Récemment est paru l'arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation.[116] L'arrêté pose les conditions de reconnaissance de la qualification des

---

[112] Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique : J.O. Numéro 77 du 31 Mars 2001, page 5070 (ci-après cité le Décret)
[113] Concept développé dans l'article 1er, al. 2 du Décret
[114] Le Décret, chapitre 1er, précité, note 112
[115] *Id.*, article 6
[116] Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation - J.O. Numéro 132 du 8 Juin 2002

prestataires de services de certification. Selon l'arrêté, le PSC qui demande à être reconnu comme qualifié devra choisir un ou plusieurs organismes accrédités qui effectueront l'évaluation des services qu'il propose. L'évaluation a pour objet de vérifier que les services offerts par le prestataire respectent les exigences fixées par l'article 6 du décret du 30 mars 2001 ainsi que les normes, les prescriptions techniques et les règles de bonne pratique applicables en matière de certification électronique. A l'issue de l'évaluation, l'organisme accrédité établit un rapport sur la conformité du prestataire ouvrant la voie à sa qualification. Ce régime de reconnaissance facilite la preuve de la conformité aux exigences du Décret et, par-là, de la fiabilité du prestataire.

[125] Pour ce qui est des dispositifs de création de signature, ils doivent être évalués et certifiés aux termes de l'article 3 (2). Notons tout de même que cette démarche de la loi française n'est qu'une voie, parmi d'autres, permettant d'apporter la preuve de la fiabilité requise sans prétendre déterminer le contenu général du standard de fiabilité. La présomption en droit français facilite la preuve de la fiabilité et réaffirme la place et le rôle du concept dans l'intégration des moyens d'authentification virtuels dans l'institution de signature en droit.

c. La possibilité de présomption de fiabilité selon l'article 8 de la Loi concernant le cadre juridique des technologies de l'information du Québec

[126] Nous interpréterons les articles 2827 C.c.Q. et 39 de la *Loi concernant le cadre juridique des technologies de l'information* relatifs au statut juridique de la signature à la lumière de la faculté offerte par le législateur d'instituer une présomption de fiabilité des moyens technologiques (article 8 de la même loi). Il s'agit ici d'un pouvoir conféré au gouvernement de décréter qu'un dispositif, un mécanisme ou un procédé, est apte à remplir une fonction déterminée. Dans les annotations accompagnant la loi sur le site Web du

Ministère de la culture et des communications[117], le but de la disposition est élucidé. L'objectif est d'éviter que les parties soient obligées de faire la preuve devant un tribunal qu'un certain dispositif, pourtant conforme à des normes reconnues par des instances nationales ou internationales, est effectivement en mesure de remplir une fonction déterminée. Dans le cas de la signature électronique, ceci signifierait que l'utilisation de certaines techniques, que le gouvernement a reconnues aptes aux termes de l'article 8, dispenserait de l'obligation de prouver que les conditions de l'article 2827 C.c.Q. et les critères d'opposabilité (article 39) sont satisfaits. Il s'agit donc d'une présomption de fiabilité du moyen de signature électronique.

[127] Les dispositifs visés par l'article 8 méritent ce statut probant renforcé, grâce à leur aptitude à remplir leurs fonctions ou, en d'autres mots, grâce à leur fiabilité. Aux termes de l'article 68 de la loi, le Gouvernement, dans son appréciation des capacités des dispositifs fondant la présomption de l'article 8, doit être guidé par la reconnaissance qui en est faite par des organismes de normalisation reconnus.[118]

[128] Le législateur québécois a recours à une démarche qui par sa nature se rapproche des présomptions européennes et qui confirme l'importance du standard sur le plan probatoire.

[129] Ainsi, le statut probatoire de la signature électronique en droit européen et québécois est conditionné par la preuve de la fiabilité de son processus de genèse. L'analyse des clauses d'assimilation de la Directive européenne et leurs contreparties dans certaines législations nationales[119], de même que les normes similaires dans le contexte du droit québécois, nous mène à la conclusion que les législateurs ont souhaité établir un lien ferme entre, d'une part, les effets juridiques de la signature sur le plan probatoire et, d'autre part, la fiabilité du procédé utilisé et de tout l'environnement de genèse et de vie de la signature électronique. Il est à noter que les législateurs européens, désireux de dispenser le juge de la tâche d'évaluer la fiabilité de la signature électronique, mettent en place des présomptions qui s'avèrent attachées à une technologie particulière, notamment celle de la cryptographie

---

[117] Ministère de la culture et des communications, Autoroute de l'information, « Loi concernant le cadre juridique des technologies de l'information (L.Q.2001, c.32) », *Texte annoté par article*, source : http://www.autoroute.gouv.qc.ca/loi_en_ligne/loi/annindex.html, visitée en mai 2002

[118] La loi cite notamment la Commission électrotechnique internationale (CEI), l'Organisation Internationale de normalisation (ISO), l'Union internationale des télécommunications (UIT), le Conseil canadien des normes et le Bureau de normalisation du Québec.

[119] Le droit belge repose sur la même prémisse aux termes de l'article 4 (4) de la Loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, Moniteur belge, 9 Juillet 2001

asymétrique mise en fonction au sein des infrastructures à clés publiques. Par ailleurs, il est douteux que le législateur désirant présumer une aptitude concrète de la signature électronique, puisse demeurer technologiquement neutre.

[130] Il serait tout de même légitime de soutenir, que derrière cette approche technologiquement spécifique, nous devrions voir un désir non pas de sanctionner un profil particulier de signature électronique, mais de mettre l'accent sur une caractéristique fort importante des moyens d'authentification du monde virtuel – leur fiabilité. Rien ne s'oppose à ce que la preuve de la fiabilité du procédé soit établie dans des cas non couverts par les présomptions. En effet, il n'existe pas d'obstacle à la preuve qu'une signature électronique est suffisamment fiable, aux termes de l'article 1316-4 du Code civil français, sans recourir à une technologie dont la fiabilité est législativement reconnue. Il en va de même de la preuve de la fiabilité dans le cadre des articles 2827 du C.c.Q. et 39 de la loi du Québec, laissant la possibilité de choisir entre une technologie présumée fiable par l'administration et toute autre. Il est vrai que la preuve est sensiblement facilitée par les effets des présomptions, mais la fiabilité comme standard possède toujours la même importance et représente une catégorie large et indépendante, nonobstant les moyens d'en apporter la preuve.

[131] Ainsi, les législateurs européens et québécois attachent la force probante des signatures électroniques à la présence d'un groupe de facteurs qui bâtissent dans leur ensemble le standard de fiabilité. De cette manière, la place des moyens du monde virtuel dans le paysage juridique de la signature et, par-là, l'égalité en droit de la preuve des signatures traditionnelles et modernes, s'avère sujette à la mise en place d'un nouveau paradigme juridique qu'est le recours au standard de fiabilité. Cette notion réaffirme encore une fois son rôle qui est, dans le cas particulier, de concilier les institutions juridiques et les réalités nouvelles.

§ 3. Le discrédit de la fiabilité de la technologie – une voie supplémentaire de contestation de la force probante de la signature électronique

a. La contestation de la force probante de l'acte sous seing privé transposée aux signatures électroniques

[132] La contestation de la force probante de la signature traditionnelle est un aspect important de sa participation sur le plan probatoire. Elle est régie par un ensemble de normes qui seraient sans conteste applicables dans le cadre de la mise en cause des capacités des signatures virtuelles. Cependant, pour rendre ces normes opérationnelles dans le contexte du monde virtuel, le besoin se fait sentir de recourir à de nouveaux outils de vérification de la signature, c'est-à-dire, l'assurance qu'elle identifie l'auteur de l'acte et qu'elle traduit son consentement audit acte.

i. La contestation de la signature dans le monde papier

[133] Le législateur a fini par considérer la signature écrite comme une donnée relativement crédible.[120] La signature, qui jouit de la capacité législativement prescrite de déterminer la conviction du juge, peut toujours être contestée. L'article 1323 du Code civil français dispose que celui à qui l'on oppose un acte sous seing privé est obligé d'avouer ou de désavouer formellement son écriture ou sa signature. Le Code de procédure civile décrit la procédure de vérification de l'écriture.[121] Il en va de même pour les dispositions régissant la procédure de contestation en droit belge.[122] Le processus d'examen de l'écriture ou de la signature est régi par les articles 883 et suivants du code judiciaire belge.[123]

---

[120] D. SYX, *loc. cit.* note 35, 136

[121] Article 287 du Nouveau Code de procédure civile : « Si l'une des parties dénie l'écriture qui lui est attribuée ou déclare ne pas reconnaître celle qui est attribuée à son auteur, le juge vérifie l'écrit contesté à moins qu'il ne puisse statuer sans en tenir compte… »

[122] Code civil belge, article 1324

[123] Le juge peut, dans cet objectif prendre toutes mesures d'instruction utiles, tels la confrontation du document contesté et d'autres documents dont l'authenticité est établie, l'imposition d'une épreuve écrite ou l'obligation de la partie qui nie sa signature de l'apposer un certain nombre de fois à titre d'essai. Le juge peut avoir recours à une preuve testimoniale quant à la rédaction de la signature contestée.

[134] Le C.c.Q dans son article 2828 énonce que l'acte sous seing privé opposé à celui qui paraît l'avoir signé ou à ses héritiers est tenu pour reconnu s'il n'est pas contesté. La procédure de contestation est prévue dans l'article 89 du Code de procédure civile qui prescrit : « *Doivent être expressément alléguées et appuyées d'un affidavit : 1. la contestation de la signature ou d'une partie importante d'un écrit sous seing privé…* » C'est dans cette procédure que peut être vérifié si la signature identifie le signataire avec une certitude raisonnable et si elle est une véritable preuve de l'expression de son consentement par rapport à un acte concret et précis. Les dispositions régissant la contestation de la signature ont donné lieu à une jurisprudence abondante. Les principes de la contestation de la signature peuvent en être extraits et ils s'appliqueront sans doute dans le cas de la contestation de la signature électronique.

[135] D'abord, la dénégation de la signature en droit québécois doit être marquée par une certitude. Dans l'affaire *Central Pontiac Buick Ltée c. Poirier*[124] l'objectif du législateur a été clairement interprété. Selon le juge, le législateur a été très précis à l'article 89. Il a employé l'adverbe « expressément », ce qui signifie, selon le Petit Robert : « *explicitement, nettement, précisément* ». Ainsi, selon la cour, une chose faite expressément, c'est une chose faite délibérément, volontairement, avec une intention spéciale.[125]

[136] Par la suite, si le désaveu est retenu, celui qui invoque la signature doit en faire la preuve. La jurisprudence a déterminé qu'elle peut se faire par des témoins instrumentaires, c'est-à-dire qui ont eux-même signé l'acte, par des témoins ordinaires qui ont vu signer l'acte, par des témoins ordinaires qui n'ont pas vu signer l'acte mais qui reconnaissent la signature ou par des experts[126]. La preuve de la signature dans la procédure de contestation doit être faite dans un contexte empreint de fiabilité. Lorsqu'elle procède à l'examen de la preuve de la signature, la Cour a toujours scruté la fiabilité de cette preuve, dans le cas en l'espèce, les conclusions de l'expert. Dans l'affaire *Bolduc c. Talbot*[127] le juge est convaincu par la conclusion de l'expert à cause de sa fiabilité et de la fiabilité de la méthode utilisée : « *L'experte (…) a préparé un rapport écrit très détaillé et bien articulé. (…) A l'audition, elle a témoigné avec précision, professionnalisme et conviction. Elle n'a*

---

[124] [1997] A.Q. no 709

[125] Voir aussi *Kahn c. Toronto Dominion Bank*, [1997] A.Q. no 61: « La preuve à l'appui de la négation de signature doit être sérieuse, cohérente et vraisemblable. Il ne suffit pas pour une personne de tout simplement nier que ce soit sa signature sur l'écrit; il lui faut dire pourquoi. »

[126] *Armand v. Checotel Finance Corp*., [1985] Q.J. No. 40

[127] *Bolduc c. Talbot*, QCCQ, 25 octobre 2001

pas été contredite. Son opinion est crédible. Le processus utilisé par cette graphologue confère à cette expertise une fiabilité indéniable… »

[137] Il ne fait aucun doute que les dispositions législatives concernant la mise en cause de la force probante de la signature s'appliqueront à l'emploi des moyens modernes. Leurs finalités sont de fournir une certitude que la signature correspond véritablement aux faits prétendus. Les formalités entourant la contestation des signatures traditionnelles et modernes demeureront dans les deux cas inchangées.

[138] Afin de se prémunir contre l'incertitude quant à l'authenticité de la signature, la Cour a toujours mis de l'avant et scruté des preuves fiables. Cependant, notre recherche n'a pas permis de retrouver de jurisprudence où un juge se serait interrogé sur la fiabilité de la signature traditionnelle en tant que procédé en soi. Ceci semble normal et le fait de le mentionner peut paraître inutile si l'on ne prend pas en considération le changement résultant de l'introduction en droit de la preuve des signatures virtuelles.

ii. Une voie supplémentaire et incontournable – le discrédit de la fiabilité de la technique de signature électronique

[139] Dans le contexte de la contestation de la signature électronique nous remarquons l'ouverture d'une nouvelle voie. La signature manuscrite a mérité son statut probatoire supérieur grâce à ses caractéristiques intersèques. Nous pourrions même dire que les dispositions consacrant une force probante à la signature ont suivi le développement et l'imposition du seing manuel. Il en est cependant tout autrement pour ce qui est des moyens de signature électronique. Comme nous l'avons observé, sur ce point, ils jouissent de la pleine équivalence avec la signature manuscrite sous condition - nouveau paradigme en droit - de leur fiabilité. Vu que le droit se penche sur la fiabilité des procédés de signature électronique pour en déterminer la valeur probante, le recours à la fiabilité trouverait aussi une place méritée dans le contexte de la contestation de cette valeur.

[140] De cette manière, le droit gouvernant les capacités probantes des signatures se voit compléter par une nouvelle réalité, inconnue jusqu'à présent. Lorsque la force probante des signatures manuscrites est mise à l'épreuve, la procédure ayant pour but de retrouver le vrai auteur de l'acte n'avait pas l'ambition, et d'ailleurs ne pouvait pas, viser l'examen de la

fiabilité du seing manuel. Le juge cherchait à s'assurer si, en l'espèce, la signature provenait de la personne prétendue avec toutes les conséquences en découlant sans s'interroger sur la capacité générale de la signature en soi d'identifier le signataire et d'en manifester le consentement. Dans le cas de la signature électronique en revanche, l'attention peut, et doit être portée sur les capacités du procédé comme tel. La fiabilité du moyen de signature électronique occupe par la suite une place déterminante sur le plan de la contestation de la force probante dans le sens où le discrédit de sa fiabilité offre des nouvelles vois de dénégation des signatures.

b. La contestation de la présomption de fiabilité – un moyen de discrédit de la fiabilité

i. La réfutation de la présomption de fiabilité selon la Directive et la loi française

[141] Comme la preuve de la fiabilité des signatures informatiques peut recourir à l'application de présomptions, le discrédit de la fiabilité peut être engagé par le biais de la contestation desdites présomptions. Par exemple, la contestation de la signature aux termes de l'article 1223 du Code Civil français, dans le cas des signatures électroniques présumées fiables, s'articulerait autour du discrédit de la fiabilité ayant donné lieu à l'assimilation.

[142] Le Décret français pose des conditions assurant la création d'un environnement technologique permettant à la signature de remplir ses fonctions sans défaillance. Les conditions du Décret concernent les trois éléments de la signature assimilée – son caractère sécurisé, sa réalisation grâce à un dispositif sécurisé de création de signature électronique et sa vérification qui repose sur l'utilisation d'un certificat électronique qualifié. Dès lors, la procédure de compromission de la fiabilité de la signature électronique peut s'engager dans les voies de la compromission de chacun de ses trois éléments. Celui qui veut prouver que la signature n'est pas une manifestation fidèle de la réalité, peut choisir d'établir qu'elle n'est pas sécurisée, c'est-à-dire soit qu'elle n'est pas propre au signataire, soit qu'elle n'est pas créée par des moyens que le signataire a gardé sous son contrôle exclusif ou qu'elle ne garantit pas avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable. Ce n'est là qu'une des possibilités de contester la force probante de la

signature, car l'exigence qu'elle soit sécurisée ne représente qu'un des préalables à l'assimilation.

[143] Celui qui conteste l'authenticité de la signature peut aussi invoquer des défauts du dispositif de création, prétendant qu'il n'est pas sécurisé. Il peut chercher à compromettre les qualités du dispositif en affirmant que les exigences de l'article 3 - I ne sont pas satisfaites ou que le dispositif en question n'est pas certifié.

[144] Le certificat qualifié qui est à la base de la vérification de la signature est une autre condition à la présomption de sa fiabilité. La fiabilité du certificat peut être attaquée par l'affirmation qu'il ne répond pas aux exigences de l'article 6 - I du Décret[128] ou bien par une preuve que le PSC l'ayant délivré ne satisfait pas aux exigences fixées à l'article 6 - II. La compromission de chacune des conditions serait en mesure de discréditer le certificat et, par-là, la fiabilité de la signature, et fournirait donc des fondements à sa contestation. Nous mentionnerons à titre d'exemple que le dépassement du montant maximal autorisé pour les transactions d'un certificat[129] ou bien la sous-estimation des procédures de sécurité[130], pourrait être des voies possibles pour la procédure de contestation de la signature. En conclusion, il est important de souligner que les exigences de l'article 6 (premier alinéa a – i, et deuxième alinéa a – p) cherchant à garantir la fiabilité du moyen de signature fournissent également les possibilités de compromission du procédé et de contestation de la force probante de la signature.

ii. Réfuter la présomption de l'article 8 de la loi québécoise

[145] Comme nous l'avons vu, aux termes de l'article 8 de la loi québécoise, un mécanisme peut être déclaré apte à remplir une fonction déterminée. Sur le plan de la signature électronique, une procédure particulière peut se voir reconnaître la capacité à identifier le signataire, à prouver son consentement[131] en préservant l'intégrité du document et le maintien du lien entre la signature et l'acte[132]. Ainsi, la signature résultant de cette technique reconnue se verrait accorder un statut équivalent à celui de la signature

---

[128] Le Décret, précité, note 112
[129] *Id.,* article 6 - I (i)
[130] *Id.,* article 6 - II (f)
[131] C.c.Q., article 2728
[132] L.C.C.J.T.I ., article 39, al. 2, précitée, note 10

manuscrite, sans qu'il soit besoin d'en prouver les capacités et d'en convaincre le juge. Dans ce contexte, la contestation de la capacité d'une signature électronique de bénéficier du statut privilégié de l'article 8 de la loi se fera à travers la compromission de la fiabilité des dispositifs visés.

[146] La reconnaissance en vertu de l'article 8 se base sur des standards techniques développés au niveau national et international. Il serait difficile, voire impossible d'attaquer la crédibilité et la fiabilité des dispositifs reconnus. Ceci signifierait affronter la fiabilité des normes et des standards ayant gagné le consensus des communautés concernées au niveau national et international. Cependant, l'assurance de la fiabilité des normes et des standards n'ôte pas la possibilité de prouver que, dans une application particulière ou dans un cas concret, le dispositif a été mal implémenté, mal utilisé ou a mal fonctionné[133]. Cette possibilité de contestation de la fiabilité des signatures électroniques reste ouverte et consiste en la contestation de la fiabilité dans une application concrète, au delà de la fiabilité du dispositif comme tel.

[147] En conclusion nous rappellerons que le droit de la preuve dans les systèmes de droit civil accorde à la signature traditionnelle un statut spécial qui s'exprime en sa capacité, législativement prescrite, d'emporter la conviction du juge sur les faits qu'elle établit, de même qu'en la procédure spécifique de contester ces faits. Dans le monde virtuel, le droit a affronté le besoin de régir cette activité particulière pour adapter les institutions juridiques le législateur a eu recours à des notions nouvelles dont la présence se révèle sur le plan de la réglementation de la force probante des signatures électroniques. Le recours à l'examen de la fiabilité des procédés informatiques d'authentification est une manifestation concrète des moyens auxiliaires du droit de s'ajuster aux phénomènes de la réalité virtuelle, étrangers à son évolution.

[133] Ministère de la culture et des communications, *op.cit.,* note 117

Section III – LE POUVOIR DISCRÉTIONNAIRE DU JUGE D'APPRÉCIER LA VALEUR PROBANTE DE LA SIGNATURE À TRAVERS LA FIABILITÉ DE SA TECHNOLOGIE

[148] Les hypothèses sous lesquelles la signature électronique peut voir sa valeur probante librement appréciée par le juge sont présentes tant dans les systèmes de droit civil qu'en *common law*. Premièrement, certaines techniques de signature électronique ne répondent pas aux exigences des clauses qui assimilent la signature électronique à la signature manuscrite, dites *clauses d'assimilation,* et mettant les deux moyens de signature sur un pied d'égalité sur le plan probatoire en droit civil. Dès lors, les signatures issues de telles techniques auraient une valeur probante qui demeurerait dépendante de la libre décision du juge.

[149] Le juge détient un pouvoir discrétionnaire quant à l'évaluation des capacités de la signature dans les systèmes de *common law*. Traditionnellement en *common law*, le problème de la capacité de la signature à établir le lien avec le signataire et le document se pose d'abord au stade de l'admissibilité du document en preuve. De plus, la signature n'est pas, en elle-même, suffisante pour prouver l'authenticité de l'acte. Ses capacités et sa valeur probante sont appréciées par le juge et le jury sans qu'il soit imposée une force probante à ces derniers.

[150] Dans les contextes ainsi décrits, nous exposerons les principes d'évaluation de la valeur probante des signatures, pour souligner parmi eux la place essentielle du critère de fiabilité.

§ 1. Les hypothèses de détermination discrétionnaire de la valeur probante de la signature en droit civil

a. La place des clauses de non-discrimination – principe ou exception dans la détermination de la valeur probante des signatures électroniques?

i. Les clauses de non-discrimination – une confirmation de la position législative envers les techniques fiables

[151] L'article 5 (2) de la Directive européenne dispose :

> *« Les États membres veillent à ce que l'effet utile d'une signature électronique et sa recevabilité comme preuve en justice ne soient pas contestés au seul motif que la signature se présente sous forme électronique, ou qu'elle ne repose pas sur un certificat qualifié, ou qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire de service de certification accrédité, ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature. »*

[152] En Belgique, cette disposition est transposée par l'article 4 par. 5 de la Loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification.[134]

[153] Les clauses de non-discrimination entrent en jeu lorsque les conditions auxquelles est soumise l'application des clauses d'assimilation ne sont pas rencontrées.[135] La non-discrimination affirme le principe de recevabilité en preuve des signatures électroniques. Toutefois, il appartiendra toujours à celui qui se prévaut seulement de la clause de non-discrimination de convaincre le juge de la valeur probante. À la différence de la situation créée par l'application de la clause d'assimilation, la signature, selon la clause de non-discrimination, ne bénéficie pas de l'équivalence automatique avec la signature manuscrite. Par conséquent, la signature électronique qui ne satisfait pas aux conditions de la clause d'assimilation, ne bénéficie pas du régime probatoire plus favorable. Elle ne peut pas être rejetée par le juge au seul motif qu'elle n'est pas manuscrite, mais il appartiendra toujours à

---

[134] Précitée, note 117
[135] E. WÉRY, T. VERBIEST, *op. cit.,* note 92, p. 343

la personne qui l'invoque d'apporter la preuve de la fiabilité de la technique utilisée pour établir le respect des critères posés par les articles qui consacrent les fonctions de la signature.

[154] Les clauses de non-discrimination représentent le deuxième volet de la double approche adoptée par le législateur européen. S'agit-il cependant d'un deuxième volet, d'une voie exceptionnelle pour intégrer en droit des signatures autres que celles bénéficiant des présomptions et des clauses d'assimilation? Rappelons que l'objectif des présomptions de fiabilité est strictement de faciliter la preuve des capacités de la signature électronique. La tendance du droit demeure toujours de recourir à l'examen de la fiabilité des moyens d'authentification modernes et d'en tirer des conclusions quant à leurs capacités probantes. Dans ce cadre juridique, les présomptions et les clauses d'assimilation doivent certainement être considérées comme des voies spécifiques d'apporter la preuve de cette fiabilité sans être vues comme une règle générale. Par les clauses de non-discrimination le principe est incontestablement réaffirmé que la valeur probante de la signature électronique est fonction de sa fiabilité. Ce ne sont que les moyens de la prouver, ses formes et ses manifestations qui varient.

ii. La perception erronée de la nature de l'exigence de fiabilité dans Chalets Boisson S.A.R.L. c. Gros

[155] Nous avons soutenu que le but de la loi française est d'attribuer une force probante comparable à celle des signatures traditionnelles aux signatures informatiques fiables. Ceci représente la règle générale du Code civil français. Le législateur français a aussi prévu un moyen de faciliter la preuve de la fiabilité exigée par l'institution d'une présomption dont le contenu est précisé par les dispositions d'un Décret du Conseil d'État. Notons cependant que ce Décret n'a pas pour objectif de sanctionner l'usage d'une technologie particulière. Il se limite uniquement à dispenser le juge de l'appréciation de la fiabilité de la signature électronique dans les cas ou le signataire a choisi d'utiliser le procédé légalement considéré fiable.

[156] Dans l'affaire *Chalets Boisson S.A.R.L. c. Gros*[136] la cour devait évaluer la fiabilité d'un moyen électronique de signature, plus concrètement, celle résultant de l'apposition à un document de l'image numérique d'une signature manuscrite. Il faut également rappeler qu'au moment du litige, les termes du Décret n'étaient pas encore connus. La Cour d'Appel de Besançon examine la possibilité d'appliquer les règles du Décret et conclue à leur inapplicabilité, selon nous, tout à fait légitimement. À notre avis cependant, la Cour arrive au bon résultat, mais pas à l'aide des bons moyens. La décision de la Cour de rejeter l'application du Décret est justifiée, mais l'argument n'est pas approprié. Le juge dispose que le Décret n'est pas en vigueur, et qu'il est donc inapplicable. Si le Décret avait une force légale, cela voudrait-il dire que le juge y aurait eu recours pour apprécier la fiabilité d'un moyen électronique de signature reposant sur la technologie du balayage optique de la surface d'un document ou sur toute autre technologie? Les dispositions du Décret sont, selon nous, inappropriées aux faits d'espèce, ce qui devrait représenter en effet le vrai fondement de leur non pertinence et de leur inapplicabilité.

[157] La Cour semble s'être tournée vers les normes du Décret pour en puiser des critères d'appréciation de la fiabilité des signatures électroniques, nonobstant les formes qu'elles peuvent emprunter. Cependant le but du Décret est de fournir le contenu d'une présomption de fiabilité ne concernant qu'une forme concrète de signature électronique, réputée répondre à un ensemble d'exigences.[137] Ses dispositions déterminent les conditions dans lesquelles une signature électronique basée sur la cryptographie à clés asymétriques est présumée fiable et dont la conformité avec la première phrase de l'article 1316-4 du Code civil n'a pas à être prouvée. Le Décret du Conseil d'État donne le contenu la présomption de fiabilité, il ne fournit pas les critères pour juger de la fiabilité en toutes circonstances.

[158] La question soulevée devant la Cour ne concernait pas la présence de conditions d'application de la présomption légale de fiabilité visée par le Décret. Le problème à résoudre était de juger de la fiabilité d'un autre moyen informatique de signature. Les dispositions du Décret ne devraient pas servir de critères d'appréciation de la fiabilité de toute signature électronique prétendant du statut de l'article 1316-4 du Code civil. Son but est autre. La non-conformité aux normes du Décret ne devrait avoir qu'une seule conséquence, à savoir la non-applicabilité de la présomption de fiabilité. Il ne s'agit que

---

[136] Appel Besançon (Ch. sociale), 20 octobre 2000
[137] *Supra,* par. 124 - 125

d'un des moyens d'apporter la preuve de la fiabilité requise et sa non-application ne nous prive que d'une seule voie, en laissant toutes les autres possibilités de convaincre le juge du respect du deuxième alinéa de l'article 1316-4 ouvertes. La propension de la cour de Besançon à faire appel aux dispositions du Décret est alarmante, car elle indique que l'intention du législateur français, déduite de la première phrase du deuxième alinéa de l'article 1316-4 et les objectifs de sa deuxième phrase sont confondus.

b. La valeur probante des signatures informatiques dans le contexte de la preuve libre

[159] Un autre exemple d'appréciation discrétionnaire du juge en droit civil par rapport à la place de la signature sur le plan probatoire est fourni par le régime de la preuve libre. Dans ce régime tout mode de preuve est recevable sans que cette recevabilité implique une force probante quelconque. L'élément de preuve, recevable sous ce régime, est soumis à l'appréciation du juge quant à la reconnaissance de sa valeur probante.

[160] À titre d'exemple, en droit civil suisse, c'est là la règle générale en matière probatoire. Les règles de preuves varient de canton en canton, mais quelques principes sont unifiés au plan fédéral. Un de ces principes est celui de la libre appréciation des preuves. En vertu de ce principe, il n'existe pas de catégories privilégiées de preuve. Ainsi, un papier original signé à la main n'aura pas, a priori, une valeur probante supérieure à celle du *print-out* d'un log file stocké sur disque optique. Selon Jaccard[138], un avantage existe pour la personne qui étaie ses affirmations par des moyens de preuve plus traditionnels que des données informatiques, car les tribunaux suisses n'y sont pas encore familiarisés.

[161] Le principe de la libre appréciation des preuves implique également que toute preuve doit obligatoirement emporter l'intime conviction du juge pour être retenue. Dans le contexte de la preuve libre, le fait qu'une preuve informatique soit admissible a priori devant les tribunaux suisses ne dispense pas celui qui cherche à s'en prévaloir de tout

---

[138]Michel JACCARD, « Problèmes juridiques liés à la sécurité des transactions sur le réseau », *Signelec.com*, *Signature électronique et droit de la preuve*, 2000,
source : http://www.signelec.com/content/se/articles/article_michel_jaccard_html , visitée en mai 2002

mettre en oeuvre pour effectivement convaincre le juge de la véracité du contenu de la preuve.

[162] Dans cette perspective, c'est bien entendu la fiabilité des systèmes de sauvegarde, le professionnalisme de l'organisation interne et la qualité des mesures de sécurité prises qui joueront un rôle décisif[139]. Comme le soutient Jaccard, ce que la partie sera obligée de mettre en avant, sera une combinaison des différents modes de preuve pour qu'une allégation soit démontrée: en plus de la production des documents pertinents imprimés à partir d'une copie de sauvegarde sûre, il s'agira de faire en sorte que le responsable de la sécurité informatique de la société en cause témoigne des mesures prises dans le traitement de l'information, dont la fiabilité pourrait encore être corroborée par un expert neutre.

[163] Les réflexions sur le mécanisme de la preuve libre en Suisse et les moyens de convaincre le juge de l'exactitude d'un moyen de preuve, s'appliquent sans doute dans les cas ou la preuve est libre. Il est logique que le standard de fiabilité jouera un rôle majeur dans l'évaluation de la valeur probante de la signature électronique qui demeure à l'appréciation du juge.

§ 2. Les capacités probatoires de la signature électronique dans le contexte juridique de la signature en *common law,* les manifestations du standard de fiabilité

[164] Le rôle premier de la signature sur le plan probatoire en *common law* est d'établir un lien entre un document et son auteur. Cette mission se révèle sur deux plans. L'authentification de l'écrit, c'est-à-dire la fourniture d'une certitude quant à son origine intervient d'abord au niveau de la recevabilité du document et, ensuite dans son examen comme élément de preuve. Sur les deux plans, les signatures traditionnelles ou informatiques servent à retracer l'auteur du document. La capacité de la signature à accomplir cette fonction sur ces deux plans est envisagée sous le principe de libre évaluation de la preuve. Dans l'application de ce principe, le juge est essentiellement guidé par la fiabilité de la technologie de signature, c'est-à-dire, celle de l'environnement de sa

[139] *Id.*

genèse. Dans les pages suivantes, nous circonscrirons le rôle de la fiabilité au regard des effets juridiques de la signature électronique sur le plan probatoire aux États-Unis.

a. L'intervention du critère de fiabilité au stade de la recevabilité de la signature en preuve

i. L'authenticité comme condition à la recevabilité de la signature en preuve en droit commun

[165] Au plan probatoire en *common law*, la signature sert à authentifier l'écrit. La question de l'authentification se pose donc dès le stade de l'admission du document en preuve. En général, la pertinence de l'écrit dépend de son origine. La personne qui invoque l'écrit doit, comme condition à l'admission en preuve, établir de manière satisfaisante que l'écrit provient de la personne qui paraît l'avoir produit. Par exemple, lorsque le document est signé, celui qui se prévaut du document doit fournir une preuve suffisante que le document a été en fait signé par la personne dont le nom apparaît sur le document. En droit de la preuve aux États-Unis, il est exigé avant même la recevabilité de l'écrit, une preuve suffisamment convaincante de son origine et de son auteur, afin que le *juge des faits* puisse conclure à l'authenticité du document.[140]

[166] Quand il s'agit de prouver l'authenticité de l'écrit préalablement à son admission en preuve, la signature ne représente pas une preuve suffisante pour établir l'origine du document. Pour convaincre le juge et le jury que le document provient de son signataire, celui qui en tire l'avantage doit fournir une preuve supplémentaire (*extrinsic evidence*). Les *Federal Rules of Evidence*[141] énumèrent certaines preuves supplémentaires devant être ajoutées à la signature pour identifier l'auteur. Parmi elles on peut citer le témoignage[142] d'une personne ayant assisté à l'apposition de la signature ou bien qui connaît l'écriture[143], bien que la dernière méthode, faute de fiabilité suffisante[144], n'a pas été appliquée avec

---

[140] Graham C. LILLY, *An Introduction to the Law of Evidence*, 3ème Édition, St Paul, West Group, 1996, p. 607

[141] Ci-après citées F.R.E., source : http://www.law.cornell.edu/rules/fre/overview.html, visitée en mai 2002

[142] F.R.E., article 901 (b) (1), précitées, note 141

[143] F.R.E., article 901 (b) (2), précitées, note 141

[144] *State v. Bond*, 12 Idaho 424, 86 P. 43 (1906)

persistance. Le recours à des experts[145] pour comparer des exemplaires de l'écriture est aussi parmi les moyens possibles. Lorsque l'écrit est produit par un processus ou un système, la preuve circonstancielle de l'authenticité serait la démonstration de la fidélité du système ou de la précision du processus[146]. Ainsi, la fiabilité du mécanisme de signature électronique s'avérera un préalable, nouveau et propre uniquement aux moyens d'authentification modernes, à son admission en preuve.

ii. L'admissibilité en preuve des enregistrements commerciaux

[167] La place de la signature électronique en droit se rapproche de la question de l'admissibilité des registres commerciaux informatisés à tout le moins dans la mesure où les deux phénomènes reflètent l'attitude juridique vis-à-vis des réalités du monde virtuel. Dans ce domaine connexe à la recevabilité de la signature en preuve, la question décisive est celle de convaincre le *juge des faits* de la fiabilité de l'ordinateur. Cette tâche n'a pas toujours été facile. Par exemple, le juge Van Graafeiland a soutenu :

> *« As one of the many who have received computerized bills and dunning letters for accounts long since paid, I am not prepared to accept the product of a computer as the equivalent of the Holy Writ. »*[147]

[168] L'attitude actuelle de la jurisprudence a été récapitulée par la Cour régionale de New Jersey dans l'affaire *Neal v. United States*. Les juges énoncent que les ordinateurs sont des outils merveilleux qui sont capables d'accomplir de nombreuses tâches à une grande vitesse et un à coût raisonnable, mais cependant, ils doivent être utilisés avec prudence. Les juges se montrent soucieux de la possibilité d'erreurs. Ils soutiennent que les personnes qui utilisent des systèmes informatiques doivent les exploiter en présence de contrôle approprié, afin de protéger la fiabilité et la précision de l'information.

[169] La jurisprudence a développé de nombreux moyens d'apprécier la fiabilité des ordinateurs. Dans certains cas, un test technique de fiabilité a été autorisé par le juge.[148] L'information sur le fonctionnement du système ayant produit les données a souvent été

---

[145] F.R.E., article 901 (b) (3), précitées, note 141
[146] G. C. LILLY, *op. cit.,* note 140, p. 611
[147] *Perma Research and Development v. Singer Co*., (2nd Cir) 542 F2d 111, 121 (1976)
[148] *United States v. Liebert* (ED Pa) 383 F Supp 1060 (1974)

fourni en appui à l'admissibilité des documents électroniques.[149] Concernant les documents informatiques, le témoignage du superviseur du système ou d'une autre personne connaissant le fonctionnement de l'environnement technologique particulier a souvent été utilisé comme moyen d'établir la précision du système[150]. La fiabilité des programmes informatiques mis en place et les mesures de vérification et de contrôles permettant de l'assurer ont aussi intéressé la cour. Les statistiques sur les défaillances antérieures du système ou l'absence de défaillances étaient souvent un argument, quoi que non exhaustif, dans la résolution des questions d'admissibilité des enregistrements informatisés.[151]

[170] La manière dont les tribunaux américains ont fait usage du standard de fiabilité pour ajuster le droit de la preuve aux phénomènes virtuels nous offre sans doute des pistes de réflexion sur leur attitude envers les signatures électroniques.

iii. L'admissibilité en preuve des produits d'innovations technologiques, la manifestation de la fiabilité et l'applicabilité de la théorie au cas de la signature électronique

[171] Jusqu'à tout récemment, la question de la crédibilité probante des technologies révolutionnaires n'était aucunement liée aux questions juridiques soulevées par la signature. L'appréciation des capacités d'une application technologique, utilisée aux fins de la signature, est cependant susceptible d'être une des premières questions auxquelles le juge fera face.

---

[149] *State v. Estill* 13 Kan App 2d 111, 764 p2d 455 (1988). Dans cette affaire de harcèlement par téléphone, le journal du système a été utilisé pour ajouter à l'information la fiabilité et la crédibilité voulues.

[150] William FENWICK, Gordon DAVIDSON, « Admissibility of Computerized Business Records », *14 Am. Jur. Proof of Facts* 2d 173, 2000 - Le témoignage doit établir la fiabilité de l'équipement de traitement de données, la manière dont elles ont été initialement introduites dans le système, le temps dans lequel se sont effectué leurs entrées. Le superviseur se devait de fournir de l'information sur les mesures entreprises dans le but de préserver la précision de l'information, les modes de stockage des données et les précautions visant à prévenir la perte de l'information pendant le stockage.

[151] Cependant, les cours ont tenu à préciser que les conditions de fonctionnement des programmes et des systèmes changent et le volume et les caractéristiques spécifiques d'un ensemble de données particulier peut causer un disfonctionnement du système qu'un autre ensemble d'informations ne pourrait pas provoquer.

[172] L'invocation d'une signature peut impliquer, pour reprendre les propos de Patenaude[152], l'apparition en cour de preuves obtenues grâce au recours à des techniques tout à fait innovatrices dont la qualité et la fiabilité n'ont pas encore été consacrées ni par un consensus de la communauté scientifique concernée, ni par des décisions judiciaires.[153] Lorsque arrivent en preuve les produits d'une technique moderne et complexe, le juge est confronté à la question de la validité de ladite technique.

[173] La décision de la Cour suprême des Etats-Unis, rendue dans l'affaire *Daubert v. Merrell Dow Pharmaceutical Inc*.[154], élabore les critères d'appréciation de la fiabilité des technologies nouvelles sur le plan probatoire. Ceux-ci ont trait au test de la théorie, la prise en considération de la publication ou la révision antérieure de la méthode en cause, l'estimation du taux d'erreur, de même que le consensus de la communauté scientifique. Ayant à juger du degré de crédibilité à accorder à une technologie moderne, le tribunal, déjà en 1923, avait élaboré la règle qui a prévalu jusqu'à tout récemment :

> *« Il est difficile de préciser à quel moment une théorie ou une découverte scientifique passe de l'expérimentation à la démonstration. À l'intérieur de cette zone grise, il faut reconnaître la force probante de la théorie, et bien que les tribunaux acceptent d'emblée les témoignages d'experts basés sur une théorie ou une découverte scientifique reconnue, il faut que ce fondement scientifique soit suffisamment prouvé pour être accepté de tous dans le domaine particulier en cause. »*[155]

[174] La Cour Suprême du Canada ajoute un critère de proportionnalité selon lequel le profit de l'utilisation de la technologie en preuve devrait dépasser les dommages éventuels qu'un manque de précision pourrait causer[156]. Un consensus a été atteint sur le point que la détermination de la fiabilité doit être un processus flexible et sensible à la réalité. Comme la cour l'a souligné dans *Kumho Tire Co. v. Caramichael*[157], dans le domaine des innovations technologiques la probabilité de variation est énorme.[158]

---

[152] Pierre PATENAUDE, « De l'expertise judiciaire dans le cadre du procès criminel et de la recherche de la vérité : quelques réflexions », *Revue de Droit, Université de Sherbrooke*, (1) 1997
[153] *Id.*
[154] 113 C. St. 2786 , p. 2797 (1993)
[155] *Frye c. U.S*, 293 F. 1013 (D.C. Cir. 1923)
[156] *La Reine c. Mohan*, (1994) 2 R.C.S., 9
[157] 526 U.S. 137 (1999)
[158] Frank TUERKHEIMER, « The Daubert Case and Its Aftermath : A Shot-gun wedding of Technology and Law in the Supreme Court», 51 *Syracuse Law Review* 2001, 803

[175] Au sujet des cas examinés, il est à noter que la question s'est posée en matière criminelle. Cependant, l'analogie avec la preuve civile, y compris avec la signature est justifiée et il serait légitime d'appliquer cette logique, développée par la jurisprudence aux États-Unis, en matière civile. Il y a une forte probabilité que certaines technologies de signature électronique se présentent comme étant tout à fait nouvelles et inconnues au public. Il est aussi possible que les applications industrielles de certaines technologies déjà existantes soient innovatrices. D'autant plus que dans certains cas, la résolution de la question de l'imputabilité d'une signature peut relever du domaine du droit criminel[159], ce qui autoriserait le juge à recourir de plein droit aux critères énoncés.

Par conséquent nous pouvons conclure que la crédibilité de la technologie est une des manifestations de la fiabilité des signatures électroniques, intervenant comme un nouveau paradigme en matière de recevabilité en preuve des moyens virtuels d'authentification.

b. La détermination de la valeur probante de la signature électronique – la corrélation entre le concept traditionnel d'imputabilité et la notion nouvelle de procédures de sécurité

i. La corrélation entre les concepts d'imputabilité et de procédures de sécurité

[176] Les dispositions régissant la valeur probante de la signature électronique selon l'*Uniform Commercial Code* et l'*UETA* s'articulent autour de deux concepts : celui d'imputabilité[160] et celui de procédures de sécurité. Le contenu et l'interdépendance de ces concepts fera l'objet des pages qui suivent. La relation entre ces concepts révélera la corrélation entre fiabilité et valeur probante de la signature électronique.

[177] Le concept d'imputabilité réfère au lien entre une personne et le résultat de ses actions, que ce soit une signature ou un document. L'acte juridique est imputable à la partie qui est à sa source. Une signature est imputable à une personne si elle résulte de l'acte de cette personne.

---

[159] Tel serait le cas de dol en matière de transfert de fonds.
[160] Le terme anglais est *attribution.*

[178] Dans le contexte des moyens d'authentification virtuels, ce concept d'imputabilité se trouve indissociablement lié au concept de procédures de sécurité commun à l'*Uniform Commercial Code* et à l'*UETA*.[161] UETA définit les procédures de sécurité comme des moyens de vérifier qu'une signature est celle d'une personne et de détecter des altérations et des changements dans le contenu d'un document électronique. À titre d'exemple, la loi énumère l'utilisation d'algorithmes ou d'autres codes, des mots ou des numéros d'identification, le chiffrement, etc. Le lien entre les procédures de sécurité et l'imputabilité peut s'exprimer avec des conséquences juridiques différentes. Dans certains cas, la mise en place de procédures de sécurité donne lieu à une présomption d'imputabilité. Dans d'autres, les procédures en question sont un moyen parmi d'autres de prouver l'imputabilité. Leur fiabilité de mesures n'affecte pas leur caractère, mais détermine plutôt le poids probant dont elles jouissent dans l'établissement de l'imputabilité.[162]

ii. L'article 2B de l'UCC et le concept de procédures d'imputabilité

[179] Le projet d'article 2B de *l'Uniform Commercial Code*[163] contient la règle générale à l'effet que celui qui affirme qu'un document provient d'une personne a l'obligation de prouver le lien entre l'auteur et l'écrit. Un effet juridique est reconnu à l'application de procédures, que l'UCC appelle des procédures d'imputabilité[164]. Les procédures d'imputabilité sont définies comme permettant la vérification qu'un message est celui d'une personne déterminée.[165] Aux termes de la loi, si les parties s'accordent sur une procédure technologique ou l'adoptent de quelque autre manière, que cette procédure est commercialement raisonnable et que le destinataire du message a agi en se fondant sur le message, ce dernier s'acquitté du fardeau de la preuve de l'imputabilité. Ensuite, il appartient à la personne qui désire répudier l'imputabilité d'apporter la preuve contraire. L'article 2B trouve sa genèse dans l'article 4A-201 sur le transfert de fonds :

---

[161] Le terme anglais est *security procedures.*
[162] UETA, précitée, note 66
[163] Projet proposé le 1er février 1999, source : http://www.law.upenn.edu/bll/ulc/ulc.htm, visitée en mai 2002 (ci-après cité U.C.C.)
[164] La loi utilise le terme *attribution procedures.*
[165] Amelia H. BOSS, « Searching for Security in the Law of Electronic Commerce » 588 *Practising Law Institute*, 1999, 401

*« « **Security procedure** » means a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure.»*

[180] La même présomption, renversant le fardeau de la preuve, est établie si des procédures de sécurité commercialement raisonnables sont en place. Les rédacteurs soutiennent que le commerce électronique, par sa nature anonyme, dépend de la reconnaissance de telles procédures en droit et en pratique. Les rédacteurs du projet d'article 2B adoptent une position flexible par rapport à la nature des procédures de sécurité. Les commentaires accompagnant le projet énoncent expressément que la loi ne dicte pas la forme qu'une procédure d'imputabilité doit emprunter à cause de l'évolution rapide de la technologie et des pratiques commerciales.[166]

[181] Dans les hypothèses des articles 4A et 2B l'imputabilité se trouve en rapport direct avec les procédures de sécurité qui sont censées réduire le risque de défaillance des techniques d'authentification. Toute forme de signature, dans la mesure où elle établit le lien entre le signataire et le document, devrait obéir aux dispositions d'imputabilité où la place centrale est tenue par les procédures de sécurité. Pour bénéficier de la présomption, la présence d'une procédure de sécurité commercialement raisonnable doit être établie. Dans ce contexte on peut conclure que les procédures de sécurité sont l'émanation du critère général de fiabilité dans le cas concret de l'UCC.

[182] En vertu de ces dispositions, le lien entre l'imputabilité et la fiabilité se manifeste sur deux plans. On peut avoir recours au standard de fiabilité de la technologie afin de fonder l'application de la présomption en démontrant que les procédures de sécurité possèdent les capacités demandées à mettre en fonction cette présomption. La partie qui veut éviter les effets de la présomption d'imputabilité aura recours à la fiabilité pour expliquer les raisons de la défaillance des procédures de sécurité. Lorsque le moyen

---

[166] Commentaires du projet d'article 2B-114, source : http://www.law.upenn.edu/bll/ulc/ucc2b/2b299.htm, visitée en mai 2002

d'imputer un écrit à sa source est une signature électronique, la fiabilité de la technique et de son application continue à tenir une place centrale sur le plan probatoire.

iii. Le concept de procédures de sécurité selon l'UETA

[183] Dans le cas de UETA, les procédures de sécurité sont toujours un facteur dans l'appréciation de la valeur probante de la signature, mais elles ne bénéficient pas d'un statut aussi privilégié. L'article 9[167] de la loi dispose :

> *« An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable. »*

[184] L'attention spéciale, portée aux procédures de sécurité parmi les autres moyens de prouver l'imputabilité, est apparente. Selon le commentaire de l'UETA, dans certaines circonstances, une procédure technique ou technologique peut être le seul moyen de convaincre le *juge des faits* que la signature est celle de la personne à qui elle apparaît appartenir. Dans d'autres cas, l'utilisation de procédures de sécurité peut être nécessaire pour désavouer l'affirmation qu'un pirate informatique est intervenu[168].

[185] En vertu de UETA, l'efficacité des procédures de sécurité, de même que la fiabilité de l'environnement de création, d'utilisation et d'existence de la signature, jour un grand rôle pour l'accomplissement de la mission première de la signature sur le plan probatoire, notamment celle d'établir un lien entre le document et son auteur. C'est autour de l'établissement de la fiabilité que s'articulent les arguments de la partie désirant persuader le *juge des faits* de l'imputabilité d'une signature. D'autre part, la partie, tentant de prouver le contraire, sera obligée de s'attacher à mettre en doute la fiabilité.

---

[167] UETA, article 9, précitée, note 66. L'artcile est intitulé « Attribution and Effect of Electronic Record and Electronic Signature ».

[168] Amelia H. BOSS, « The Uniform Electronic Transactions Act in a Global Environment», 37 *Idaho Law Review* 2001, 275

[186] La loi dispose que le recours légal à des procédures de sécurité à l'appui des allégations d'imputabilité est crucial à cause de l'importance primordiale des procédures de sécurité dans l'environnement électronique. Cette affirmation indique que le recours du droit au nouveau paradigme en matière probatoire résulte du besoin impérieux de prendre en considération l'origine virtuelle de la signature électronique. Ainsi, comme la notion de procédures sécuritaires est la manifestation du standard plus large de fiabilité, la place de ce standard dans l'ajustement du droit de la preuve au cyberespace est soulignée.

Conclusion partielle

[187] Il est justifié de rappeler que les systèmes de droit civil et ceux de *common law* se dotent de nouveaux paradigmes pour remodeler leurs institutions en harmonie avec les nouveaux phénomènes. Il est aussi apparent qu'en matière de preuve, l'adaptation du droit de la signature consiste en des recours et des interrogations sur la fiabilité des technologies d'authentification virtuelles. Les différents cadres juridiques ne s'engagent pas dans les mêmes voies pour appliquer le test de fiabilité. Tout de même, le concept de fiabilité garde son importance dans tous les cas et son rôle s'articule toujours autour de la même finalité – l'adaptation du droit de la preuve aux signatures électroniques. C'est à travers de l'application de ce critère auxiliaire que les institutions juridiques assurent l'intégration des nouvelles réalités dans les catégories existantes. Ainsi, le standard de fiabilité, fait l'objet d'un consensus en ce qui concerne sa mission en droit.

[188] Nous avons démontré que de par sa nature le standard de fiabilité est une règle de droit, il fait partie de l'institution juridique de la signature électronique. De point de vue de son contenu, ce standard s'identifie à un ensemble de règles techniques liées aux procédés de signatures électroniques. Ainsi, la substance du standard de fiabilité trouve sa source dans les propriétés techniques de l'architecture du cyberespace.

[189] Dans la partie suivante nous exposerons les composantes du standard de fiabilité, pour conclure qu'elles sont toutes des éléments liés à la technologie et, par-là, rendent le standard juridique tributaire des capacités de l'architecture du cyberespace. À la toute fin, nous examinerons la substance du standard de fiabilité, notamment au cours d'un examen de la morphologie du cyberespace.

Partie II - L'ARCHITECTURE DU CYBERESPACE – LA SOURCE DES CERTITUDES ET DES INCERTITUDES EN DROIT

Chapitre III – LA FIABILITÉ DES MOYENS INFORMATIQUES DE SIGNATURE – UNE RÉSULTANTE DE L'ARCHITECTURE DE L'ENVIRONNEMENT

[190] La signature électronique est une donnée renfermant de l'information qui lie une personne et un document. La signature peut donc être située dans la structure stratifiée du cyberespace, organisée sur trois niveaux - le milieu matériel, le code et son contenu[169]. Dans ce cadre, la signature électronique, en tant qu'information, fait partie, parmi d'autres informations, tels les textes, les films en ligne et les images numériques, du *contenu* du cyberespace.

[191] Par ailleurs, la signature électronique, résulte d'un procédé électronique[170] mis en oeuvre au sein d'un ensemble hétéroclite de machines, processus, données, logiciels, organisé autour de la notion de base du monde virtuel, celle de *système d'information*[171]. Les procédés de réalisation de signatures électroniques résident, de leur part, dans les strates inférieures du cyberespace – le *milieu physique* et le *code*. C'est la fiabilité de ces procédés qui a préoccupé les législateurs. Le résultat de ces procédés, la signature comme donnée porteuse d'une information est authentique ou fausse, et ceci, dans la majorité des cas, en raison de la fiabilité des moyens de sa création. Comme cela a été explicité, la fiabilité des moyens de signature sur le plan probatoire est fondée sur quelques assurances concrètes, à savoir la garantie d'un lien fiable avec l'auteur de la signature et d'une liaison fiable entre la signature et l'acte auquel elle est apposée de même qu'une garantie de l'intégrité de cet acte.

[192] Au sujet du document informatique, Dunberry souligne que le document électronique fiable est celui qui est créé, conservé, reproduit ou transféré dans un environnement qui présente des garanties suffisantes de fiabilité.[172] Dans ce chapitre nous porterons l'accent sur l'environnement de la signature électronique. Nous démontrerons

---

[169] L. LESSIG, *op. cit.,* note 7, p. 23
[170] P. TRUDEL, G. LEFEBVRE, S. PARISIEN, *op. cit.,* note 61, p.83
[171] Ci-après SI
[172] Éric DUNBERRY, «L'archivage des documents électroniques», dans Vincent GAUTRAIS (dir.), *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002, 124

que les moyens de signature électronique possèdent des capacités qui sont intimement liées aux propriétés du monde virtuel qui les héberge. Ce sont les particularités de l'architecture qui attribuent aux procédés d'authentification la capacité de fournir la base d'une identification et d'une manifestation du consentement fiables qui permettent de garantir l'authenticité de la signature produite. Nous examinerons aussi les composantes du standard de fiabilité. La fiabilité de chaque élément est importante, soutenant qu'en effet la *«…chaîne n'est jamais plus solide que le plus faible de ses maillons* »[173]. Le lien entre la valeur de la signature électronique et les caractéristiques du cyberespace étant établi, nous examinerons l'évolution de l'état de l'art en mettant en relief une modification fondamentale de l'architecture du cyberespace.

Section I – L'ENVIRONNEMENT DES PROCÉDÉS DE SIGNATURE ÉLECTRONIQUE – UNE SOURCE DES CERTITUDES ET DES INCERTITUDES

§ 1. Le noyau: le système d'information – l'analyse de la notion générale de fiabilité

a. Le concept de système d'information – le point commun des signatures modernes

[193] La signature traditionnelle affiche une constance indétrônable, à l'opposé les moyens d'authentification du cyberespace sont d'une infinie diversité. Cette variété s'illustre aisément. Ainsi, selon le professeur Trudel[174], il apparaît légitime de soutenir qu'une signature présentée sous la forme d'un code secret constitue une marque personnelle aux termes de l'article 2827 du C.c.Q. Aux États-Unis, l'UETA autorise, entre autres, une forme sonore de la signature[175]. Ceci laisse à penser que le fait d'appuyer sur une

[173] *Id.*
[174] S. PARISIEN, P. TRUDEL, *op. cit.,* note 27, p. 33
[175] UETA, Commentaires, article 9, al. 8, précitée, note 66

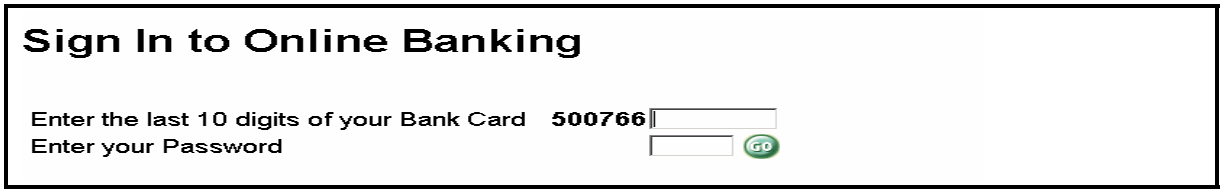
combinaison de touches lors d'une conversation téléphonique aurait les effets d'une signature, tout comme dans le cas ou la conversation téléphonique serait matérialisée sur un support papier, signé par les parties. Aux termes des législations modernes, un nom dactylographié au bas d'un message envoyé par courrier électronique, peut bel et bien représenter une signature électronique, de la même manière qu'une signature numérique réalisée au sein d'une infrastructure à clés publiques. La diversité technologique, ainsi que la créativité des concepteurs peuvent nous offrir des formes de signatures innombrables qui seraient toutes dignes de reconnaissance légale.

Image 1 *- Différents types de signatures électroniques*

1 A. Séquence représentant une clé publique participant dans le modèle de la cryptographie asymétrique

```
3081 8902 8181 00D9 8C9E 2B14 F9C5 62DE 67A2 B7EF 95E3 F7DC C586 F37A BC0B C127 52EC 0736
730B E6F8 2A39 2901 22FA B6AB 1EF0 B9DD 395A 2AAA 080A 629E CF06 E46B 1B6D 83CD 98DC 173E
0138 B1D2 D210 30F4 6331 1FD3 CFFB 2787 C5DB 2A9B E84A E34B ABA1 2CF7 4335 3F12 989D CAE4
4548 C5C2 6133 9E09 48C8 4BC3 F18E 0B2C E50B 9987 3307 85FC 7C75 1D02 0301 0001
```

1 B. Procédure « numéro de carte et code »

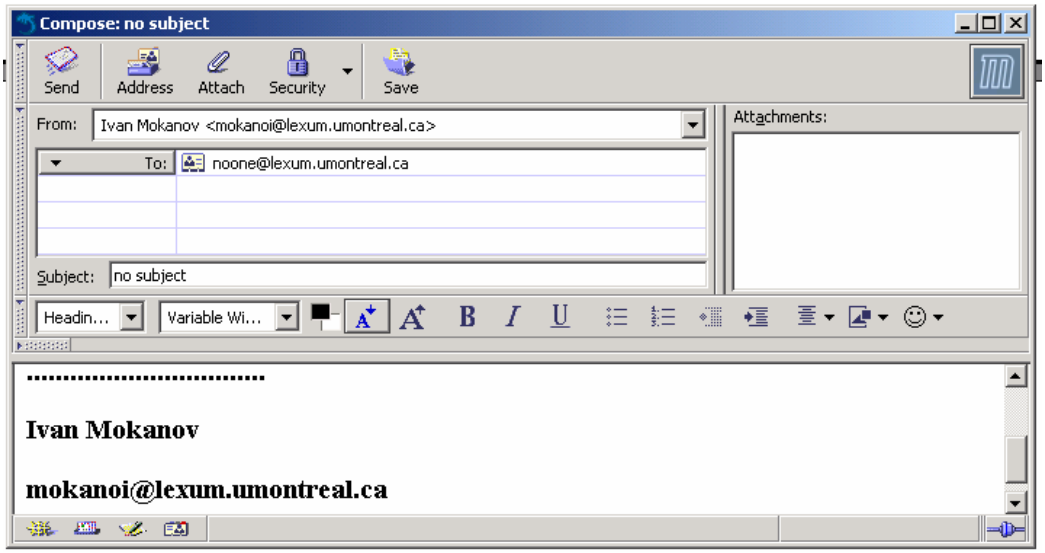


1 C. Combinaison sonore lors d'une conversation

"If .....press "pound""

1 D. Signature manuscrite numérisée à la suite d'un balayage optique

1 E. Nom dactylographié dans un message électronique



[194] Les différences entre les procédés énumérés à titre d'exemple sont fondamentales. L'exemple du guichet bancaire est révélateur, le système en question se composant en premier lieu d'un guichet qui distribue des billets sur demande de l'utilisateur, d'un logiciel du guichet qui requiert l'information nécessaire de l'usager, d'une carte magnétique, d'un serveur central, etc. Un autre exemple, le système qui rend possibles nos communications

par courrier électronique moyennant les services de *Hotmail*, implique aussi un nombre considérable d'éléments, parmi lesquels citons le serveur Web servant à l'interface[176], le serveur SMTP[177] utilisé pour envoyer et recevoir les messages des autres systèmes, un serveur POP[178] autorisant la communication entre les usagers du système, la technologie de création de comptes de courrier électronique (une interface Netauth par exemple), des mots de passe Unix ou NT ou encore un logiciel client fonctionnant à travers du Web qui permettra aux usagers de créer et lire des messages.

[195] Tout en n'ayant pas l'ambition d'approfondir les spécificités des exemples envisagés, cette énumération met en avant les différences considérables entre les divers types d'environnements. Aussi faut-il rappeler que tous les systèmes, guichets bancaires, *Hotmail*, système téléphonique, permettent la création de signatures électroniques jouissant d'une reconnaissance légale. Les systèmes étudiés à titre d'exemple, tout en faisant preuve de différences majeures pour ce qui est de leur fonctionnement et de leur conception, possèdent le point commun d'appartenir à une catégorie fondamentale – celle des *systèmes d'information* (ci-après SI), comme île informationnelle et fonctionnelle et noyau du cyberespace. Par conséquent, les signatures créées, tout en ayant différents modes de création, sont réalisées au sein de la même unité fondamentale du monde virtuel, le système d'information.

[196] Le concept de SI réfère à un ensemble d'intervenants (acteurs), données, processus, interfaces et communications qui interagissent pour rendre possibles ses fonctionnalités[179]. La distinction entre le système d'information, une notion autonome, et les technologies de l'information qui en sont le support est importante. Nous nous intéresserons à la structure du SI pour en distinguer les composantes qui rendent possibles ses fonctionnalités, notamment celles qui sont déterminantes pour le déroulement du processus d'apposition de signatures non-traditionnelles et en déterminent les spécificités.

---

[176] Office de la langue française, *Signet*, source : http://w3.olf.gouv.qc.ca/banque/index.asp, visitée en mai 2002

[177] Le terme désigne le serveur qui sert à l'utilisation du protocole *Simple Mail Transfer Protocol*. Laura VICTOR, John MULHERN, « Sending E-mail: Selecting & Configuring Your SMTP Server », *Univesity of Pensilvanya*, *Univesity of Pensilvanya Computer Center*,
source : http://www.upenn.edu/computing/help/doc/email/smtp.html, visitée en février 2002

[178] Le terme désigne le serveur qui sert à l'utilisation du protocole *Post Office Protocol*. About.com, « Post Office Protocol », *Learn the Net Glossary*, source : http://www.learnthenet.com/english/glossary/pop.htm, visitée en mai 2002

[179] Jeffrey L. WHITTEN, Lonnie D. BENTLEY, Kevin C. DITTMAN, *System Analysis and Design Methods*, 5ème Édition, Boston, McGraw-Hill, 2001, p. 8

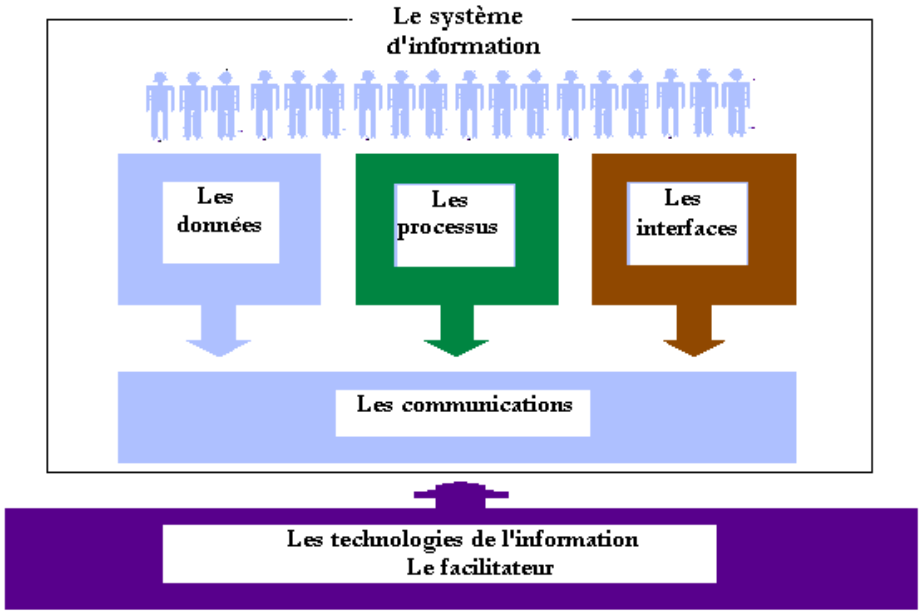


Image 2. *Les unités structurantes du SI. Les technologies de l'information – « the enabler »*

b. Les unités structurantes du système d'information

i. Les intervenants

[197] Le monde nouveau que constitue la société numérique ne peut faire abstraction du facteur humain. Les acteurs dans un système d'information sont un élément central dans la chaîne de sécurité.[180] Les acteurs (ou les intervenants) sont les personnes qui sont concernés d'une manière quelconque par le fonctionnement du système d'information[181]. Il nous apparaît opportun de nous arrêter brièvement sur quelques considérations pratiques afin d'illustrer l'influence des divers intervenants au sein du système d'information.

---

[180] Vincent GAUTRAIS, « Les aspects relatifs à la sécurité », *Juris International*, *Commerce Électronique*, *Guide juridique du commerçant électronique*, source : http://www.jurisint.org/pub/05/fr/index.htm, visitée en mai 2002

[181] Edward YOURDON, *Modern Structured Analysis*, NJ, Englewood Cliffs, 1989, 3ème Chapitre

[198] D'abord, les propriétaires des systèmes assurent le financement, le développement, le fonctionnement et la maintenance du SI.[182] La pertinence de leur rôle s'explique par l'intérêt que présente pour eux la valeur du système. Le coût de l'implémentation de la majorité des dispositifs et des éléments des SI est à leur discrétion, d'où leur rôle primordial pour les spécificités du système, pris dans son ensemble.

[199] Les utilisateurs des SI représentent la deuxième catégorie d'acteurs.[183] Ce sont les personnes qui se servent du SI ou sont associés à son fonctionnement sur une base régulière. Il existe plusieurs classes d'utilisateurs, parmi lesquelles deux peuvent être distinguées, à savoir les utilisateurs internes et les utilisateurs externes.

[200] Les utilisateurs internes regroupent les employés de l'entreprise pour laquelle le SI est conçu. Cette catégorie englobe le personnel de service, ainsi que les personnels technique et professionnel[184], les superviseurs, les gestionnaires et la direction, ayant tous une relation spécifique au SI. Les utilisateurs externes, d'autre part, sont les consommateurs et les entreprises contractantes. Les entreprises recourent de plus en plus souvent à des connexions directes entre leurs SI et celui de leurs des partenaires d'affaires. Ainsi, deux entreprises interconnectent leurs SI et sont, l'une pour l'autre, des utilisateurs externes. Il en va de même pour le consommateur qui accède à un site Web pour effectuer un achat.

[201] Les concepteurs des SI[185] représentent un ensemble d'acteurs très important. Ils traduisent les objectifs du système d'information en solutions techniques – configurations, bases de données, réseaux et applications logicielles. Leur importance stratégique tient au fait qu'ils effectuent les choix technologiques. Les solutions technologiques du SI, telles que pensées par les concepteurs, sont ensuite réalisées par les constructeurs[186]. Bien évidemment d'autres spécialistes techniques peuvent être impliqués, tels les programmeurs de systèmes ou de bases de données, les administrateurs de réseaux. Dans la catégorie directement concernée par le développement du SI se trouve aussi l'analyste de système[187] dont le rôle consiste à faciliter l'évolution du SI et des applications logicielles. Cet acteur interagit avec tous les autres et occupe une place centrale dans les rapports entre tous les

---

[182] J. L. WHITTEN, L. D. BENTLEY, K. C. DITTMAN, *op. cit.,* note 179, p. 9
[183] *Id.*, p. 11
[184] Des exemples de la catégorie sont les ingénieurs, les scientifiques, les statisticiens, les concepteurs.
[185] J. L. WHITTEN, L. D. BENTLEY, K. C. DITTMAN, *op. cit.,* note 179, p. 12
[186] *Id.*, p. 13. Selon l'auteur, un exemple classique de constructeur et le programmeur d'applications.
[187] *Id.*, p. 13

intervenants. Il assure l'interopérabilité de tous les acteurs et concilie leurs efforts au nom de la performance du SI.

[202] Pour les SI basés sur les technologies de l'information, une attention particulière doit être portée aux vendeurs de produits TI[188] qui développent, vendent et assurent le support des technologies, de même les consultants externes qui assistent les entreprises lors du choix, du développement ou de l'achat de produits TI.

[203] Le facteur humain, que nous avons choisi de citer en première place dans l'étude de l'environnement des moyens virtuels d'authentification, a été organisé en de différentes classes. Les groupes qui le forment diffèrent entre eux par leurs influences, leurs pouvoirs et leurs possibilités d'affecter le SI. Leurs profils sont aussi distincts et la fiabilité de chacun se compose de divers éléments[189]. Cependant, la qualité avec laquelle chaque acteur intervient influencera la qualité des fonctionnalités du SI et c'est la raison pour laquelle le facteur humain y mérite une place aussi importante.[190]

ii. Les données

[204] Les données sont l'unité structurante fondamentale des SI. Elles réfèrent à la source primaire de l'information, à sa genèse et à son contenu[191]. Les données font l'objet de saisie, stockage, traitement, édition et utilisation. Celles qui se trouvent à la base d'un SI peuvent être nombreuses et de types divers, tel le nom d'une personne, son adresse, le numéro et le solde de sa carte de crédit. Les différents processus de réalisation de signatures électroniques se basent sur les divers types de données qui forment le socle de l'information que la signature renferme. Par exemple, la séquence de symboles que représente la clé de chiffrement réfère à des données qui portent l'information utilisée aux fins de l'application de l'algorithme de chiffrement. Les identifiants sont des données qui permettent de repérer

---

[188] Le terme anglais est *IT vendors.*

[189] J. L. WHITTEN, L. D. BENTLEY, K. C. DITTMAN, *op. cit.,* note 179, p. 28. À titre d'exemple, on pourrait mentionner les qualités de l'analyste du système. Selon les auteurs cet acteur doit posséder des connaissances en technologies de l'information, en programmation, en gestion et commerce. Parmi les habilités plus concrètes, les auteurs soulignent l'aisance de communication, la flexibilité et l'adaptabilité, l'éthique.

[190] Gordon B. DAVIS, « Knowing the Knowledge Workers : A Look at the People Who Work with Knowledge and the Technology That Will Make Them Better »*, ICP Software Review*, 1982, 70-75

[191] J. L. WHITTEN, L. D. BENTLEY, K. C. DITTMAN, *op. cit.,* note 179, p. 52

et de localiser des objets et des documents[192] et peuvent se retrouver à la base de l'identification d'un texte signé. L'identité du signataire, de même que ses attributs, telle sa fonction, sa qualité, ses droits au sein d'une personne morale, etc.[193] représentent des informations dont un certificat peut faire état. Toutes ces données nécessaires au déroulement d'un processus d'apposition de signature peuvent, elles aussi, être basées sur d'autres données.

[205] Les données d'un système sont organisées, notamment par des schémas des bases de données, de manière à permettre et à augmenter l'efficacité de leur utilisation. Certains systèmes d'information ne mettent pas en place la technologie des bases de données. C'est les cas, par exemple, des vieux systèmes patrimoniaux mettant à profil des technologies d'organisation de données simples (flat-file), comme VSAM[194]. Selon les approches plus modernes, le schéma des bases de données organise les données à l'aide de structures, de champs, de colonnes. Les systèmes de gestion de bases de données (Oracle, DB2, SQL Server, Access, FoxPro) peuvent faire l'objet de standardisations diverses. Dans ces cas, leurs données pouvant être rendues accessibles sont représentées par le biais de langages publics comme SQL[195]. Le degré de précision du traitement et de l'organisation des données est un autre préalable à la performance du SI.

iii. Les processus

[206] Les processus, comme unité structurante des SI, assurent leurs fonctionnalités. Tout comme les données, les processus sont une unité structurante caractéristique pour tous les systèmes d'information, indépendamment de leur « facilitateur ». Avant la numérisation des systèmes de cartes de crédit, la vérification de leur validité s'effectuait par le commerçant, dont la seule tâche était de s'assurer que le numéro de la carte qui lui avait été présentée n'était pas parmi un certain nombre de numéros invalides, contenus dans des

[192] L.C.C.J.T.I ., article 46, al. 4, précitée, note 10
[193] *Id*., article 47, al. 2
[194] Dénomination pour *Virtual Storage Access Method.* Selon cette technologie, la structure des données est insérée directement à l'intérieur du langage de programmation qui crée les applications utilisant les données.
[195] Abréviation pour *Structured Query Language*.

livrets que les commerçants recevaient sur une base hebdomadaire. Cette vérification était un processus remplissant le rôle d'unité structurante inhérente aux SI d'alors.

[207] Dans un modèle d'apposition de signatures modernes, les processus qui sont employés peuvent relever tant du monde réel que du cyberespace. À titre d'exemple, la vérification de l'identité ou des attributs d'une personne, précédant la délivrance d'un certificat[196] se déroule généralement dans le monde physique et en présence des acteurs, alors que la vérification de la validité d'un certificat auprès d'un répertoire souvent distant de certificats révoqués repose essentiellement sur des moyens électroniques.

[208] Dans le monde moderne fréquemment les processus peuvent être représentés dans un *environnement de développement d'application*[197]. L'automatisation des processus s'effectue au moyen d'applications logicielles dont le contenu est déterminé par des langages de programmation, tels COBOL, C++, Visual Basic, Powerbuilder, Smalltalk ou Java. Certains systèmes de gestion de bases de données offrent leur propre langage de programmation, comme Visual Basic for Applications (dans Access) et PL-SQL (dans SQL)[198].

iv. Les interfaces

[209] Le rôle des interfaces dans les SI se manifeste de deux manières. L'interface se présente comme un lien entre le système et les utilisateurs d'une part et comme un point de rencontre entre les différents SI. Les interfaces destinées aux utilisateurs assurent leur contact avec le SI et doivent se caractériser par le transparence et la simplicité. Leur importance est majeure pour la participation fiable des utilisateurs dans le fonctionnement du SI. Les interfaces entre les différents systèmes d'information visent à garantir leur interconnectivité. Les systèmes d'information existants reflètent généralement l'état de l'art au moment où ils ont été conçus. Certains d'entre eux résultent d'un «développement maison »[199] (*in-house development*), d'autres sont basées sur des solutions acquises des vendeurs de produits TI. Ces différences de conception engendrent des

[196] L.C.C.J.T.I ., article 51, al. 2, précitée, note 10
[197] Le terme anglais est ADE qui est une abréviation de *Application Development Environment.*
[198] J. L. WHITTEN, L. D. BENTLEY, K. C. DITTMAN, *op. cit.,* note 179, p. 56
[199] Le terme désigne le logiciel réalisé par l'utilisateur lui-même en fonction de ses besoins.

difficultés d'intégration des systèmes. Cette problématique explique que la qualité des interfaces présentes au sein des unités structurantes des SI soit susceptible d'affecter les qualités du système dans sa totalité.

[210] Comme dans le cas des autres unités structurantes, les interfaces d'un système d'information qui repose sur les technologies de l'information, prennent la forme de solutions technologiques. À titre d'exemple de technologies d'implémentation d'interfaces on peut mentionner l'interface utilisateur graphique Windows servant à implémenter des applications compatibles Windows. Pour ce qui est des applications d'interface entre des SI différents, les exemples de DCOM et COBRA sont pertinents.

v. Les communications

[211] Les communications se sont vues attribuer la place d'unité structurante dans le cadre des SI par la majorité des auteurs et des analystes de systèmes.[200] Elles représentent des flux de données entre des entités différentes, qui se caractérisent par leur volume et leur fréquence. Les communications peuvent ne pas être effectuées au moyen des technologies de l'information, si elles font partie d'un système basé sur des supports « classiques ». Les moyens logiciels impliquent des systèmes d'exploitation et de protocoles, tels NetWare, Windows/NT Server, IBM Lotus Notes/Domino, Unix ou Linux. Dans le contexte de l'informatique, les communications s'effectuent par le biais d'une architecture de réseau qui comprend des stations de travail, des terminaux, des serveurs, des périphériques et des dispositifs de connexion entre ces éléments. La performance du système d'information, noyau du cyberespace, est sensiblement influencée par l'organisation des communications. Les communications sont un facteur important dans les architectures d'authentification.

[212] Un des grands avantages du monde virtuel est l'autorisation d'interactions sans exigence de présence physique. Par conséquent, la signature électronique fait presque incessamment l'objet de communications de données pendant son cycle de vie. De surcroît, les données employées par le processus création de la signature sont aussi, dans la majorité des cas, communiquées, l'exemple en étant la divulgation d'une clé publique pour permettre le fonctionnement d'une infrastructure à clé publique.

---

[200] John A. ZACHMAN, « A Framework for Information System Architecture », *IBM Systems Journal* 26, No. 3, (1987)

[213] Les acteurs, les données, les processus, les interfaces et les communications forment le cadre des SI. Leurs qualités et leur degré de fiabilité, de même que la qualité avec laquelle toutes ces unités sont assemblées dans l'architecture du système, sont les éléments qui déterminent la qualité du fonctionnement du SI dans son ensemble. Comme nous l'avons démontré, les activités spécifiques de ces unités structurantes sont à l'heure actuelle véhiculées par des solutions technologiques.

§ 2. Le système d'information - unité informationnelle et fonctionnelle constitutive du cyberespace, les strates du cyberespace

[214] Les unités structurantes qui ont fait l'objet de l'analyse des pages précédentes présentent le profil type d'un SI, nonobstant ses objectifs ou ses supports. La majorité des organismes agissant dans le domaine des affaires, le domaine social ou gouvernemental ont recours dans leurs activités à un ou plusieurs SI.

[215] En revanche, lorsque le système d'information joue le rôle de noyau du cyberespace, au sens d' « île » informationnelle et fonctionnelle, les technologies de l'information conduisent ses unités structurantes. Ainsi, transposé dans le cyberespace, le système d'information devient sujet à la stratification de son architecture. Pour organiser nos idées sur l'architecture du cyberespace nous aurons recours à la classification de Lessig[201], qui y distingue trois strates[202], à savoir, le plan physique, le code et le contenu.

[201] L. LESSIG, *op. cit.,* note 7*,* p. 23
[202] Lessig utilise le terme *layer.*

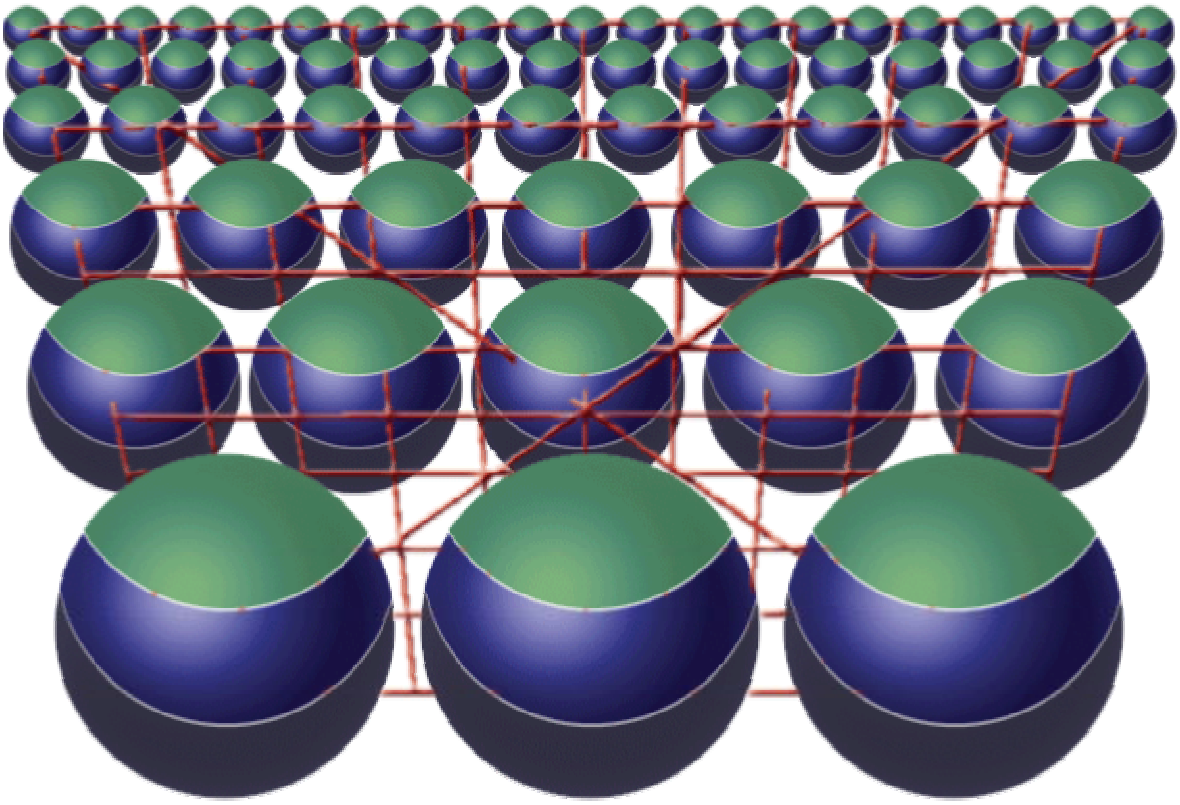


Image 3. *Les systèmes d'information - une « île » constitutive du cyberespace. Chaque système d'information qui participe, en tant qu'unité constitutive, à la composition du cyberespace, obéit à l'architecture stratifiée du cyberespace. La partie grise désigne la strate physique, la partie bleue – la strate logique et la partie verte – la strate supérieure formée par le contenu.*
Le dessin est conçu par François Viens.

a. La strate physique – le niveau de base

[216] La strate physique réfère aux dispositifs, aux équipements et aux structures matérielles sur lesquels l'information, qui forme le contenu du cyberespace, est produite, acheminée et hébergée. La référence est faite à cette strate comme à la première couche du cyberespace à cause son rôle de soutien de l'ensemble des composantes du monde virtuel. Cette strate offre aussi l'infrastructure nécessaire aux processus servant à la réalisation de signatures informatiques.

[217] Dans la démonstration de l'importance de la strate physique pour la performance des systèmes d'information du cyberespace, nous nous arrêterons sur les réseaux, le matériel et le milieu physique.

i. Les réseaux

[218] Les réseaux réfèrent à des ordinateurs ou des dispositifs connectés entre eux. Ils impliquent des liens physiques – des fils de réseau local d'entreprise (LAN)[203], des lignes téléphoniques, des terminaux d'accès par composition, des câbles à fibres optiques. Les liens peuvent aussi être électromagnétiques, tels les liaisons hertziennes, des micro-ondes. Les communications sur les réseaux varient selon leurs architectures, déterminées par des protocoles. Parmi eux, citons Ethernet, un exemple d'architecture de réseau local permettant d'offrir un débit standard de 10, 100 ou 1000 mégabits par seconde[204]. Ethernet constitue la base sur laquelle opèrent les protocoles de plus haut niveau d'Internet comme par exemple TCP[205], responsable de la préparation des données sous forme de paquets avant l'expédition et de leur assemblage dans le bon ordre à la réception. Le fonctionnement des réseaux implique encore un grand nombre de dispositifs qui en composent l'architecture. Ces dispositifs peuvent être englobés sous la notion d'ensemble d'équipements.

[219] Dans le cyberespace les systèmes d'information sont interconnectés sur des réseaux.[206] Les réseaux peuvent exister tant à l'intérieur d'un SI qu'en dehors de celui-ci, lorsqu'il est connecté à d'autres SI. Ceci posé, il est indispensable de considérer la stabilité du réseau comme tel, pour en tirer des conclusions sur la fiabilité du système d'information. Parmi les technologies, les réseaux tiennent la place d'un facteur important dans la conception de SI fiables.

---

[203] Système de communication privé, circonscrit géographiquement, reliant en réseau l'ensemble des ordinateurs d'une entreprise., Office de la langue française, *Signet*,
source : http://w3.olf.gouv.qc.ca/banque/index.asp, visitée en février 2002

[204] Gilbert HOWARD, « Ethernet », *Yale University*, *PC Lube and Tune*,
source http://www.yale.edu/pclt/COMM/ETHER.HTM, visitée en mai 2002

[205] Abréviation pour le terme *Transmission Control Protocol.*

[206] Citons des exemples comme les systèmes de compensation de cartes de crédit, les systèmes de téléphones cellulaires, ceux de machines à sous dans les casinos.

ii. Le milieu physique et le matériel

[220] Comme le souligne Vincent Gautrais[207], il serait injustifié de considérer que le passage du papier à l'électronique amène un désintéressement du caractère physique. L'environnement physique se compose de lieux de stockage, de serrures, de portes, de murs, de coffres-fort et d'alimentation électrique pour ne mentionner que ces items. Les contrôles physiques aussi font partie intégrante de l'encadrement des SI, tels les systèmes d'alarme, la patrouille, le moniteur de télévision en circuit fermé.[208] Le fonctionnement infaillible des SI est très souvent entravé par des menaces provenant du milieu physique, soient-elles d'ordre humain ou naturel. Les propriétés du milieu physique sont d'une grande importance pour assurer les finalités des SI.

[221] Un autre élément de la couche physique est le matériel, l'ensemble des éléments physiques d'une installation informatique. Il comprend les câbles, les disques durs, les ordinateurs, les cédéroms, les disquettes, les périphériques, les guichets bancaires. Comme toute installation, ces éléments sont susceptibles de faire l'objet de tentatives illicites d'accès et de pannes. Ainsi, la fiabilité du matériel tient à son caractère plus ou moins inviolable *(tamper resistence)* d'une part et sa résistance contre les pannes d'autre part[209]. Le matériel inviolable est celui qui résiste aux tentatives d'atteintes, par exemple l'inviolabilité d'une carte magnétique comme prévention des atteintes à la puce. L'élément du matériel peut être aussi conçu de manière à permettre de détecter les violations, notamment par sa propriété de les rendre évidentes postérieurement. À part l'inviolabilité, le matériel doit aussi pouvoir accomplir ses fonctions avec une probabilité de fonctionnement suffisamment forte.

[222] Après le plan de base, qu'est la strate physique, et avant d'arriver aux images numériques, aux messages électroniques ou toute information qui forme le contenu du monde virtuel et à laquelle appartient aussi la signature électronique, il convient de situer le plan intermédiaire, le code informatique qui fait fonctionner le cyberespace. L'importance

---

[207] V. GAUTRAIS, *loc. cit.,* note 180
[208] *Id.*
[209] Bruce SCHNEIER, *Secrets and Lies: Digital Security in a Networked World*, NY, John Wiley & Sons, 2000, p. 214 - 218

de toutes les subdivisions de cette couche pour l'existence même ainsi que pour les missions du système d'information est capitale.

b. La strate logique – le plan intermédiaire

i. La cryptographie

[223] La cryptographie est l'élément central de la sécurité dans le cyberespace. Elle a une longue histoire qui remonte à l'usage de la langue écrite en Chine ancienne où uniquement certaines classes avaient le privilège d'apprendre à lire et à écrire[210], mais voit son importance augmenter à l'époque contemporaine.

[224] Il serait erroné de croire que la cryptographie revêt une importance pour les processus de réalisation de signatures électroniques uniquement dans le cas des infrastructures à clé publique. Sans doute, c'est dans la création de la signature numérique que la présence des modèles cryptographiques est la plus apparente. Tout de même, les nombreuses applications des schémas de chiffrement font de la cryptographie un élément central pour l'appréciation de la fiabilité de tout processus d'authentification lorsque le cyberespace en est le théâtre.

[225] La technologie de la cryptographie repose sur la connaissance privée que seules les personnes autorisées sont censées avoir. Pour les fins de la protection d'un secret connu d'un nombre déterminé de personnes, la cryptographie met en place des algorithmes de chiffrement de données sensibles. L'application des algorithmes est combinée avec l'utilisation de clés de chiffrement ce qui évite le besoin d'utiliser plusieurs algorithmes pour les communications avec des groupes de personnes différents.

[226] La fiabilité et la stabilité des modèles de chiffrement dépendent de plusieurs facteurs, à savoir les qualités des algorithmes, les capacités des clés, les propriétés des générateurs de clés et les protocoles de mise en fonction.

---

[210] *Id.*, p. 85 – 87. L'auteur stipule que la première utilisation documentée de la cryptographie date de l'année 1900 av.J.-C. et réfère à l'usage de hiéroglyphes non-standardisés. En Mésopotamie la formule de préparation de pots de glaçure était chiffrée sur des tablettes (1500 a.j.c.). D'autres exemples sont le Atbash juif de 500-600 a.j.c., le skytale Grec de 486 av.J.-C. et le chiffre de simple substitution de Jules César de 50-60 av.J.-C.

[227] La qualité des algorithmes est essentielle pour l'efficacité du chiffrement et par de là pour la sécurité du SI. Avant qu'un algorithme soit lancé par la communauté cryptographique, il doit surmonter avec succès de nombreuses épreuves. Le choix entre des algorithmes propriétaires et publics a donc une grande signification car ces derniers auront eu à franchir avec succès le test que constitue l'examen par leurs utilisateurs. Des arguments peuvent formulés en faveur des deux types d'algorithmes, mais la question ici n'est pas d'identifier la meilleure politique de choix d'outils cryptographiques, mais plutôt d'exposer les facteurs qui déterminent la fiabilité d'un modèle cryptographique.

[228] Les algorithmes peuvent être grossièrement classifiés selon deux types, à savoir les algorithmes symétriques et asymétriques. Ainsi, parmi les algorithmes symétriques, ceux qui autorisent le chiffrement et le déchiffrement à l'aide de la même clé, DES[211] a trouvé une application dans des milliers de produits. D'autres exemples d'algorithmes symétriques méritent d'être mentionnées, tels que triple DES, RC4[212], RC5[213], IDEA[214], Blowfish[215] ou l'algorithme standardisé du gouvernement américain - AES.[216] Ces standards sont mis en place pour sécuriser le courrier électronique, les fichiers personnels sur un disque dur, les transactions électroniques bancaires, les codes des missiles nucléaires. Ils ont aussi un rôle direct ou indirect dans les procédés de réalisation de signature.

[229] L'autre modèle cryptographique, la cryptographie asymétrique, se base sur l'utilisation de deux clés différentes, une pour coder le message et l'autre pour le déchiffrer. Ceci est possible grâce à la mise en place d'un algorithme qui est facilement exécutable dans une direction et difficilement réalisable dans le sens inverse. Le modèle rappelle la multiplication de 2 chiffres dont le résultat peu être facilement obtenu alors qu'il existe une quasi impossibilité à deviner efficacement les chiffres initiaux à partir de ce même résultat[217]. De nos jours il existe quelques standards d'algorithmes asymétriques comme

---

[211] Abréviation pour le terme *Digital Encrytption Standart.*
[212] Bruce SCHNEIER, « Security », *Counterpane Internet Security*, *Crypto-gram Newsletter*, 15 mars 2001, source: http://www.counterpane.com/crypto-gram-0103.html , visitée en mai 2002
[213] *Id.*
[214] Marx Software Security, « CRYPTO-BOX Stands Alone Using Internationally Acclaimed Algorithm», *News*, source: http://www.marx.com/news/1999/apr07.html, visitée en mai 2002
[215] Bruce SCHNEIER, «The Blowfish Encryption Algorithm», *Counterpane Internet Security*, *Counterpane Labs*, 2002 , source: http://www.counterpane.com/blowfish.html, visitée en mai 2002
[216] B. SCHNEIER, *op. cit.,* note 209, p. 89
[217] *Id.*, p. 95

RSA[218], ElGamal[219], les courbes elliptiques[220]. Malgré la commodité de la cryptographie asymétrique, les méthodes cryptographiques modernes se servent le plus souvent d'une approche hybride des deux types de chiffrement. La sécurité du courrier électronique[221], celle des transactions sur le Web[222], la sécurité TCP/IP et celle des communications téléphoniques reposent sur des solutions combinant les deux mécanismes de chiffrement, symétrique et asymétrique.

[230] En deuxième place viennent les générateurs de clés de chiffrement. Presque tous les systèmes informatiques sont basés sur des générateurs de numéros aléatoires qui servent à la création de clés ou d'autres valeurs uniques. Or, les mathématiciens sont unanimes à dire qu'un vrai caractère aléatoire est impossible à atteindre. L'accent est plutôt porté sur le caractère imprévisible et non-reproductible des numéros générés, comme en étant les caractéristiques essentielles. Pour la génération de numéros aléatoires un grand nombre de phénomènes peuvent être utilisés, tels le caractère aléatoire des circuits de courant à l'intérieur du matériel, les mouvements physiques de l'usager. La technologie de la génération de ces numéros est à la base de la génération de clés de chiffrement dans un grand nombre de cas.

[231] Toujours dans le contexte des modèles cryptographiques, l'utilisation de mots de passe est fréquente et ses finalités variées, comme par exemple la génération de clés de chiffrement. Les mots de passe peuvent énormément varier en complexité. Leur diversité est énorme, à commencer par des exemples comme « motdepasse » ou « 1234 » jusqu'à des combinaisons se distinguant par une sophistication admirable. La qualité de cette source de création de clés de chiffrement est significative pour la solidité des clés mêmes et pour l'efficacité du chiffrement auquel elles servent. La qualité des mots de passe peut être mesurée de bien de façons parmi lesquelles on compte la complexité. Les statistiques montrent que 16 pour cent des mots de passe se composent de 3 ou de moins de 3 caractères et 86 pour cent sont encore plus faciles à compromettre. La complexité des mots

---

[218] RSA Security, « What are some of the more popular techniques in cryptography? », *RSA Laboratories*, *Frequently Asked Questions About Today's Cryptography*, source : http://www.rsasecurity.com/rsalabs/faq/1-3.html, visitée en mai 2002

[219] *Id.*

[220] *Id.*

[221] La sécurité du courrier électronique est assurée moyennant les protocoles PGP, PEM, S/MIME. IETF, « Examples of S/MIME Messages », *Groupe de travail S/MIME Mail Security*, 5 novembre 2001 Internet Draft , source : http://www.ietf.org/internet-drafts/draft-ietf-smime-examples-07.txt, visitée en mai 2002

[222] RSA Security, *op. cit.*, note 218

de passe n'est pas cependant une panacée pour la sécurité des SI. Le contexte dans lequel le mot de passe est utilisé est aussi important. Des systèmes avec des interfaces manuelles, tels les guichets bancaires, peuvent être fiables, grâce à des NIP de quatre chiffres. Cependant, dans le cas d'une interface informatique, des mots de passe de cet ordre n'assurent pas le même degré de certitude. Pour sécuriser la source de génération des clés de chiffrement, les experts ont souvent recours à des techniques combinées, faisant appel à des mots de passe, auxquels des chiffres aléatoire sont rajoutés. Le changement régulier des mots de passe est aussi susceptible d'augmenter la fiabilité du recours à cette technique.

[232] Une autre composante de la fiabilité du chiffrement est la longueur des clés. Les algorithmes symétriques utilisent des clés de différente longueur, allant de 90 bits jusqu'à 256 bits (les clés du Advanced Encryption Standart du Gouvernement américain). Pour ce qui est des algorithmes asymétriques, les experts recommandent des longueurs de 1024 bits ou plus. Cependant, il ne serait pas justifié d'associer la fiabilité d'un modèle de chiffrement uniquement à la longueur des clés qui sont utilisées.

[233] Les prérequis à l'existence d'un schéma cryptographique étant exposés, il faut examiner une dernière condition très importante à la fiabilité du chiffrement. Elle tient à la façon dont les outils cryptographiques sont organisés et activés et elle est centrale pour déterminer l'efficacité de la technologie. Cette organisation se manifeste dans la forme de protocoles cryptographiques. Les protocoles réfèrent à un ensemble de règles et d'étapes prédéterminées selon lesquelles se déroule une application cryptographique. À ce chapitre, les exemples ne manquent pas. La sécurisation des échanges de courriers électroniques sur Internet s'effectue au moyen de S/MIME ou Open PGP. Le protocole SSL a été inventé par Netscape pour la sécurisation du commerce électronique du type client-serveur. Les paquets de données IP sont protégés par le Point-to-Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP) et IPsec. SET qui n'a pas atteint l'application souhaitée par ses concepteurs VISA et Mastercard, était destiné à des transactions sécuritaires de cartes de crédit sur Internet. SSH est conçu pour authentifier les connexions de lignes de commande à distance, PKIX et SPKI s'occupent des schémas de signatures numériques.

[234] Ainsi nous avons exposé les éléments de la stabilité des applications cryptographiques. La fiabilité d'une technologie cryptographique est un concept qui a de

multiples aspects dont certains ont été mentionnés. Tous ces aspects déterminent, en partie, les caractéristiques et la fiabilité du plan intermédiaire du cyberespace qu'est le code.

ii. Les logiciels

[235] La présence de cet élément logique dans la structure du cyberespace, y compris dans les procédés de réalisation de signatures électroniques, est incontournable. Par conséquent, la fiabilité des applications logicielles au sein d'un SI est d'une portée majeure pour la performance de l'ensemble du système. Il est à noter que les caractéristiques des logiciels ont évolué tout comme le processus de leur création. Dans les années '70 la programmation était un processus qui se distinguait surtout par sa complexité[223]. Les programmes étaient difficiles à écrire et à maintenir. Ensuite la programmation a pris une orientation différente, à savoir la division des programmes en plus petites composantes plus indépendantes et modulaires. Dans ce courant s'inscrit la programmation orientée objet[224] selon laquelle un système est bâti par de composantes qui se divisent en sous-composantes[225] et ainsi de suite. De cette manière même si un programme est assemblé dans un seul produit, il se compose de plusieurs éléments[226] pouvant dans une bonne mesure être mis au point de façon indépendante ce qui multiplie les facteurs de sa précision. En contrepartie, des complications concernant la fiabilité des logiciels ont été introduites par l'assemblage dynamique. Avant l'introduction de cette méthode, les modules du produit logiciel étaient assemblés par le concepteur et testés ensemble. Désormais, les composantes sont souvent liées de manière dynamique lorsque l'application est lancée. Dans les systèmes Windows le couplage dynamique s'effectue par de bibliothèques dynamiques (DLLs). Des équivalents existent dans Unix et Macintosh.

[236] Ceci dit, il est évident que le concept de fiabilité du logiciel emprunte une forme qui se distingue par une double complexité. Pour atteindre le degré de précision requis, il faut d'abord que les composantes d'un programme soient stables pour assurer le fonctionnement

---

[223] B. SCHNEIER, *op. cit.,* note 209, p. 354
[224] *Id.*, p. 355
[225] Un fureteur contient en soi une machine virtuelle Java. Elle de sa part est composée par des miniapplications Java. Les macros sont des composantes d'un processeur Word ou d'un tableur., *Id.*, p. 356
[226] Par exemple Microsoft Word repose sur l'interaction de plus de 1000 composantes.

fiable de l'application. Ensuite, les éléments et les sous-éléments doivent fonctionner correctement dans toutes les configurations possibles. Les systèmes d'exploitation modernes ne sont pas conçus de manière assurer une solution globale à ce double problème. Selon le modèle plus ancien, le système d'exploitation agissait comme intermédiaire entre les différents éléments de logiciel et prévenait les conflits. Les composantes modernes sont en connexion directe et n'utilisent plus le système d'exploitation pour interagir.

[237] Les réflexions sur la complexité du concept de fiabilité des applications logicielles, seraient incomplètes sans mentionner que certains produits, fonctionnant au sein de beaucoup d'organismes, sont le résultat de développements internes (nommés des développements « maison »), ce qui réduit la possibilité d'essais de fonctionnement à grande échelle.

[238] Ces composantes de la strate logique (la cryptographie et les logiciels) ayant été mises en relief, l'importance de leur fiabilité pour la fiabilité du SI se révèle. Reste un dernier élément que ce plan intermédiaire du cyberespace vise à gérer : les ressources et les informations qui forment le contenu du monde virtuel.

c. La strate supérieure - le contenu du cyberespace

[239] Selon Lessig[227], le contenu du cyberespace est formé par ce qui est dit et transmis dans le monde virtuel. L'auteur y situe les images numériques, les textes, les films en ligne. Le contenu représente l'information acheminée, sauvegardée, traitée, archivée et rendue fonctionnelle par les moyens du cyberespace. Dans ce texte, l'information est avant tout la signature électronique. Le processus technologique de création de la signature électronique réside dans les deux premières couches du cyberespace - c'est grâce à des dispositifs physiques (appartenant à la strate physique) et logiques (faisant partie du *code* ou de la strate logique) qu'une signature est réalisée. Pourtant la signature en tant que résultat de ce processus n'est qu'une donnée porteuse d'une certaine information qui, tout comme les autres éléments du *contenu* du monde virtuel, est créée, apposée, transmise, vérifiée, et rendue fonctionnelle dans la strate supérieure du cyberespace. C'est d'ailleurs sous cet angle que le droit l'appréhende. Aux termes des cadres législatifs étudiés, elle réfère à une

[227] L. LESSIG, *op. cit.,* note 7, p. 23

donnée identifiant son auteur et le liant au contenu de l'acte signé. Ainsi, les allégations que la signature établit peuvent être vraies ou fausses alors, comme élément du contenu du cyberespace, elle peut être authentique ou contenir de l'information contraire à la réalité. Les garanties de l'authenticité de l'information sont recherchées par le droit dans le procédé d'authentification au sujet duquel se pose la question de fiabilité. En fin de compte, la fiabilité du procédé de signature est une résultante de la performance de son milieu ambiant, c'est-à-dire, des capacités de l'architecture du cyberespace.

Section II – LES VULNÉRABILITÉS DE L'ENVIRONNEMENT

[240] Jusqu'à présent nous avons présenté la structure du cyberespace, y compris de son noyau qu'est le SI, affirmant que la fiabilité de chacun des éléments participe de la fiabilité du système dans sa totalité. Maintenant nous nous pencherons sur les risques et leur gestion - les phénomènes qui compromettent ou affermissent la fiabilité des composantes de l'environnement et, par-là, des procédés servant à l'apposition de signatures électroniques. Dans les pages qui suivent nous allons identifier les points de vulnérabilité du SI et de ses composantes. Ensuite nous mentionnerons les mesures de protection, de détection et de réaction possibles contre les risques identifiés. Le choix des contre-mesures et de politique sécuritaire effectué dans un processus d'évaluation et de gestion du risque nous occupera ensuite comme étant un aspect fondamental de la fiabilité.

§1. Les risques menaçant le bon fonctionnement de l'architecture

[241] Les risques existant en matière de signature électronique peuvent être facilement définis par leurs conséquences. Ainsi, lorsque la signature identifie la signataire et démontre son attitude envers le texte signé, tout phénomène susceptible de mener à la non-identification du vrai signataire et, éventuellement, à la répudiation du message de la part de celui-ci représente un risque pour la fiabilité du procédé de signature. Il en est de même pour tout incident conduisant à l'identification d'une personne autre que le signataire. Aussi, dans le cas où une modification postérieure du contenu de l'écrit signé, représentant

une compromission de l'intégrité de l'acte, est susceptible de survenir, la fiabilité du moyen de signature serait entachée de vice. Ces conséquences non désirées peuvent être provoquées par un large spectre de périls différents.

[242] Il existe des risques inhérents à l'échange de données sur support papier. Ces risques sont relativement bien connus et des solutions ont été dégagées par une longue expérience.[228] Le cyberespace est un monde aussi dangereux, mais moins connu. L'énumération des risques propres au monde virtuel est une tâche importante mais par trop ambitieuse dans le cadre de cette étude. Cependant, il serait possible de classifier les menaces et leurs sources afin d'obtenir une image générale des vulnérabilités de l'environnement de la signature électronique.

[243] Les risques peuvent être regroupés en trois catégories, à savoir les accidents, les erreurs et les fraudes[229]. Notons que dans la troisième catégorie nous envisagerons tous les risques découlant d'un comportement humain malveillant qui comprennent les fraudes proprement dites, mais aussi d'autres sources de risque de nature humaine intentionnelle.

a. Les accidents et les erreurs

[244] Les risques accidentels sont ceux qui entraînent une destruction partielle ou totale de l'équipement, des supports informatiques ou de leur environnement. Il s'agit par exemple des incendies, des inondations, de la fumée, des tremblements de terre, des grèves, en fait de tout type d'accident susceptible non seulement d'entraver le bon fonctionnement du SI, mais aussi d'en détruire les équipements et d'en menacer l'architecture.

[245] Les risques attribuables aux erreurs ne peuvent non plus être ignorés. Nous arrêterons notre attention plus particulièrement sur les erreurs dans la conception des logiciels et leur application et celles attribuables aux acteurs intervenant dans le fonctionnement des SI.

---

[228] P. TRUDEL, G. LEFEBVRE, S. PARISIEN, *op. cit.,* note 61, p. 66
[229] *Id.*, p. 67

[246] Comme le soutient Mireille Antoine, tout programme est susceptible de contenir des erreurs.[230] Elles peuvent concerner tant la conception que l'implémentation.[231] Les erreurs de nature logicielle sont un problème persistant des systèmes informatiques complexes, telles les grandes bases de données, les logiciels de réseau, les microprocesseurs complexes. Les vices peuvent concerner le design comme par exemple l'activation simultanée de deux logiciels identiques sur le système primaire et le système de copies de sauvegarde. Les défauts d'implémentation, de programmation et d'usage sont aussi fréquents. Dans cette perspective, la fiabilité du logiciel consiste en sa capacité de fonctionner malgré la survenance d'erreurs. Il est également possible de tenter de les prévenir en faisant scruter les applications logicielles par un large groupe d'utilisateurs sur divers types de matériel, dans un grand nombre de configurations possibles et pour des fins diverses. Dans cet esprit, la technique du test bêta[232] apparaît comme un moyen efficace. Cette méthode de vérification permet d'identifier les vices et de les corriger et c'est de sa profondeur et ampleur que dépend la résistibilité du logiciel contre les défaillances inattendues.

[247] Une autre source d'erreurs très importante tient au facteur humain. Nous avons déjà constaté que les personnes physiques interviennent dans les activités des SI à plusieurs étapes et en différentes qualités. L'influence des acteurs sur la fiabilité des systèmes d'information est majeur et il a mérité l'attention particulière des législateurs. Citons à titre d'exemple l'annexe II (e) de la Directive européenne et la jurisprudence américaine relative à la fiabilité des systèmes d'information[233].

[248] Il est certain qu'en ce qui concerne les acteurs, l'appréciation de leurs compétences professionnelles figure en bonne place dans l'analyse de leur fiabilité. Néanmoins, celle-ci

---

[230]Mireille ANTOINE, Marc ELOY, Jean-François BRAKELAND, « Droit de la preuve face aux nouvelles technologies de l'information », dans Cahiers du CRID, Namur, CRID, 1992, 13

[231] L'exemple de la fusée de l'Agence spatiale européenne, Ariane 5 est éclairant. En 1996 l'engin spatial a explosé après le lancement à cause d'une erreur de logiciel qui essayait d'insérer un numéro de 64 bits dans un espace de 16 bits entraînant un dépassement de capacité. La NASA a vécu la même triste expérience avec son satellite vers la planète Mars dont la disparition a été provoquée par un vice de conversion de données., B. SCHNEIER, *op. cit.,* note 209, p. 203. La grande nouvelle du mois de décembre était la découverte d'un vice de sécurité dans le connecteur universel de Microsoft, une entité centrale dans certains produits Windows. Le défaut permettait la prise de contrôle de l'ordinateur qui s'en sert., B. SCHNEIER, *op. cit.,* note 212

[232] Le terme fait appel à un test d'un produit informatique en cours de développement effectué par des utilisateurs choisis (clients privilégiés ou testeurs professionnels) afin de déterminer s'il subsiste encore des erreurs de logique ou de fonctionnement avant la commercialisation., Office de la langue française, *Signet*, source : http://w3.olf.gouv.qc.ca/terminologie/fiches/8370739.htm, visitée en mai 2002

[233] *supra*, par. 167 - 170

ne réfère pas seulement aux habilités professionnelles. Selon Schneier[234], les facteurs de nature humaine qui exercent une influence sur la stabilité des systèmes et qui peuvent s'avérer la source d'erreurs, sont au nombre de trois, à savoir la manière dont les acteurs perçoivent les risques, leur façon de gérer des situations exceptionnelles et l'interaction entre les intervenants et les ordinateurs.

[249] Les acteurs doivent être capables de définir les vulnérabilités du système d'information dans lequel ils sont impliqués afin d'apprécier avec justesse la dangerosité particulière de chaque type de circonstances. Cette appréciation se fait sur la base d'un calcul de probabilité de survenance d'un risque et consiste en attribution au regard de l'importance attribuée à l'information. Par ailleurs, la façon dont les intervenants réagissent dans des circonstances exceptionnelles est déterminante pour la fiabilité du fonctionnement des SI. La troisième source potentielle d'erreurs est le contact entre les hommes et les SI. Le lien entre les systèmes d'ordinateurs et les utilisateurs s'effectue au moyen des interfaces homme-ordinateur. Les interfaces aident les acteurs à mieux comprendre la sécurité et à y participer efficacement. Le manque de formation concernant la gestion des interfaces pourrait provoquer des erreurs flagrantes et désastreuses comme l'insertion d'un virus au moyen de pièces jointes à des messages électroniques.

[250] Les erreurs de nature humaine sont susceptibles de causer des défaillances et d'affecter la fiabilité des SI. Le facteur humain est, d'autre part, la source d'un autre groupe de risques très importants, impliquant un comportement intentionnel. Il s'agit notamment des attaques.

b. Les attaques

[251] La complexité des SI et la créativité des attaquants ne nous permettent pas de produire un exposé exhaustif de ce type de menaces. Nous en établirons cependant une typologie à partir de laquelle seront introduites des mesures formant le socle de la politique sécuritaire.

---

[234] B. SCHNEIER, *op. cit.,* note 209, p. 255 - 261

i. Les attaques et les attaquants

[252] L'identification des différents groupes d'attaquants fait partie intégrante du paysage virtuel et est une étape importante dans le processus de gestion du risque. Elle nous permet non pas d'énumérer tous les types de sources possibles d'atteintes de nature intentionnelle, mais plutôt de les regrouper afin de tirer des conclusions sur les profils des attaques qui peuvent survenir, tels l'expérience des attaquants, leur propension à assumer un risque, les moyens et les ressources dont ils disposent, leurs objectifs et l'accès qu'ils ont aux systèmes[235].

[253] Les pirates informatiques sont la catégorie à mentionner en premier lieu. Ils forment une communauté qui possède ses propres caractéristiques, des pseudonymes, son propre langage et ses règles de conduite.[236] Il existe des *newsgroup* pour ces communautés, des sites Web et des conventions. Selon les experts, globalement ils possèdent une connaissance technologique de base, mais ils ont une expérience considérable. La majorité d'entre eux ont des ressources financières relativement modestes et ne sont pas enclins à courir des risques majeurs. Leurs accès aux SI sont aussi limités, ils abordent les systèmes de l'extérieur. Ce type de profilage en fonction de l'expérience, la propension à assumer un risque, les moyens et les ressources à disposition, les objectifs poursuivis et l'accès aux systèmes peut être effectué non seulement par rapport aux pirates informatiques, mais encore par rapport à d'autres groupes d'attaquants comme les criminels isolés, les employés malicieux, les espions industriels, les criminels organisés, les activistes terroristes et ainsi de suite.

[254] Les attaques, tout comme leurs auteurs, peuvent aussi être de différente nature. Pour le commerce électronique en premier lieu vient la fraude. C'est une attaque contre tout système commercial nonobstant son support. Tous les instruments commerciaux ont fait l'objet de contrefaçons, l'argent, les certificats de valeurs mobilières, les cartes de crédit, les chèques, les lettres de crédit. Le commerce électronique ne fait pas exception et il est lui aussi la cible de fraudes. Il ne faudrait pas oublier d'attribuer les places méritées à d'autres

---

[235] *Id*., p. 42 - 58
[236] *Id.*, p. 43 - 46

catégories d'attaques comme les attaques destructives[237], les attaques publicitaires non directement lucratives.[238]

[255] Ce bref survol des types d'attaquants et d'attaques est important pour fournir ensuite la base de l'identification des risques auxquels un SI concret est susceptible d'être la cible. Cette analyse offre des pistes de réflexion sur la nature possible des attaques, dont la compréhension et l'évaluation précises sont partie intégrante de la fiabilité des systèmes d'information.

ii. Les attaques contre les différents éléments des SI

[256] Les attaques contre un SI prennent la forme de tentatives d'atteintes concrètes contre une ou plusieurs de ses composantes - le facteur humain, les réseaux, la cryptographie, les logiciels. Puisque chaque unité du système d'information participe à la stabilité de l'environnement et à la fiabilité des processus qui s'y déroulent, les violations de chacun de ses éléments peuvent être en mesure de compromettre ces valeurs. Enfin, ce sont les attaques concrètes contre les éléments de l'environnement qui dictent les mesures de protection et par-là, les principes de la politique sécuritaire.

[257] Parmi les attaques les plus réussies, celles contre les acteurs se distinguent par leur efficacité. Le *social engineering*[239] est une attaque qui n'est pas associée à l'environnement informatique des SI, mais cible le lien le plus faible dans le paysage sécuritaire des systèmes – le facteur humain. L'essence de cette attaque consiste à persuader une personne, impliquée dans le fonctionnement d'un SI, d'agir de la manière désirée par l'attaquant. C'est fréquemment ainsi que des informations sensibles – des codes, des mots de passe et des comptes – ont été obtenus par les personnes malveillantes.[240]

---

[237] En 2000 une vague massive de pareilles attaques a été lancée contre des sites oeuvrant dans le domaine du commerce électronique parmi lesquels étaient Amazon.com, E Trade, Buy.com, eBay, Yahoo!.

[238] L'exemple en est le retard de Sony de lancer un nouveau produit suite à une attaque contre la sécurité de la technologie DVD.

[239] B. SCHNEIER, *op. cit.,* note 209, p. 266 - 269

[240] En 1993 les utilisateurs du prestataire de services Internet Phantom Access, ont reçu un message électronique stipulant que leurs comptes avaient été attaqués et qu'ils devaient temporairement changer leurs mots de passe à « DPH7 ». Ce message falsifié est un exemple illustratif de social engineering, comme l'est le message que les utilisateurs de AOL reçoivent à titre régulier, stipulant que leurs comptes ont été abolis par la suite d'une attaque et que les administrateurs du système nécessitent les mots de passe des usagers pour accéder aux copies de sauvegarde., *Id.* p. 267

[258] Les attaques contre les outils cryptographiques peuvent cibler les algorithmes, les clés et les protocoles. Pour briser un algorithme cryptographique, une possibilité est l'attaque *cyphertext only*. Dans ce cas l'attaquant ne connaît que le texte encrypté et doit en déduire le texte en clair. Cependant les algorithmes modernes sont suffisamment fiables pour résister à ce type d'atteinte. Une autre possibilité est l'attaque de texte en clair connu. Pour réaliser cette attaque le fraudeur dispose du texte en clair et du résultat chiffré, ce qui lui permet de se procurer la clé de chiffrement. Par exemple, tous les fichiers Microsoft Word commencent avec la même entête, interne pour le programme et invisible pour l'utilisateur, qui consiste en une séquence de bits connue. Cette séquence peut souvent offrir le texte en clair dont l'attaquant a besoin pour découvrir la clé de chiffrement. Le texte en clair faisant objet du chiffrement peut aussi être intentionnellement choisi par l'attaquant. Cette attaque est effective contre les systèmes de cartes à puce dans lesquelles le fraudeur peut insérer un message selon son gré.

[259] Parmi les attaques contre les clés, les attaques de force brute sont les plus simples et les plus connues. L'essai de toutes les clés possibles, l'essence de la technique, n'est pas toujours impensable selon la capacité et la puissance de l'ordinateur dont l'attaquant dispose. Cette attaque appliquée contre un mot de passe peut emprunter la forme d'une attaque de dictionnaire, selon laquelle les combinaisons essayées seront des mots de dictionnaire. En ce qui concerne les protocoles cryptographiques l'attaque la plus populaire est celle dite de « l'homme au milieu »[241]. Elle consiste en l'inclusion d'un intermédiaire entre deux personnes en communication, persuadées, l'une et l'autre d'agir en connexion directe, telle que prescrit par le protocole de leur interaction.

[260] Le code malicieux et toutes ses variations illustre l'attaque contre le logiciel. Selon les statistiques, il existe de nos jours entre 10 000 et 60 000 virus qui, classifiés par les similitudes de leurs technologies, forment le premier groupe de code malicieux.

[261] Les contaminateurs de fichiers sont parmi les plus connus de ces virus. Selon leur technologie, ils s'attachent à une application et, après son lancement, s'installent dans la mémoire du système pour infecter d'autres applications. Les virus de secteur d'amorçage sont moins connus, mais aussi dangereux car ils sont hébergés dans une partie du disque

---

[241] Bhavin Bharat BHANSALI, « Man-In-the-Middle Attack - A Brief », *System Administration, Networking, and Security Institute*, *Reading Room*, 16 février 2001, source: http://rr.sans.org/threats/middle.php, visitée en mai 2002

dur d'où ils peuvent se propager sur toutes ses parties, les disquettes et les autres systèmes. Les virus se propageant le plus rapidement sur Internet sont les macro-virus. Les vers (worms) sont d'autres exemples de logiciel malicieux qui diffère des virus par son indépendance. Les vers ne sont pas intégrés dans d'autres programmes, mais constituent eux-même des programmes auto-reproductibles et exécutables. La troisième catégorie de logiciel malicieux regroupent les chevaux de Troie, qui dissimulent un malice sous des dehors inoffensifs.

[262] Pour ce qui est des attaques contre le matériel, nous ne mentionnerons que TEMPEST[242] qui se caractérise par son coût très élevé et l'exigence d'équipement spécial. Cette attaque repose sur le fait physique que tout dispositif de l'équipement électronique émet des radiations, nommée radiations de Van Eck[243]. Ces radiations sont susceptibles d'être captées par un récepteur sensible et d'être ensuite analysés par des moyens électroniques afin de révéler l'information véhiculée. L'attaque et la protection (un bouclier TEMPEST) sont extrêmement coûteuses, mais possibles. D'autres possibilités d'attaque au matériel sont les attaques qui utilisent des facteurs comme l'irradiation de chaleur par les outils électroniques, la détection de la consommation d'électricité ou les bruits des réseaux.

[263] Les ordinateurs et les systèmes d'ordinateurs sont sensibles aux attaques de *refus de service*. La saturation d'un système avec de l'information peut causer un dysfonctionnement qui pourrait être utilisé à des fins frauduleuses ou simplement maintenir le système hors service pendant une certaine période de temps. L'efficacité de ces attaques peut être augmentée par leur distribution et leur automatisation. L'attaquant peut profiter de plusieurs ordinateurs sur Internet pour y installer, à l'insu de leurs propriétaires, des programmes malicieux, qui feraient de chaque ordinateur un attaquant séparé et de cette manière distribuerait et automatiserait l'attaque de refus de service.

[264] L'analyse du trafic est un autre exemple d'attaques contre les réseaux. Même si les messages circulant dans les réseaux sont cryptés et illisibles, l'analyse de leur volume, leur intensité et leur fréquence est révélatrice pour l'attaquant. Les attaques contre les réseaux, tout comme celles contre les autres éléments des technologies de l'information et des unités des systèmes d'information, on le voit, peuvent être extrêmement variées, cependant

---

[242] Michael MCCARTHY, « Security Woe: Computer-Screen Spies », *ZDNET*, *ZDNET Technology News*, 6 Août 2000, source: http://zdnet.com.com/2100-11-502732.html?legacy=zdnn, visitée en mai 2002

[243] *Id.*

l'Étude de toute cette abondance d'activités malveillantes ne fait pas l'objet spécifique de notre étude.

[265] Les attaques, tout comme les risques sont des phénomènes inhérents au paysage du processus de la signature électronique. Leurs capacités à compromettre leurs finalités ne sauraient être sous-estimées. Par conséquent, l'analyse du standard de fiabilité des moyens de signature électronique ne peut se désintéresser de l'aptitude desdits moyens à résister aux risques du monde virtuel.

§2. La gestion des risques – une tentative de maîtrise de l'environnement

a. L'élément de base de la gestion des risques - les contre-mesures

[266] Les contre-mesures sont des méthodes pour réduire les vulnérabilités. Elles ont été développées par la communauté informatique et par la société civile. Il ne serait pas inexact de dire que toutes les vulnérabilités identifiées possèdent leurs contreparties parmi les contre-mesures. Ainsi, le choix de produits logiciels fiables diminue le risque de défauts causés par cet élément. Les programmes anti-virus et leur mise à jour régulière fournissent une protection contre les logiciels malicieux. La formation du personnel diminue sans doute les erreurs d'origine humaine et une bonne politique de recrutement et de contrôle est en mesure de parer à l'essentiel des tentatives malveillantes des employés. Parmi les contre-mesures concrètes les exemples sont innombrables, tels les coupe-feu, les zones démilitarisées, les réseaux virtuels privés, les scanners de vulnérabilités, les systèmes de détection d'intrusions[244] qui repèrent des anomalies dans le fonctionnement d'un système.

[267] Selon leurs finalités, les contre-mesures peuvent être divisées en trois catégories : des mesures de protection, de détection et de réaction[245]. Les mesures de protection réduisent la possibilité que des défaillances surviennent. Celles de détection sont destinées à signaler la survenance de défaillances et d'attaques et finalement les contre-mesures de

[244] Les « pots de miel » sont un sous-type de systèmes de détection d'intrusions. Ils représentent des parties du SI qui sont conçues dans le but de paraître attrayantes aux personnes malveillantes, de devenir la cible de leurs attaques afin d'alarmer les administrateurs de systèmes.

[245] B. SCHNEIER, *op. cit.,* note 209, p. 279

réaction sont mises en fonction pour éviter les dommages qu'une défaillance serait susceptible de causer. Très souvent elles coexistent au sein d'un SI. La protection contre les défaillances va de pair avec leur détection.

[268] Les contre-mesures se distinguent par une diversité qui ne le cède en rien à celle des vulnérabilités. Il se pose bien sûr la question de leur efficacité et des vulnérabilités que les contre-mesures elles-mêmes peuvent contenir, ceci faisant aussi partie du profil fiable d'un SI. Cependant, il faut avouer qu'une bonne politique sécuritaire n'est pas une simple combinaison de contre-mesures. La politique sécuritaire, qui fait partie de la fiabilité des SI, réfère à un choix éclairé de mesures de protection adéquates. L'étude des risques et leur impact sur la fiabilité des systèmes nécessite l'analyse de la politique sécuritaire qui résulte d'un processus de gestion du risque.

b. L'adoption de politique sécuritaire – le modelage de l'environnement selon les besoins

[269] La gestion du risque implique en premier lieu une étape de *risk modeling*. Ce concept désigne une analyse des risques véritables qui menacent le système et commence par l'étude et l'identification des vulnérabilités réelles qu'un SI peut contenir. La compréhension du paysage varié des vulnérabilités est la clé de la prise de décisions adéquates en faveur la fiabilité des systèmes. Il est évident qu'un SI peut présenter un grand nombre de possibilités de défaillances. Tout de même, ces possibilités ne présentent pas toutes des menaces réelles à son fonctionnement. Le mode de fonctionnement du SI, ses objectifs et les valeurs qu'il protège permettent d'ignorer certaines menaces comme étant négligeables. Les particularités spécifiques d'un SI peuvent nous fournir des indices sur le degré de sécurité requis. Il est tout à fait possible de soutenir que les menaces au bon fonctionnement du système, provoquées par ses vulnérabilités, ne sont pas toutes pertinentes et la compréhension adéquate du paysage des vulnérabilités implique une sélection de celles qui représentent des véritables risques, compte tenu des objectifs du système, de ses différents usages, ainsi que des circonstances particulières d'utilisation.

[270] L'étape de *risk modeling* est suivie par une évaluation du risque, afin d'en établir un prix. Les probabilités de leur survenance sont aussi des valeurs qui sont susceptibles d'être

statistiquement déterminées. À l'issue de cette analyse le résultat obtenu exprime le degré de dangerosité. La compréhension des véritables risques et leur évaluation est essentiellement empirique et constitue la première étape de l'adoption de politique sécuritaire.

[271] Cette étape permet de définir les besoins du fonctionnement du SI qui se matérialisent ensuite par l'adoption d'une politique sécuritaire. Celle-ci réfère à des impératifs généralement définis qui sont censés augmenter la stabilité du fonctionnement de l'ensemble et sa fiabilité. La politique sécuritaire peut se manifester par des directives concernant divers domaines de l'activité du SI, à partir des méthodes de recrutement, de la politique d'achat de logiciels, des pratiques de négociations jusqu'aux questions relatives à la gestion des accès, les choix d'algorithmes cryptographiques, la prise de décisions sur le besoin de l'installation d'un coupe-feu ou un bouclier *TEMPEST*[246]. Finalement, la politique sécuritaire est implémentée moyennant des contre-mesures de protection, de détection et de réaction qui en assurent l'efficacité.

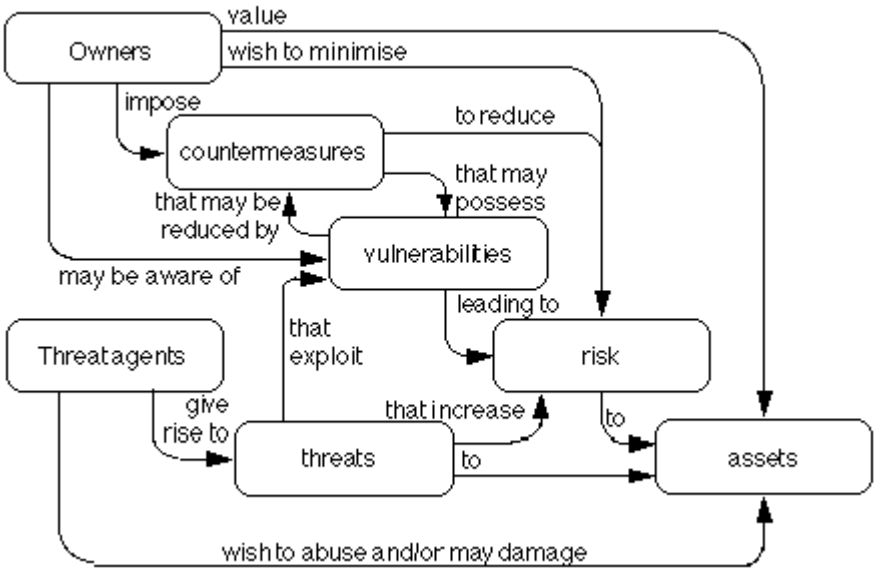


Image 4. *Schéma général du processus de sécurité. L'image est disponible sur* http://www.commoncriteria.org/index.html*, visité en mars 2002*

[246] Le bouclier TEMPEST fournit une protection contre l'attaque TEMPEST, *supra,* par. 262

[272] La gestion du risque est une activité qui vise à maîtriser l'environnement informatique. Ce processus sécurise le système d'information auquel il est appliqué et renforce la certitude que les finalités du système soient atteintes avec une précision et une qualité suffisantes. C'est en partie dans la sécurisation de l'environnement que le processus de réalisation de signature trouve les fondements de sa fiabilité. Ce lien souligne encore une fois l'identité entre l'état des capacités de l'environnement virtuel, et la fiabilité du moyen de production de signatures informatiques qui s'y prépareront.

En conclusion de ce chapitre consacré à la fiabilité de l'environnement de la signature électronique, nous tenons à rappeler la distinction entre l'authenticité de la signature, la fiabilité du moyen de sa réalisation et la fiabilité du cyberespace. En effet lorsque l'on s'interroge sur le caractère fiable d'une signature électronique la pensée chemine à travers les questions de la fiabilité du procédé de réalisation de la signature et celle des propriétés de son environnement virtuel.

[273] L'authenticité de la signature électronique est un objectif que le droit poursuit. Pour s'entourer de garanties d'authenticité de la signature électronique, le droit s'est tourné vers des interrogations sur la fiabilité du moyen de sa production.

[274] Ensuite, comme nous avons démontré dans ce chapitre, les assurances de la fiabilité du moyen de signature électronique résident dans l'ensemble des caractéristiques de l'architecture de l'environnement virtuel. Par conséquent, l'attention que le droit porte au standard de fiabilité des moyens virtuels d'authentification traduit l'intention de l'ensemble de la communauté d'associer des règles techniques aux signatures électroniques. La substance du standard juridique de fiabilité est fournie par les propriétés de la morphologie de l'architecture.

Section III – LES TENDANCES – LA POUSSÉE VERS UNE ARCHITECTURE UNIFORME CONTRÔLÉE

[275] Tout au long de ce chapitre nous avons démontré que les possibilités offertes par l'architecture du cyberespace déterminent l'attitude du droit vis-à-vis des moyens électroniques de signature. Il nous est donc difficile de ne pas prêter attention au

développement de la morphologie du cyberespace ainsi qu'aux tendances qui se sont démarquées.

[276] À l'origine du développement de l'architecture se place le *jeune* Internet, le royaume de l'anonymat. Internet que nous connaissons à l'heure actuelle autorise l'identification à un degré supérieur à travers de différentes infrastructures architecturales au sein du réseau. Parmi ces infrastructures d'identification, notons la présence des Infrastructures à clé publique, de courrier électronique sécurisé, ainsi que divers procédés d'apposition de signatures électroniques.

[277] Bien que prévoir le profil d'Internet de la prochaine génération soit un exercice difficile, la poussée vers une architecture de contrôle permettant un haut degré d'identification est de plus en plus apparente. À notre avis,, le passage de la structure d'Internet d'aujourd'hui, composée d'unités d'informations interconnectées mais demeurant toujours des « îles » autonomes, à une plate-forme globale distribuée conduira à l'uniformisation et à la globalisation des possibilités de contrôle de ladite architecture. Dans cette perspective nous sommes témoins des premiers pas vers une architecture robuste d'identification concrétisée par le lancement de certains produits et initiatives tant privées que publiques.

§1. Le contrôle à travers les services *Web* et l'architecture XML

a. Des îles d'information autonomes à une plate-forme commune

[278] L'Internet d'aujourd'hui reflète le caractère centralisé du monde.[247] Le modèle que nous utilisons actuellement est serveur-centrique, la relation entre le serveur et le navigateur est celle d'un terminal. La plus grande partie de l'information est concentrée dans des bases de données centralisées. Internet est composé d'unités interconnectées représentant des îles d'informations et de fonctionnalité autonomes.

[279] Selon Gates[248], le cyberespace de demain représentera un monde en ligne, faisant appel à une constellation de serveurs, de postes de travail, de dispositifs intelligents, de téléphones mobiles, de services Internet capables de collaborer en partageant leurs données, intégrant leurs processus et unifiant leurs efforts. Ce but est devenu accessible notamment grâce à *l'eXtensible Markup Language*[249]*(XML)* - un standard ouvert, administré par le W3C. Entre autres, XML est le moyen technologique rendant possible le fonctionnement des *services Web*. Il permet de décrire et, par-là, d'organiser, programmer, éditer et échanger les données qui circulent entre les postes de travail, les applications logicielles, les dispositifs intelligents, les sites Web. XML se trouve à la base des solutions d'une architecture globale du cyberespace, dite plate-forme intégrée ou distribuée. Jusqu'alors *Napster* et les messageries instantanées étaient des exemples de plate-formes distribuées selon lesquelles les postes de travail ou les autres unités collaboraient directement entre eux à travers le Web. Cependant, ces exemples ne représentent que des infrastructures isolées, non pas une architecture globale commune comme celle qui s'élabore présentement.

[280] Le fonctionnement des services Web repose sur 4 principes. Premièrement, les systèmes interagissent sur Internet et profitent de la disponibilité et de la connectivité du réseau. En deuxième lieu, il existe un mécanisme de repérage des services Web sur internet. Pour identifier les systèmes offrant des services Web sur Internet certaines grandes

---

[247] Bill GATES, « Why We're Building .NET Technology », *Microsoft, PressPass,* 18 juin 2001, source: http://www.microsoft.com/presspass/misc/06-18BillGNet.asp, visitée en mai 2002

[248] *Id.*

[249] Ci-après XML.

compagnies[250] ont développé *Universal Description, Discovery, and Integration*[251], un moyen de localiser et utiliser les services Web offerts par les autres compagnies. Le troisième principe est l'utilisation d'un format commun de données entre les différents langages de programmation, les différentes applications, systèmes d'exploitation qui est fourni par XML. Le quatrième dispositif de cette architecture est le protocole commun de base, SOAP[252], qui permet l'interaction des systèmes.

[281] Ainsi, l'intégration et la collaboration entre des systèmes, des applications et des processus est assurée. L'exemple le plus fréquemment utilisé pour illustrer l'effet des services Web est celui de l'intégration du système d'appel d'offres d'une entreprise avec celui de ses fournisseurs. Ces derniers seraient en mesure de concevoir, de planifier et de procéder aux fournitures sans qu'une commande soit expressément effectuée. Les services Web sont des technologies flexibles unifiant l'informatique personnelle (*personal computing*), l'informatique d'entreprise (*enterprise computing*) et le Web. Ce processus fait appel à une macro-fusion des ressources et des fonctionnalités des unités sur Internet. La logique sous-jacente de la technologie est d'assurer le passage de l'architecture composée de centres autonomes à une structure intégrée et distribuée, qui, il faut le dire aussi, représente une plate-forme homogène à l'échelle globale.

[282] L'application de ce modèle fait déjà l'objet d'efforts de certaines compagnies dont Microsoft qui a récemment lancé la plate-forme .NET - une plate-forme logicielle de services Web.[253] Le but de .NET est la création d'une infrastructure contrôlée d'activités commerciales sur Internet[254]. Quoique cette plate-forme représente un sous-environnement dans le réseau global, son déploiement est susceptible de mener à sa généralisation et de faire en sorte que .NET détermine l'architecture de l'Internet. Le produit de Microsoft a même été bâtisé Supranet.[255] À ce propos Lessig affirme qu'Internet de demain sera déterminé du point de vue architectural par deux importantes compagnies américaines, la corporation Microsoft et AOL Time Warner :

---

[250] Microsoft, Ariba, COMPAQ, Dell, HP, IBM, SAP
[251] Ci-après UDDI. Des informations sont disponibles sur www.uddi.org, visitée en mai 2002.
[252] Abréviation pour *Simple Object Access Protocol.*
[253] Des informations sur .NET sont disponibles sur http://www.microsoft.com/net/, visitée en mai 2002.
[254] Voir l'image No. 2 à la page suivante
[255] The Economist , « Mach 1 at Microsoft », *The Economist Technology Quarterly*, 33 – 34, 16 Mars 2002

« These two companies – AOL Time Warner and Microsoft – will define the next five years of the Internet's life »[256]

[283] .NET a été conçu au sein des Microsoft Research Laboratories (MSR)[257] et représente une initiative ambitieuse visant à offrir des services sur le Web, services inconcevables jusqu'alors et pour lesquels l'authentification occupe une place importante.

[284] Le produit comprend en premier lieu des instruments pour les développeurs *(developer tools)* parmi lesquels *Microsoft Visual Studio®* - le langage de programmation permettant la conception de services Web dans le cadre de .NET. La compagnie a aussi lancé des serveurs véhiculant les services, tels Windows 2000, Microsoft SQL Server 2000, Microsoft Exchange 2000, Microsoft BizTalk Server. Le troisième élément structurant de .NET est le logiciel pour les unités participantes dans le modèle distribué, les machines de jeux, les postes de travail, les téléphones cellulaires, les assistants numériques personnels *(Personal digital assistant ou PDA)*. .NET inclut aussi des services aux utilisateurs, MSN pour les consommateurs, bCentral pour les petites entreprises. Le *Passport* de Microsoft est aussi partie de ce projet technologique et il méritera une attention spéciale dans notre développement concernant la globalisation des architectures de sécurité et celles de l'authentification.

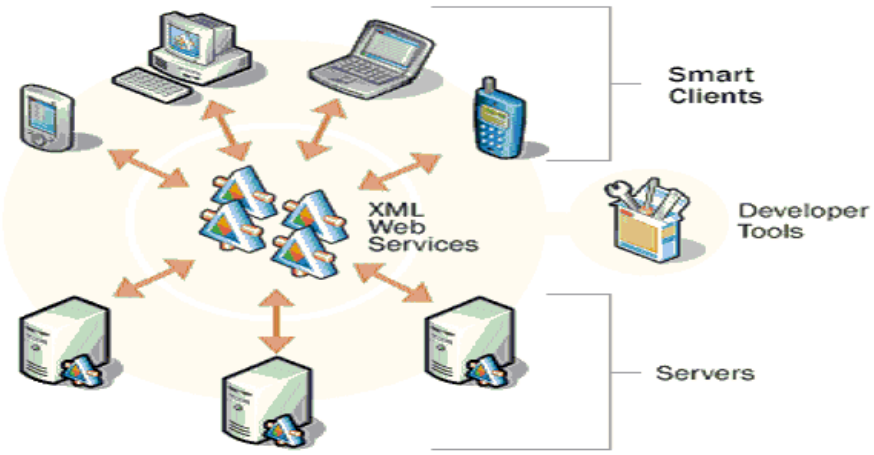


Image 5. *Les éléments de base du cadre .NET. L'image est disponible sur* http://www.microsoft.com/net/defined/whatis.asp

[256] L. LESSIG, *op. cit.*, note 7, p. 267
[257] The Economist, *loc. cit.,* note 255

b. Des modèles de sécurité autonomes à un modèle sécuritaire commun

[285] Tout comme les unités autonomes formant le cyberespace d'aujourd'hui, les présentes solutions sécuritaires mises en place font appel à des modèles indépendants, accompagnant les îles fonctionnelles et informationnelles qui forment Internet. Ainsi, le cyberespace actuel est sécurisé par des implémentations partielles, telles les infrastructures à clés publiques, le courrier électronique sécurisé, des applications cryptographiques diverses.

[286] Dans un environnement de services Web, la plate-forme distribuée homogène implique un cadre sécuritaire intégré et commun. À notre avis, ceci uniformise les moyens de se prémunir contre les dangers du cyberespace. Par ailleurs, l'uniformité de la solution sécuritaire renforce les possibilités de contrôle. En ce qui concerne le modèle commun, les corporations Microsoft et IBM ont publié la première version de leur proposition d'architecture de sécurité commune pour enrober et sécuriser l'environnement des services Web.[258] (Web Services Security)

[287] La sécurité WS proposée (*Web Services Security*) repose sur la mise en fonction de technologies de sécurité jusqu'alors incompatibles entre elles, comme celles des infrastructures à clés publiques et de *kerberos*[259]. Elle ambitionne d'unifier les concepts anciennement incompatibles et de créer une coordination à grande échelle. Le but du modèle est la création d'un cadre uniforme enveloppant des systèmes hétérogènes.

[288] Le modèle *WS Security* utilise des jetons sécuritaires *(security token)* - des porteurs d'informations relatives à la sécurité, tels des certificats X.509, des sceaux et des identifiants *kerbero*, ou des modules d'identification de l'abonné (MIA ou SIM) pour les dispositifs mobiles. Les jetons sécuritaires signées *(signed security token)* sont ceux qui contiennent des assertions *(claims)* endossées avec des moyens cryptographiques par le titulaire. Les assertions concernent l'identité, la fonction ou l'autorité du titulaire. Le cadre sécuritaire commun utilise aussi la preuve de possession *(proof of possession)* en faisant appel à une information qui associe une personne avec un dispositif de sécurité ou un

---

[258] Microsoft Corp., IBM Corp., «Security in a Web Services World: A Proposed Architecture and Roadmap», *Joint White Paper,* le 7 avril 2002, Version 1, source: http://msdn.microsoft.com/library/?url=/library/en-us/dnwssecur/html/securitywhitepaper.asp?frame=true, visitée en mai 2002

[259] Protocole d'authentification qui permet à un correspondant de s'assurer de l'identité de son interlocuteur à l'aide d'un serveur d'authentification externe.

ensemble d'assertions. Les auteurs de la spécification développent plusieurs scénarios d'application du modèle qui se divise en des sous-spécifications - *WS-Security, WS-Policy, WS-Trust, WS-Privacy, WS-SecureConversation, WS-Federation, WS-Authorization.*

[289] Elles ne sont pas cependant l'objet de notre étude. Notre but est de démontrer la tendance à une globalisation d'une solution technologique sécuritaire, capable d'envelopper le cyberespace. La sécurité WS se veut un contexte uniforme pour l'ensemble d'appareils mobiles, de passerelles *(gateway)*, de serveurs mandataires *(proxy),* d'équilibreurs de charge, de zones démilitarisées, de données provenant de l'extérieur, de systèmes globalement distribués et configurés de manière dynamique. Il en ressort que la sécurité se dirige des applications isolées et autonomes d'hier vers un cadre global commun. (voir l'image 6)

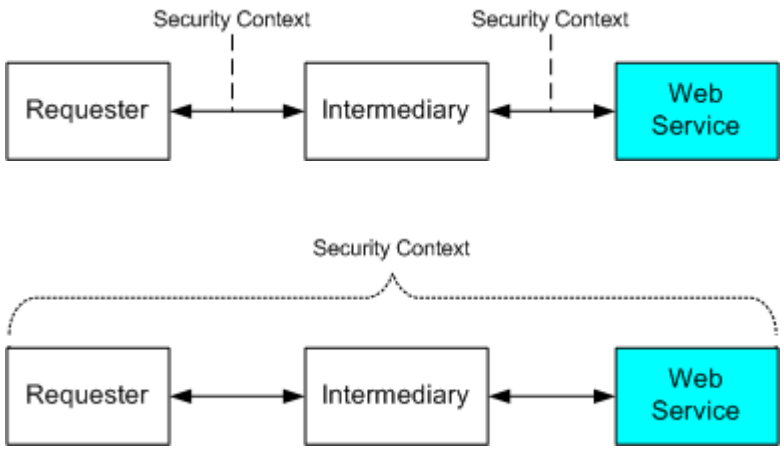


Image 6. *Le passage des solutions sécuritaires partielles à un cadre global. L'image est disponible sur http://msdn.microsoft.com/library/?url=/library/en-us/dnwssecur/html/securitywhitepaper.asp?frame=true*

[290] La globalisation et la distribution des choix technologiques des services Web est en mesure de déterminer l'architecture du cyberespace. Si les modèles de services Web distribués et les solutions sécuritaires qui les accompagnent atteignent le développement désiré par les concepteurs et recouvrent l'essentiel de l'espace virtuel (la téléphonie mobile, les réseaux d'achat, les systèmes informatiques, les systèmes bancaires, Internet etc.), ces technologies définiront à la suite l'architecture du cyberespace dans sa totalité.

[291] Notons que la plate-forme .NET de Microsoft est déjà une réalité. Elle s'inscrit dans l'application de la politique *Trustworthy Computing* de la compagnie qui représente un virage important dans les priorités de Microsoft. Prônée par Bill Gates[260], cette philosophie concernant le design, le développement et l'implémentation, inverse les priorités de la compagnie en préférant la sécurité à la fonctionnalité. À ce propos, Bruce Schneier, un des sceptiques au sujet de Microsoft, déclare :

> *« I congratulate Bill Gates on his willingness to move the company in this manner. To have Microsoft as a company focusing on security will make the Internet a safer place. »*[261]

[292] Cette affirmation souligne encore une fois la globalisation des constructions architecturales des services Web ainsi que des solutions sécuritaires qui les accompagnent au point de créer une identité entre ces nouvelles structures et l'architecture du cyberespace en général.

c. Une conséquence de la globalisation de l'architecture – un modèle global d'identification, le *Passport* de Microsoft

[293] Le cadre global des services Web nécessite aussi un cadre global de confiance. Selon Craig Mundie, vice-président senior et directeur technologique en chef de Microsoft, le but da la plate-forme de services Web est de devenir aussi sécuritaire que la téléphonie et l'électricité.[262] Selon Mundie, la confiance repose sur la gestion de l'identité. L'idée d'un cadre global de confiance reposant sur une gestion globale uniforme de l'identité trouve un nombre considérable de supporteurs.[263] Elle assurerait une authentification interdomaine

---

[260] Dennis FISHER, « Gates : Security over Features », *eWeek*, *News and Analysis*, 21 Janvier 2002, source : http://www.eweek.com/article/0,3658,s=701&a=21528,00.asp, visitée en mai 2002

[261] *Id*.

[262] Craig MUNDIE, « Keynote Address », *Conférence « Managing Identity and Authentication on the Internet »*, le 11 mars 2002, source: http://www.csis.org/tech/events/020311event/Mundie/index.htm, visitée en avril 2002

[263] Gordon EUBANKS, « Identity Management: A Key Element of Critical Infrastructure Assurance », *Conférence « Managing Identity and Authentication on the Internet »,* le 11 mars 2002, source: http://www.csis.org/tech/events/020311event/eubanks/index.htm, visitée en mai 2002, Arthur COVIELLO,

des machines, des personnes et des entreprises. À ces fins, l'auteur met en relief le *Passport* de Microsoft, un produit se voulant capable de fournir une architecture commune et robuste de l'identité sur Internet.

[294] Le « *Passport* .NET » est intimement lié à la plate-forme .NET de Microsoft. La compagnie met en valeur la rapidité et la facilité des achats sur Internet qu'il apporte.[264] Le fonctionnement du *Passport* suppose l'existence d'une communauté de sites participants ou sites-membres, qui forme un sous-environnement dans le cyberespace, obéissant à des règles d'authentification communes uniformes. Basé sur la technique du *Single Sign-in* (SSI), le passeport offre la possibilité de faire des achats rapidement et efficacement à travers les sites-membres. Ainsi les détenteurs d'un *Passport* sont capables de magasiner, chercher des loisirs en ligne, faire affaires avec des cyberbanques, utiliser des services basés sur la téléphonie mobile dans un environnement bâti par des sites participants et pour lequel un seul système de gestion de l'identité est valide. Le produit utilise Secure Socket Layer (SSL) et triple DES comme algorithme de chiffrage. Le *Passport* assure un identifiant unique (PUID) à chaque utilisateur, celui-ci peut être utilisé par les compagnies comme une clé primaire de leurs bases de données. Le PUID est associé à l'utilisateur et non-pas à un système ou un poste de travail. Microsoft souligne que le *Passport* est quasiment anonyme, son obtention n'exigeant qu'un compte de courrier électronique et un mot de passe. Les concepteurs énoncent que les données stockées dans le profil personnalisé du passeport sont organisées dans 14 champs, la plupart n'étant pas en mesure d'identifier la personne ou d'en révéler des informations sensibles. Une image toute différente est cependant révélée par l'énumération des champs de données. Ils regroupent le mot de passe, le prénom, le nom, le compte de courrier électronique, le pays et la région, l'État, le code postal, le fuseau horaire, le sexe, la date de naissance, l'occupation et l'accessibilité. Dans certains cas, le numéro de téléphone et un NIP personnel peuvent être exigés par des sites appliquant une politique de *Strong Credential Features*. Comme l'énonce Kennedy[265] l'initiative .NET et le *Passport* possèdent le potentiel de rendre

---

« Identity Management: An Important Enabler of E-Government », *Conférence « Managing Identity and Authentication on the Internet »,* le 11 mars 2002,
source: http://www.csis.org/tech/events/020311event/coviello/index.htm, visitée en mai 2002,

[264] Des informations sur le passeport .NET de Microsoft sont disponibles sur http://passport.com/Consumer/default.asp?lc=3084, visitée en mai 2002.

[265] John B. KENNEDY, Mary WONG, «Recent Developments in U.S. Privacy Law», *Practising Law Institute, Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series*, novembre 2001

l'anonymat sur Internet impossible. En Europe l'attitude envers le mécanisme d'authentification qu'est le *Passport* est empreinte d'inquiétude. Comme l'énonce Wéry, Microsoft n'a pas convaincu les autorités européennes de l'innocuité de Passport, son nouveau système de collecte, d'enregistrement et de partage des informations fournies par les utilisateurs de XP et de .NET.[266]

[295] Pour l'instant le SSI du *Passport* fournit un mécanisme d'authentification commun sur Internet dans la communauté des participants au programme. Cependant, l'aspiration vers une universalisation de ce modèle d'identification est apparente. L'accès à certains services de Microsoft exige la possession d'un *Passport*. Il suffit ici de mentionner que l'accès à des portions du support en-ligne du système d'exploitation Windows XP exige un *Passeport*.[267] Il devient clair que le produit est orienté vers une acceptation globale et vise à devenir une plate-forme commune d'authentification sur Internet.

[296] La perspective d'un mécanisme global et uniforme de gestion de l'identité dans le cyberespace est une nouveauté. Elle n'est pas cependant une initiative isolée, mais s'inscrit dans la logique de la globalisation du modèle sécuritaire, qui pour sa part, suit le déploiement des services Web. Pour l'instant les modèles cités ne représentent qu'une structure architecturale au sein du cyberespace, mais ils ont l'ambition de devenir un macro-cadre qui, selon nous, changera fondamentalement l'architecture du monde virtuel pris dans sa totalité au point que la morphologie de base du cyberespace sera déterminé par ce cadre.

§2. Autres initiatives vers une architecture uniforme de contrôle

[297] Le passeport de Microsoft n'est pas le seul produit ayant pour but de bâtir une architecture robuste d'identification. D'autres initiatives peuvent être mentionnées.

---

[266] Étienne WÉRY, « Microsoft « Passport » et « .net », la FTC transige, mais l'Europe poursuit l'enquête», *Droit des nouvelles technologies*, *Actualités,* le 3 septembre 2002, source : http://www.droit-technologie.org/1_2.asp?actu_id=627, visitée en mai 2002

[267] Microsoft, « .NET Passport Overview », *.NET, My Services*,
source : http://www.microsoft.com/MYservices/passport/overview.asp, visitée en mai 2002

[298] Il s'agit en premier lieu d'initiatives technologiques comme le protocole IPv6 de l'IETF désigné sous le slogan « The Next Generation Internet! ».[268] Le lancement de IPv6 a été dicté par les limites de IPv4 dont les adresses IP se composaient de 4 octets et qui risque d'être saturé bientôt à cause de la croissance du nombre de machines connectées sur le réseau. En consacrant 16 octets au lieu de 4 à l'adresse IP, le nouveau protocole prévoyait à l'origine de réserver 6 octets au numéro de série de la carte réseau qui est unique. Ainsi, chaque internaute aurait transmis ce numéro, unique au monde et stable dans le temps dans toutes ses utilisations d'Internet. Cette technique est, à notre avis, une autre tentative de construction d'une architecture globale d'identification, même si ce n'est qu'un but marginal de l'adoption du protocole. Par ailleurs l'implémentation du protocole a été encouragée par une communication de la Commission européenne adoptée le 21 février 2002.[269]

[299] Il s'agit en second lieu d'initiatives de nature privée de vaste envergure dont les chances de succès sont majeures. Au sein du CSIS[270], un groupe de travail en matière d'authentification et d'identité, co-présidé par Craig Mundie et Laurence Lessig, est chargé d'une étude du développement d'identités numériques. Les travaux du groupe sont censés résulter en une proposition d'une plate-forme commune de gestion des identités numériques à travers les entreprises et les frontières.[271] Le groupe de travail examine aussi le rôle des gouvernements et de l'industrie dans la construction de cette plate-forme. L'étude s'est aussi penchée sur l'idée d'établir un schéma de gestion des identités cybernétiques semblable à celui instauré pour administrer les adresses Internet par la *Internet Corporation for Assigned Names and Numbers*.[272] L'initiative dévoile sans conteste un mouvement résolu vers la généralisation des architectures d'identification et la construction d'un cadre commun d'authentification.

---

[268] Abréviation pour *Internet Protocol Version 6*. Des informations sur IPv6 sont disponibles sur http://www.ipv6.org/, visitée en mai 2002.
[269] Communication du 21 Février 2002
[270] Center for Strategic and International Studies, « Trust and Security in Cyberspace », le 6 Mars 2002, source : http://www.csis.org/press/ma_2002_0311.htm, visitée en mai 2002
[271] *Id.*
[272] Gara GARRETSON, « Industry examines government role in digital Ids », *InfoWorld*, le 11 Mars 2002, source :http://ww1.infoworld.com/cgi-bin/fixup.pl?story=http://www.infoworld.com/articles/hn/xml/02/03/11/020311hndigitalid.xml&dctag=online communities, visitée en mai 2002

[300] Il s'agit en troisième lieu d'initiatives publiques de création d'une architecture d'authentification, en particulier d'efforts législatifs récents. Le législateur belge a adopté une loi du 31 Décembre 2002[273] modifiant La Loi fixant le cadre juridique des opérateurs et prestataires de services de télécommunications en Belgique. La loi confère, par un nouveau paragraphe 6 de l'article 109 E, le pouvoir au gouvernement d'imposer le respect de mesures techniques et administratives aux abonnées et aux utilisateurs finaux pour en permettre l'identification dans des hypothèses prévues. Bien que les mesures ne servent que les fins de l'instruction criminelle, l'adoption d'une telle politique doit être considérée que comme étant un indice révélateur de l'attitude du législateur envers le cyberespace de demain. L'aspiration à la création d'une architecture de contrôle est apparente et s'inscrit dans les tendances vers une morphologie générale du cyberespace autorisant un plus haut degré de sécurité et d'identification.

[301] Il est difficile de dire si bientôt des possibilités d'identification égales ou supérieures à celles du monde matériel nous seront offertes par la nature-même de l'architecture du cyberespace. L'aspiration vers une telle architecture est cependant un fait. Dans ce contexte, l'image actuelle de la sécurité des communications en ligne et de l'identification des acteurs, apparaît comme une solution conjoncturelle, témoignant de l'état de l'art dans l'attente de la prochaine modification du cyberespace.

[273] Étienne WÉRY, « Surfer anonymement devient illégal en Belgique », *Droit des nouvelles technologies*, *Actualités,* le 18 Mars 2002, source : http://www.droit-technologie.org/1_2.asp?actu_id=553, visitée en mai 2002

CHAPITRE IV - L'ÉVALUATION DES CAPACITÉS DE L'ARCHITECTURE

[302] La fiabilité de l'environnement technologique est la notion au centre des interrogations du droit de la preuve confronté au numérique. Nous avons démontré sa relation étroite entre la fiabilité du moyen de signature électronique et les caractéristiques de l'environnement qui l'héberge. À ce stade de notre étude, il convient de s'intéresser aux réponses fournies concernant la fiabilité des procédés de signature.

[303] La technique de signature est une fonctionnalité du système d'information. L'appréciation des qualités de cette technique pourrait être légitimement assimilée à l'évaluation des capacités du système à assurer cette fonctionnalité. Dans ce contexte, il nous est difficile de faire abstraction de deux caractéristiques essentielles du standard de fiabilité du moyen de signature électronique, à savoir son caractère polymorphe et sa relativité.

[304] Pour ce qui est des aspects multiples du standard, il a été considéré en détails dans le chapitre qui précède. Il suffirait de rappeler que la complexité des systèmes d'information, rajoutée à celle des technologies cybernétiques, divise le standard en plusieurs éléments, correspondant aux unités structurantes des SI et à celle des éléments constitutifs des technologies mises en place. Les vulnérabilités et les risques, quant à eux, rendent le paysage fort complexe.

[305] Le standard de fiabilité est aussi empreint de relativité. Il est proportionné à la nature et aux spécificités des circonstances qui l'entourent. Comme l'exprime Bernard Brun[274], la sécurité que doit revêtir le site d'une compagnie oeuvrant dans le milieu financier doit être plus élevée que celle prévue pour des transactions de moindre valeur. La relativité de la fiabilité est mise en avant par la Loi Type de la CNUDCI sur les signatures électroniques[275] qui, dans son article 6, dispose :

> *« Lorsque la loi exige la signature d'une certaine personne, cette*

---

[274] Bernard BRUN, « Nature et impact juridique de la certification dans le commerce électronique sur Internet », *Lex Electronica*, 2000, source : http://www.lex-electronica.org/articles/v7-1/Brun.pdf, visitée en mai 2002

[275] La Loi-type sur les signatures électroniques, précitée, note 90

exigence est satisfaite dans le cas d'un message de données s'il est fait usage d'une signature électronique dont la fiabilité est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris toute convention en la matière. »

[306] Ceci dit, l'évaluation de la fiabilité du moyen de signature à la lumière des capacités de l'architecture doit répondre de manière adéquate à la complexité de l'objet d'évaluation et à la relativité de ses caractéristiques, liée à l'existence de risques.

[307] Pour arriver à une conclusion sur la fiabilité de la technologie de signature, un processus se décomposant en plusieurs étapes doit être envisagée. L'enchaînement comprend l'établissement de standards (la base normative du jugement), le processus même d'évaluation (l'examen d'un objet concret) dans le but d'aboutir à une conclusion sur la fiabilité (le résultat de cet examen).

Section 1 – L'ENCADREMENT NORMATIF DE L'ÉVALUATION

[308] Notre étude sur les normes qui entourent l'évaluation de la fiabilité à travers les caractéristiques de l'environnement se penchera dans un premier temps sur le concept de standards (les paramètres qui fournissent la base substantielle de l'évaluation). Nous envisagerons ensuite les règles organisationnelles et procédurales qui gouvernent la procédure d'évaluation.

§ 1. Les standards – le point de départ de l'évaluation

a. Le processus de standardisation

[309] C'est la conformité à des critères déterminés que sont les standards qui conditionne les résultats de l'évaluation. Leur apparition est engendrée par la nécessité de régir, soit officiellement soit officieusement un secteur d'activité.[276]

[310] Une distinction existe entre deux différents types de standards, les standards *de facto* et les standards officiels. Certaines industries développent leurs propres standards. On peut

[276] B. BRUN, *loc. cit.*, note 274

assister à l'élaboration de standards internes dans les grandes entreprises. Ces standards *de facto* pourront bénéficier de la protection accordée par le droit d'auteur. Selon Brun[277], les standards *de facto* sont d'application limitée et sont donc susceptibles de provoquer des désavantages pour ceux qui en sont privés et aboutir à une fermeture des marchés. Cependant ces normes existent dans la communauté technologique et peuvent servir de base d'évaluation compte tenu de leur crédibilité.

[311] Les standards officiels, quant à eux, sont accessibles à tous et poursuivent avec succès le but d'ouverture des marchés.[278] Ils impliquent une dimension étatique et apportent un caractère public aux standards. La préférence à attribuer aux uns et aux autres est une question délicate qui nécessite une analyse des avantages et des inconvénients.

[312] Cette distinction apparaît pleinement en matière de signature électronique. Aux termes de la Directive européenne, le droit est délégué à la Commission d'attribuer d'officialiser les standards *de facto* par l'attribution de numéros de référence à des normes généralement admises et leur publication dans le Journal Officiel des Communautés européennes[279]. De cette manière, des standards *de facto* voient leur autorité sanctionnée par le pouvoir des institutions communautaires et obtiennent par la suite un caractère officiel. Il en est de même avec la loi québécoise, article 67, aux termes duquel le Gouvernement peut attribuer un caractère obligatoire à des normes qui sont, en l'absence d'intervention réglementaire, d'application volontaire. Il s'agit concrètement des normes récapitulées par le Comité pour l'harmonisation des systèmes et des normes[280], contenues dans les guides et ayant pour objet les « …*formats et des langages de balisage de données, des codes de représentation de caractères, des algorithmes de signature, de chiffrement, de compression de données ou d'amélioration de l'image ou du son, des longueurs de clés, des protocoles ou des liens de communication*. »[281]

---

[277] *Id.*
[278] *Id.*
[279] Directive européenne, article 3 (5), précitée, note 9
[280] L.C.C.J.T.I ., article 63, précitée, note 10
[281] *Id*., article 65

i. Les facteurs moteurs de la standardisation

[313] La première catégorie de facteurs favorisant la standardisation dépend des habitudes du marché. Parmi eux, il faut citer les externalités du réseau qui base et la valeur d'un produit sur son acceptation par les autres usagers du réseau.[282] Le deuxième facteur relevant de cette catégorie est la transformation en standards de solutions préexistantes pour des raisons d'habitude et de commodité[283]. Le troisième facteur est celui de la compatibilité. Il peut se manifester selon deux scénarios différents[284]. Premièrement, les attentes du marché en faveur d'un standard dominant, forcent les concepteurs à développer des standards gravitant autour de la norme dominante. Deuxièmement, des standards préexistants pour une technologie de base peuvent mener à la création de standards similaires pour les technologies dépendantes de la technologie de base. Le quatrième facteur est le besoin de différentiation des produits, un impératif capital du marché, pour qui la possibilité de classifier les produits étant d'un intérêt majeur[285].

[314] Les initiatives de standardisation du gouvernement, comme contre-point de la normalisation du marché, varient selon les politiques concrètes des juridictions. Par exemple, le gouvernement américain a toujours privilégié une faible intervention dans le processus de standardisation, malgré des sursauts après la Première Guerre Mondiale et encore plus durant la Guerre Froide.

[315] Des standards peuvent être développés par la communauté académique et, le cas échéant, ils ne découlent ni des besoins du marché, ni d'une intervention gouvernementale. Le besoin ressenti d'un standard est une initiative suffisante pour le lancement du processus de sa création. La création du système de nom de domaines Internet au sein de *l'University of Southern California* a ainsi été initiée par la difficulté de retenir des adresses numériques.[286]

---

[282] Marcus MAHER, « An Analysis of Internet Standardization », 3 *Va. J.L. & Tech*. 5, Spring 1998, source : http://scs.student.virginia.edu/~vjolt/graphics/vol3/home_art5.html, visitée en mai 2002
[283] *Id.*
[284] *Id.*
[285] *Id.*
[286] *Id.*

ii. Les organismes de standardisation

[316] L'existence d'organismes normalisateurs dans le processus de standardisation peut receler un nombre important d'avantages mais elle présente aussi des risques.[287] Les avantages consistent, d'une part, en l'établissement d'un meilleur processus de développement des standards. La qualité supérieure du processus s'exprime par sa flexibilité, sa vélocité et la combinaison d'expérience de professionnels différents, afin de surmonter le problème d'information. Ils résident aussi en leur aptitude à mieux percevoir les effets de réseaux, soit l'acceptation du standard par les utilisateurs interconnectés[288]. Enfin, les organismes peuvent assister le marché pour motiver les acteurs à faire des choix adéquats et appropriés. Ils facilitent l'échange d'information et rassurent les concepteurs quant à la crédibilité de la technologie en développement.

[317] Les risques inhérents à la participation des organismes normalisateurs méritent l'attention. Il s'agit notamment de la représentation inéquitable des intérêts au sein d'une organisation de standardisation, du manque de *leadership* dans la communauté des organismes normalisateurs et de la présence d'intérêts antagoniques.

[318] Maher développe les éléments nécessaires à l'efficacité et à la crédibilité d'un organisme normalisateur[289]. L'auteur cite en premier lieu le besoin d'une structure efficace dotée d'un impact profond sur la fiabilité des procédures. Le deuxième élément réfère à la participation effective des parties intéressées dans le processus de développement d'un standard afin d'aider à la cueillette de toutes les informations indispensables et renforcer la légitimité des décisions. Les acteurs doivent se voir ouvrir une possibilité de participation tant dans la procédure de développement des standards, qu'à l'étape de leur contestation. L'auteur mentionne aussi la comptabilité organisationnelle comme autre aspect de la fiabilité de l'organisme normalisateur. Les liens entre l'organisation et son administration doivent permettre une transparence et une accessibilité de l'information, ainsi que des moyens de contrôle et d'appel disponibles. Finalement, le dernier élément fait appel à l'existence de moyens d'exécution des décisions de l'organisation.

---

[287] *Id.*
[288] *Id.*
[289] *Id.*

iii. Le rôle du gouvernement

[319] L'image de la standardisation ne serait pas complète sans y situer le rôle du gouvernement. Le gouvernement est fréquemment une partie intéressée par le processus de standardisation[290]. Dans d'autres circonstances il intervient en imposant diverses formalités afin de pallier les défaillances des méthodes de création de standards. Le gouvernement peut également financer un organisme normalisateur. Il peut encore participer au processus de standardisation, coordonner les efforts entre des organismes existants ou simplement créer et adopter ses propres standards. Le gouvernement s'est déjà, à plusieurs reprises, engagé dans le règlement de la représentation inéquitable des intérêts dans les organismes normalisateurs comme aux États-Unis, en vertue de la législation antitrust. À l'inverse, l'intervention gouvernementale peut avoir pour objet de mettre une activité de normalisation à l'abri de la législation antitrust. L'implication des autorités étatiques peut aussi être motivée par l'objectif de remédier au manque de *leadership* au sein de la communauté ou pour concilier des intérêts extrêmement divers. En fin de compte, le gouvernement peut être impliqué dans la mise en œuvre des décisions adoptées.

[320] Comme nous l'avons déjà mentionné[291], la loi concernant le cadre juridique des technologies de l'information confère au Gouvernement dans son article 67 la capacité d'attribuer une autorité aux guides reflétant les résultats de standardisation. Même si, en l'espèce, l'État n'intervient que subsidiairement et seulement s'il est constaté que les guides ne sont pas appliqués volontairement et après consultation du comité, cette participation du Gouvernement dans le processus de normalisation est significative. Elle représente un exemple de la présence active du gouvernement dans la régulation technologique du cyberespace. Il en va de même des hypothèses d'intervention réglementaire de la Commission européenne. Enfin, même aux Etats-Unis, L'UETA réserve une possibilité d'intervention au gouvernement. La loi stipule dans son artcile 19[292] :

> *« The [governmental agency] [designated officer] of this State which adopts standards pursuant to Section 18 may encourage and promote*

[290] *Id.*
[291] *supra*, par. 126
[292] UETA, article 19, précitée, note 66

consistency and interoperability with similar requirements adopted by other governmental agencies of this and other States and the federal government and nongovernmental persons interacting with governmental agencies of this State. If appropriate, those standards may specify differing levels of standards from which governmental agencies of this State may choose in implementing the most appropriate standard for a particular application. »

[321] Il est vrai que la disposition est très prudente et n'autorise qu'un champ restreint de promulgation de standards ne portant que sur les relations impliquant des agences gouvernementales. Cependant, pour nos fins, la disposition représente la base d'une normalisation réglementaire émanant du gouvernement.

[322] Ce survol des principes et de la logique de la standardisation étant fait, nous nous pencherons sur les organismes qui oeuvrent dans le domaine de la standardisation des systèmes d'information basés sur les technologies de l'information et leur fonctionnement sur les réseaux de communication. Les travaux de ces organismes nous fourniront la grille d'évaluation de la fiabilité des SI servant à la réalisation de signatures électroniques. Les standards représentent fréquemment la base d'évaluation des qualités d'un objet. Cependant, ils ne sont pas l'unique source en la matière et la non-conformité à un standard précis ne signifie pas automatiquement et incontestablement que l'objet évalué n'est pas fiable.

b. L'appréciation des caractéristiques du monde virtuel – les standards concrets en la matière

[323] Le premier exemple de standardisation des communications via Internet remonte aux temps de la naissance du réseau avec l'adoption du protocole TCP/IP par le gouvernement américain. L'introduction de ce protocole a mené à l'expansion du réseau par le biais du renforcement de l'interopérabilité et la compatibilité des solutions technologiques des postes interconnectés.

i. Les organismes oeuvrant en la matière

[324] Nous pouvons définir deux groupes d'organismes normalisateurs dans le domaine des communications via Internet, le groupe *universel* et le groupe *orienté Internet*. Cette classification peut être tracée à la base des activités des organismes normalisateurs. Le groupe universel comprend des organisations oeuvrant dans plusieurs domaines sujets à la normalisation, y compris la sphère du cyberespace. Le groupe orienté Internet inclut des organismes spécialisés dans le champ des activités reliées au cyberespace. Une autre classification peut aussi être faite selon le caractère international ou national des organisations. Dans le groupe universel au niveau international rentrent des organismes qui étaient impliqués depuis longtemps dans le processus de standardisation, tels l'Organisation Mondiale de normalisation (ISO), l'Union Internationale des télécommunications (UIT) qui sont à l'heure actuelle impliqués dans le processus d'élaboration de standards destinés au cyberespace. Ainsi, l'ISO définit l'architecture d'interconnexion des systèmes ouverts dont la partie *« cadre de sécurité »* couvre largement la signature électronique. L'organisation travaille actuellement sur la standardisation de l'organisation des architectures à clé publique. De nombreuses normes adoptées par cet organisme peuvent trouver une application dans le domaine de la fiabilité des SI. L'UIT, pour sa part, a édité la norme X.509[293]. Elle fait partie de la liste des normes X.500 définissant le fonctionnement des annuaires et joue un rôle important pour les systèmes basés sur le schéma des infrastructures à clé publique. Le groupe orienté Internet au niveau supranational comprend des organismes comme l'IETF[294], le W3C[295], l'ISOC[296], l'IESG[297], IAB[298], IRTF[299] tous oeuvrant directement ou indirectement dans le domaine de la signature électronique.

---

[293] The International Telecommunication Union, « New Edition of X.509 ITU standard to Accelerate Global E-commerce Through Enhancements to Authentication and Authorization Specifications », *Communiqué de presse,* 2000, source: http://www.itu.int/newsarchive/press/releases/2000/05.html, visitée en mai 2002

[294] The Internet Engineering Task Force. Des informations sont disponibles sur http://ietf.org/, visitée en mai 2002.

[295] The World Wide Web Consortium. Des informations sont disponibles sur http://www.w3.org/, visitée en mai 2002.

[296] The Internet Society. Des informations sont disponibles sur http://www.isoc.org/, visitée en mai 2002.

[297] The Internet Engineering Steering Group. Des informations sont disponibles sur http://iesg.org/, visitée en mai 2002.

[298] The Internet Architecture Board. Des informations sont disponibles sur http://www.iab.org/, visitée en mai 2002.

[299] The Internet Research Task Force. Des informations sont disponibles sur http://irtf.org/, visitée en mai 2002.

L'ISOC par exemple développe un projet ayant pour but l'établissement d'une infrastructure de signature numérique, basée sur une carte à puce intelligente dans les opérations bancaires.[300] L'IETF est un groupe de travail coopératif de la communauté des utilisateurs et des développeurs d'Internet divisé en groupes de travail, organisés autour des thèmes techniques, parmi lesquelles se place le groupe de travail oeuvrant dans le domaine de la sécurité[301] qui développe entre autres, et en collaboration avec le W3C[302] ,un schéma de signatures électroniques XML.[303] Le projet de recherche de IRTF, *Authorisation Authentication Accounting Architecture*[304], est un exemple d'efforts de développement d'une architecture d'authentification dans le cyberespace.

[325] Comme au niveau international, il existe au niveau national des organismes normalisateurs universels et d'autres orientés Internet. Il serait impossible d'en citer tous les représentants, mais il convient de souligner que leurs travaux portent soit directement, soit de manière dérivée, sur les questions d'architectures de signatures électroniques. Aux Etats-Unis, l'ANSI[305] qui fait partie du groupe universel porte son attention sur les applications de schéma de signature numérique dans le domaine de la santé.[306] Le NIST[307], parmi le groupe orienté Internet a notamment adopté la norme ANSI X9.62-1998 codifiant un schéma d'infrastructure à clé publique reposant sur l'algorithme des courbes elliptiques pour l'industrie financière.[308] En Europe, le CEN (Comité européen de normalisation) travaille essentiellement dans le domaine des périphériques – cartes à puces, postes de

---

[300] ISOC, «LDAPv3 Versus X.511 DAP Security: A Comparison and How to Sign LDAPv3 Operations », *Digital Signature Project*,
source http://www.isoc.org/isoc/conferences/inet/98/proceedings/1a/1a_1.htm#Project, visitée en mai 2002

[301] IETF, « Active IETF Working Groups » *Security Area*, source http://www.ietf.org/html.charters/wg-dir.html#Security_Area, visitée en mai 2002

[302] IETF, W3C, «XML Signature WG», source : http://www.w3.org/Signature/ , visitée en mai 2002

[303] IETF, «XML Digital Signatures (xmldsig)»,
source http://www.ietf.org/html.charters/xmldsig-charter.html, visitée en mai 2002

[304] IRTF, IRTF Research Groups, « Authentication Authorisation Accounting Architecture Research Group (AAAA) », source: http://www.irtf.org/charters/aaaarch.html, visitée en mai 2002

[305] The American National Standards Institute. Des informations sont disponibles sur http://www.ansi.org/, visitée en mai 2002.

[306] Ann GEYER, « MEDePASS Healthcare Checklist », *ANSI*,
source: http://www.ansi.org/rooms/room_41/public/ppt/hisb184.ppt , visitée en mai 2002

[307] The National Institute of Standards and Technology. Des informations sont disponibles sur http://www.nist.gov/, visitée en mai 2002

[308] ANSI, « Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature algorithm (ECDSA) », *ANSI X9.62*, source: http://csrc.nist.gov/encryption/tkdigsigs.html, visitée en mai 2002

calcul de signatures, etc[309]. L'ETSI (European Telecommunication Standardization Institute) réalise des travaux de normalisation sur la signature[310]. Au Québec, la *Loi concernant le cadre juridique des technologies de l'information* prévoit l'existence d'un comité multidisciplinaire qui sera un nouvel organisme dans la sphère de la normalisation des activités du cyberespace. Parmi les institutions universelles, le Bureau de Normalisation du Québec continue à tenir sa place, l'article 68 de la loi y faisant expressément appel.

[326] Il est difficile d'établir une liste exhaustive des organismes dont les travaux pourraient fournir une base pour évaluer la fiabilité des procédés de signature électronique. Des travaux de normalisation et de recherche sont menés à plusieurs niveaux et ils englobent pratiquement toutes les formes sous laquelle la signature électronique peut se présenter. Au surplus, même si elles ne portent pas directement sur les schémas de signatures électroniques, les normes peuvent présenter un intérêt pour l'évaluation des divers aspects des capacité des SI qui abritent des processus de création de signature et en conditionnent la fiabilité.

ii. Les normes – un éventail de réponses aux complexités de l'objet évalué

[327] Il n'existe pas de normalisation générale couvrant l'ensemble des éléments nécessaires à la création d'un système de signature électronique.[311] Les normes semblent s'organiser autour de deux sujets principaux, à savoir l'interopérabilité des systèmes et la sécurité des systèmes[312]. Les normes d'interopérabilité couvrent les architectures globales de signature électronique, les formats des messages, les structures des données et la sémantique qui leur est associée. Les protocoles d'échanges qui réalisent des transactions complètes peuvent aussi être gouvernés par des normes. Les normes se rapportant à la sécurité guident la spécification claire des fonctions de sécurité à réaliser, ainsi que l'évaluation de la sécurité des SI, tant du point de vue technique que de sa gestion.

[328] La variété des normes est impressionnante et ne cède aucunement au caractère polymorphe de l'objet d'évaluation. Ainsi, le domaine des algorithmes cryptographiques a attiré l'intérêt du NIST, de l'ISO, du RSA Security Inc. et de Certicom et a donné lieu aux

---

[309] Des informations sont disponibles sur http://www.cenorm.be/aboutcen/aboutcen.htm, visitée en mai 2002.
[310] A.-F. FAUSSE, *op. cit.,* note 37, p. 57
[311] *Id.*, p. 55
[312] *Id.*

normes FIPS[313] et PKCS 1[314]. Pour les messages cryptographiques les normes suivantes ont été élaborées : PKCS 1,6,7,9,10, ISO 14888, RFC 2630, par l'UIT, l'IETF, le RSA Security Inc., le World Wide Web Consortium[315]. Les architectures à clés publiques ont été définies par l'UIT, l'ISO, le RSA Security Inc. et l'IETF moyennant les normes X.509, PKCS 6, RFC PKIX. Cette liste de secteurs directement ou indirectement associés à la fiabilité des SI produisant des signatures électroniques peut se poursuivre à travers les architectures de sécurité, la maîtrise de la qualité, l'accréditation, l'administration des certificats, les cartes à puces et les cadres généraux de la sécurité des systèmes.

[329] Nous sommes portés à croire que tous les éléments constitutifs de la fiabilité des SI développés dans notre 3ème chapitre peuvent être couverts par des normes correspondantes. Ces normes représentent la source principale des critères d'évaluation de la fiabilité de toutes les unités et composantes des SI. Cependant, leur importance n'est pas absolue. La conformité d'un élément de la chaîne de la fiabilité à la norme correspondante ne saurait, dans tous les cas et sans réserve, imposer la conclusion de la fiabilité dudit élément. Cette conformité est sans doute le meilleur moyen de fournir des indices sur la fiabilité d'un objet d'évaluation, mais n'est tout de même pas le seul. Similairement, la non-conformité ne devrait que mettre en doute la fiabilité sans en déclarer le défaut de manière absolue. Il faut avouer qu'il serait simpliste de conclure qu'un logiciel « maison », résultant d'un développement interne, n'offre pas de garanties nécessaires de fiabilité pour la seule raison qu'il ne s'inscrit pas dans le cadre prescrit par les standards. En effet, même si les standards gèrent avec succès la complexité de la fiabilité des SI, la relativité de cette fiabilité demeure toujours liée à une appréciation tenant compte des circonstances particulières, d'où l'importance majeure du processus d'évaluation – l'audit.

[330] Avant de procéder à l'analyse du processus de l'audit, nous nous attarderons brièvement sur normes qui l'encadrent, à savoir les règles organisationnelles et procédurales gouvernant le statut et la hiérarchie des entités auditrices, leur accréditation et leurs activités.

---

[313]NIST, «Federal Information Processing Standards Publications», source :http://www.itl.nist.gov/fipspubs/geninfo.htm, visitée en mai 2002

[314]RSA Security, « Public-Key Cryptography Standards », *RSA Laboratories*, source : http://www.rsasecurity.com/rsalabs/pkcs/, visitée en mai 2002

[315] A.-F. FAUSSE, *op. cit.,* note 37, p. 151

§ 2. Le contexte normatif de la procédure d'évaluation de la fiabilité

a. Les aspects organisationnels de l'audit

[331] Les interrogations sur la fiabilité des techniques de signature peuvent trouver leurs réponses en s'appuyant sur des standards établis et en ayant recours à une procédure d'audit. L'audit se caractérise par une méthode et par des objectifs strictement déterminés. Souvent, référence est faite à la procédure d'audit comme le seul élément concernant la vérification et l'assurance des caractéristiques d'un certain objet. Il faut reconnaître l'exactitude de cette allégation dans la mesure où l'évaluation des capacités d'un certain produit ou service est en effet le processus qui nous fournit l'information finale. Cependant, l'audit n'est pas le seul processus encadrant l'évaluation de la fiabilité d'un objet. Avant de nous pencher sur les caractéristiques du processus d'audit, il importe d'exposer le cadre normatif dans lequel se situe cette vérification. La hiérarchie à laquelle se subordonnent les entités auditrices représente un préalable normatif au déroulement du processus de vérification. L'audit est le dernier maillon d'une chaîne dont le but est l'obtention d'une certitude de fiabilité du moyen de signature.

[332] Parmi les intervenants, notons la présence de l'État, des agences nationales de sécurité, des accréditeurs et, au bas de l'échelle, des laboratoires d'essais pour les produits ainsi qu'enfin des auditeurs.

i. Les gouvernements et les Agences nationales de sécurité

[333] De nombreux gouvernements ont créé des organismes d'État spécialisés – des agences nationales de Sécurité. Par exemple, le Centre de certification de la sécurité des technologies de l'information est un service de la division « sécurité informatique » du Service central de la sécurité des systèmes d'information en France[316]. Le SCSSI devient Direction centrale de la sécurité des SI au sein du Secrétariat général de la défense nationale qui est un service du Premier ministre. La Direction doit occuper une place très importante dans la prise de décisions relatives aux assurances de sécurité de la nouvelle

[316] Des informations sont disponibles sur http://www.scssi.gouv.fr/fr/index.html, visitée en mai 2002.

économie. L'Agence gouvernementale allemande est le *Bundesamt fur Sicherheit in der Informationstechnik*[317]. La *National Security Agency* est l'exemple américain d'agence gouvernementale de sécurité.

[334] Généralement les agences nationales de sécurité assurent des fonctions de base, touchant aux fondements de l'évaluation. Elles procèdent à l'agrément des centres d'évaluation de la sécurité des technologies de l'information. Elles peuvent aussi certifier les produits évalués par les centres d'évaluation agréés. Les schémas d'agrément des évaluateurs sont, dans la majorité des cas, établis par ces organismes. Les agences participent aux actions de normalisation nationales et internationales relatives à la sécurité des systèmes et assurent les relations avec leurs homologues étrangers. Les organismes gouvernementaux synthétisent les normes et les standards relatifs à l'évaluation des produits pour publier des profils génériques de sécurité et des spécifications de sécurité des produits. Ils travaillent aussi à l'établissement de profils de protection des fonctions-types des systèmes, telles les spécifications sécuritaires types des prestataires de services de certification. Leur contribution est majeure et directe dans la conception des normes techniques directes ou plus indirectes dans celle des lois et des règlements. Elles interviennent de manière décisive dans la signature d'accords de reconnaissance réciproque des certificats d'évaluation des produits, tels l'Accord SOG-IS[318] qui réunit 12 pays d'Europe et le *Mutual Recognition Agreement*[319] d'une portée connue comme universelle.

[335] L'autorité des agences nationales de sécurité n'influence pas directement l'évaluation des technologies de signatures électroniques. Cependant ces organismes ont un impact profond et majeur à travers de leurs rôles et leurs pouvoirs en matière de sécurité des systèmes informatiques tant au niveau réglementaire qu'au niveau du contrôle.

ii. Les accréditeurs

[336] L'accréditation vise à vérifier la capacité d'une entreprise à mener une mission. Les entreprises qui font l'objet d'accréditation sont les évaluateurs finaux qui effectuent la

---

[317] Des informations sont disponibles sur http://www.bsi.de/, visitée en mai 2002.
[318] A.-F. FAUSSE, *op. cit.,* note 37, p. 65
[319] Agreement on Mutual Recognition between the United States of America and the European Community, US Government Export Portal, *Market Access and Compliance*,
source : http://www.mac.doc.gov/mra/mra.htm, visitée en mai 2002

vérification des SI, à savoir les évaluateurs des produits et les évaluateurs des systèmes de gestion de sécurité. Dans la majorité des hypothèses, l'évaluateur qui effectuera la cueillette des preuves de la fiabilité d'une technologie de signature électronique se verra dans l'obligation de demander une accréditation afin de pouvoir mener sa mission.

[337] Les accréditeurs représentent des organismes indépendants qui s'assurent de la compétence des entités menant les essais des produits et les audits des systèmes afin d'attester de leur crédibilité. Les accréditeurs vérifient la conformité d'une entité eu regard des normes déterminées afin de fournir éventuellement l'accréditation. Un exemple de délivrance d'accréditation est la suite de normes EN 45000 utilisées pour mesurer les capacités des laboratoires d'étalonnages et d'essais (les laboratoires d'évaluation des produits), les organismes procédant à la certification des produits et les entités effectuant l'audit concernant la qualité des systèmes. Le Comité français d'accréditation est l'exemple d'un organisme s'acquittant des fonctions de vérification et d'attestation de la capacité des laboratoires et des auditeurs de mener leurs missions. Il a été mis sur pied en avril 1994 pour offrir aux consommateurs, mais aussi aux pouvoirs publics une garantie de confiance dans les prestations effectuées par les entités accréditées.

iii. Les certificateurs de produits et les auditeurs

[338] Après les accréditeurs, dans la hiérarchie de la confiance d'un système d'information viennent les certificateurs de produits. Comme nous l'avons observé, un système d'information repose sur une organisation complexe d'unités et d'éléments. Au sein de sa structure, dans tous les cas qui nous intéressent, il existe des dispositifs référant aux technologies de l'information. Ces produits peuvent trouver une application dans plusieurs systèmes d'information et leurs caractéristiques, indépendamment de leur implémentation, sont les mêmes. Pour cette raison, les produits peuvent faire l'objet d'une évaluation de leurs paramètres et d'une appréciation de leurs capacités. Le résultat de cet examen est l'obtention de l'assurance de la stabilité des différents dispositifs et de garanties de leur conception fiable. Dans le cas de la signature électronique, ce processus sera une étape vers nos conclusions sur la fiabilité de sa technologie.

[339] Nous avons placé l'évaluation des produits avant l'audit dans la hiérarchie de l'évaluation des capacités des systèmes d'information. Cette démarche se justifie par le fait

que les conclusions sur la fiabilité des produits peuvent très souvent s'avérer un préalable à l'évaluation du système d'information qui met en oeuvre. Il est vrai que de façon organisationnelle les entités auditrices ne sont pas subordonnées aux évaluateurs de produits. Cependant, si nous envisageons le processus d'évaluation comme une suite de garanties, d'assurances et de vérifications débouchant sur l'audit, la vérification des caractéristiques des produits précède l'examen concret de la fiabilité d'un système d'information déterminé.

[340] La hiérarchie de l'évaluation nous révèle le contexte dans lequel se situe la vérification concrète. Si, entre la base normative (les standards) et l'affirmation sur les qualités de l'objet qui nous intéresse (les conclusions sur la fiabilité) se trouve l'étape intermédiaire de l'évaluation, cette évaluation est aussi un processus complexe, encadré dans cette hiérarchie normative. Finalement, rappelons que la hiérarchie ainsi décrite n'est pas dans tous les cas une organisation obligatoire dans laquelle toute procédure d'audit devrait se situer. Elle peut être mise en place dans le but de faciliter l'obtention de la certitude dans les résultats que l'on souhaite.

[341] À la toute fin, c'est dans l'examen concret d'un SI déterminé que la chaîne d'évaluation se concrétise sur un objet précis, les capacités de l'environnement des processus d'authentification virtuels comme préalable à la fiabilité desdits procédés. Cet examen concret s'effectue lors de la procédure d'audit.

b. Les exigences envers l'auditeur

[342] L'audit est encadré de normes qui en régissent la procédure. Chaque type d'audit exige un encadrement différent. Il existe cependant des principes généraux qui rendent la procédure fiable et qui renforcent la légitimité des résultats de la vérification. Les conditions de la norme EN 45012[320], relatives aux préalables d'accréditation des auditeurs en reflètent une grande partie. La norme définit la mission et les éléments de qualité et de compétences que les évaluateurs des systèmes de gestion de la sécurité de l'information doivent démontrer pour être accrédités. Cette norme ne se rapporte qu'à un type d'audit, celui dont la mission est d'évaluer la qualité des prestataires de services de certification

[320] A.-F. FAUSSE, *op. cit.,* note 37, p. 65

émetteurs de certificats d'identité. Tout de même, la norme systématise des principes qui peuvent trouver une application au-delà du cadre précis d'audit auquel elle se rapporte.

[343] Parmi les premières exigences se trouve celle selon laquelle les services d'évaluation doivent être non-discriminatoires et l'évaluation, impartiale. Un moyen d'atteindre ce but est l'adoption d'un schéma selon lequel les fonctions d'auditeurs et celles de décideurs du résultat de l'évaluation sont accomplies par des personnes différentes. L'évaluateur doit être en mesure de prouver que son organisation et ses activités renforcent son impartialité. D'autre part, l'organisation et la structure légale de l'évaluateur doivent être transparents. L'entité auditrice doit posséder une structure financière lui permettant d'être indépendante dans ses actions et d'éviter la soumission aux pressions corruptrices. L'évaluateur doit assurer la confidentialité de son travail et des données qu'il requiert. Un système de gestion de la qualité des activités doit être en place, y compris un système de gestion documentaire fiable et capable d'accueillir les documents produits pendant l'évaluation et ses suites. Les activités de l'évaluateur doivent être conservées et documentées de manière sûre et durable. Un point important dans le profil de l'évaluateur pour assurer sa crédibilité est la transparence des conditions d'enregistrement, de retrait ou de suspension des certificats d'évaluation. Une attention particulière est requise quant à la place des sous-traitants et du personnel. L'entité auditrice doit pouvoir répondre de ses sous-traitants en termes de savoir-faire et de respect des devoirs d'un évaluateur. De même, l'évaluateur doit définir, formaliser et maîtriser l'intervention de son personnel. Celui-ci doit être compétent dans le domaine de l'évaluation des systèmes de gestion de sécurité

[344] Un exemple d'encadrement normatif de l'évaluation des capacités des systèmes d'informations est le Décret français no 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.[321] L'acte institue une Direction centrale de la sécurité des systèmes d'information (DCSSI), des centres d'évaluation agréés ainsi qu'un Comité directeur de la certification en sécurité des technologies de l'information. Les termes de ce décret représentent une application normative concrète des principes généraux du cadre organisationnel de l'évaluation.

[321] J.O. Numéro 92 du 19 Avril 2002 page 6944

[345] Il importe maintenant de tourner notre attention sur la procédure même de vérification et d'évaluation afin de dépister sa logique, les principes sur lesquels elle repose et les objectifs qu'elle vise. Cette analyse démontrera l'acheminement vers la décision sur la fiabilité d'un système d'information et celle sur la performance d'une technologie de signature se déroulant au sein de ce système.

Section II – VERS UNE RÉPONSE AUX INTERROGATIONS – LE PROCESSUS ET LES RÉSULTATS DE L'ÉVALUATION

[346] Dans cette section concernant la procédure d'évaluation et son résultat, nous examinerons d'abord l'audit en tant que moyen de cueillette et d'analyse des informations. Ensuite, nous présenterons les modèles d'audit directement applicables en matière d'appréciation des caractéristiques des processus de réalisation de signatures électroniques.

§ 1. Le processus d'audit

[347] La fiabilité des procédés de signature électronique s'apprécie en plusieurs étape., Ses indicateurs ont fait l'objet de notre 3ème chapitre. L'évaluation du caractère fiable des moyens d'authentification informatiques implique donc la cueillette d'éléments probants dont l'analyse fournira la base des réponses. La recherche de ces éléments s'effectue au cours de la procédure d'audit.

a. La cueillette et de l'évaluation des informations

i. L'audit - généralités

[348] L'audit est une procédure de vérification systématique.[322] Il poursuit l'objectif d'obtenir et d'évaluer objectivement une preuve afin d'établir l'exactitude de certaines

[322] B. BRUN, *loc. cit.*, note 274

affirmations. Ce mode d'évaluation peut être effectué de diverses manières et couvrir des champs différents.

[349] Les professeurs Parisien et Trudel distinguent deux grands types de missions en audit informatique, à savoir l'audit financier et l'audit opérationnel[323]. L'audit financier a pour objectif la certification des états financiers. Les objectifs de l'audit financier sont d'évaluer le contrôle interne informatique comme composante du contrôle interne des entreprises. Les buts que vise l'audit financier sont notamment la vérification de la fiabilité, l'intégrité et la pérennité des données et des traitements, ainsi que l'observation des dispositions se rapportant aux traitements informatisés. L'audit qui représente un intérêt pour les fins de notre étude est l'audit opérationnel parce que c'est la procédure qui peut fournir des conclusions sur les capacités d'un système.

[350] L'audit opérationnel se caractérise par une plus grande ampleur.[324] Très souvent il sert à répondre aux interrogations des dirigeants qui souhaitent contrôler le choix et les investissements informatiques. Ayant pour objet la vérification de l'organisation informatique de l'entreprise, l'efficacité des services, la performance des matériels et des logiciels[325], ce type d'examen cible les informations pertinentes compte tenu des interrogations sur le bon fonctionnement des SI et de la fiabilité des processus qui s'y déroulent.

[351] L'étendue de l'audit opérationnel peut varier. L'évaluation peut avoir pour objet les procédures d'une entreprise au sens large, le niveau de qualité des processus ou un secteur spécifique.[326] L'audit opérationnel, comme l'audit financier, peut être interne et externe. Dans l'hypothèse de l'audit interne, l'entreprise concernée effectue elle-même l'examen à l'aide des procédures qu'elle détermine.

[352] L'audit externe procure des garanties maximales de fiabilité. C'est la forme la plus fréquente, elle jouit d'une plus grande confiances, mais elle est aussi plus longue et coûteuse.

---

[323] S. PARISIEN, P. TRUDEL, *op. cit.,* note 27, p. 80
[324] *Id.*
[325] *Id.*
[326] B. BRUN, *loc. cit.*, note 274

ii. L'essence de l'audit - la cueillette et l'évaluation d'éléments probants

[353] L'audit désigne le processus d'examen destiné à recueillir et à évaluer les éléments probants relatifs à certaines assertions. Cette définition, de Abbyad, Chlala et Anderson au sujet de l'audit financier[327], peut être étendue à d'autres types d'audit, car tous les types d'audit ont la même mission : la vérification de certains faits. Selon ces auteurs, cette affirmation ne signifie pas que le vérificateur doit fonder son opinion sur des preuves certaines et absolues, mais son but est de recueillir et d'évaluer des éléments probants, suffisants et adéquats en vue d'appuyer une opinion.

[354] Pour que les éléments probants soient considérés adéquats et suffisants aux fins de la justification d'une opinion, trois facteurs doivent être pris en considération[328] : la précision, le degré de certitude et la disponibilité des éléments probants. En ce qui concerne le premier facteur, l'opinion généralement admise est qu'il est impossible et irraisonnable de rendre impérative l'obtention d'une précision absolue. L'importance de l'information déterminera le degré de précision requis, compte tenu des risques associés à la procédure de vérification. Généralement, le risque est apprécié par l'évaluateur lui-même et, dans le contexte de l'audit, il découle de la possibilité que des erreurs ne soient pas décelées.

[355] Ces risques sont appréciés selon l'importance relative des objets de vérification. Par conséquent, l'entité vérificatrice fixe le niveau d'exactitude requis selon l'importance relative des éléments probants.

[356] Dans le contexte de l'audit, ces deux concepts se trouvent en étroite dépendance. La notion de degré de certitude ne peut s'exprimer qu'en relation avec l'importance relative. Lorsque les auditeurs réfèrent à un degré de certitude attaché à leurs conclusions, ils font toujours appel à la portée que pourrait avoir une éventuelle inexactitude.

[357] La cueillette et l'évaluation des preuves relatives aux faits intéressant l'audit est l'étape autour de laquelle s'articule toute procédure de vérification. Pour cette raison nous avons jugé pertinent de dépister les principes qui guident le processus. Ayant circonscrit ses principes, nous nous pencherons sur les applications concrètes de la procédure d'évaluation.

---

[327] S. PARISIEN, P. TRUDEL, *op. cit.,* note 27, p. 79
[328] *Id.*, p. 81

b. Les applications concrètes des principes de l'audit

i. Les méthodes d'évaluation

[358] L'évaluation de la fiabilité d'un processus de réalisation de signatures au sein d'un système d'information fait appel à la vérification du degré de sécurité du système au niveau de sa conception et sa réalisation, de même que du point de vue de sa sensibilité aux vulnérabilités. La méthode usuelle s'appuie sur un ensemble de critères indépendants servant à mesurer et à quantifier les caractéristiques du système. Cette méthode s'oppose à la procédure de « validation et vérification indépendantes » (IVV)[329] selon laquelle une équipe de professionnels s'acquittaient de la fonction de concevoir et de bâtir le système, alors qu'une autre était chargé de l'évaluation du design. Ce qui entraînait parfois la construction d'un système identique pour fins de comparaison avec l'objet de l'évaluation[330].

[359] Parmi les premiers documents contenants des critères d'évaluation indépendants nous citerons les Critères d'évaluation des systèmes d'ordinateurs sûrs du Département de la Défense des États-Unis, nommés le Livre orange[331]. Le livre a été publié en 1985 par le Centre national de la sécurité des ordinateurs (NCST)[332], une division de la NSA. Le livre Orange permet de mesurer la sécurité des systèmes et de les classifier par niveaux de sécurité. Il propose aussi des méthodes de vérification. L'évaluation se solde par l'attribution d'un niveau de sécurité, D (sécurité minimale), C (protection discrétionnaire), B (protection obligatoire) et A (design vérifié). Ces classes se divisent en sous-catégories pour mieux répondre aux divers besoins.

[360] Le livre orange n'était pas suffisamment flexible et ne pouvait pas toujours refléter objectivement le niveau de sécurité des SI, parce que ses niveaux ne rendaient pas compte de manière adéquate du profil de fiabilité des systèmes. De plus, initialement le livre n'était pas adapté aux systèmes interconnectés, ce qui en a réduit sensiblement l'utilité.

---

[329] Le terme anglais est *Independent Verification and Validation.*
[330] B. SCHNEIER, *op. cit.,* note 209, p. 131
[331] U.S. Department of Defense, « U.S. Department of Defense Trusted Computer System evaluation Criteria », Décembre 1985, source: http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html, visitée en mai 2002
[332] The National Computer Security Center. Des informations sont disponibles sur http://csrc.nist.gov/, visitée en mai 2002.

[361] Plusieurs essais de codification des critères d'évaluation de la fiabilité des systèmes d'information ont récemment été proposés comme les Critères canadiens d'évaluation des produits informatiques sûrs[333] ou les Critères d'évaluation de la sécurité des technologies de l'information (ITSEC)[334] européens. La proposition du Gouvernement américain à ce sujet s'est matérialisée par les Critères Fédéraux.

[362] Face à la croissance des échanges internationaux et aux besoins de communications sécurisées, comme les communications interbancaires, Internet, la télévision payante, les systèmes transactionnels, les systèmes de signature électronique, un ensemble de critères aspirant à l'universalité ont été mis sur pied. Les *Critères d'évaluation de la sécurité des technologies de l'information*[335], nommés couramment la méthode des *« critères communs »* ont été élaborés à la suite des efforts mutuels des gouvernements allemand, américain, anglais, australien, canadien, français, hollandais ainsi que celui de la Nouvelle Zélande[336] (voir la figure 1, présentant le processus de création des Critères communs) . Par la suite ont adhéré la Finlande, la Grèce, l'État d'Israël, l'Italie, le Norvège et l'Espagne.[337] Ces critères ont été votés en norme ISO/IEC 15408. L'accord d'adhésion aux Critères communs est ouvert. Ces critères deviennent peu à peu la base universelle de reconnaissance mutuelle des résultats d'évaluation sécuritaire entre pays. Fausse soutient[338] que les critères communs représentent un socle international solide en matière d'évaluation sécuritaire et que le standard, appliqué aux signatures numériques, représente une opportunité d'apprécier leur degré de sécurité. L'industrie de la carte à puces a investi des efforts considérables afin d'en adopter une propre version adaptée. Les critères communs, appliqués en matière de signature électronique en général, semblent donc offrir une base méthodologique solide pour l'évaluation de la fiabilité des SI et des signatures réalisées à l'aide desdits systèmes.

---

[333] Canadian Trusted Computer Products Evaluation Criteria
[334] Information Technology Security Evaluation Criteria
[335] Common Criteria for Information Technology Security Evaluation, Version 2.1 / ISO IS 15408, ci-après cités Critères communs, source: http://www.commoncriteria.org/ , visitée en mai 2002
[336] Critères communs, « Origins of the Common Criteria », *Roadmap to the Common Criteria*, source: http://www.commoncriteria.org/docs/origins.html, visitée en mai 2002
[337] Critères communs, « CCRA Participants », source : http://www.commoncriteria.org/registry/NatScheme.html, visitée en mai 2002
[338] A.-F. FAUSSE, *op. cit.,* note 37, p. 334

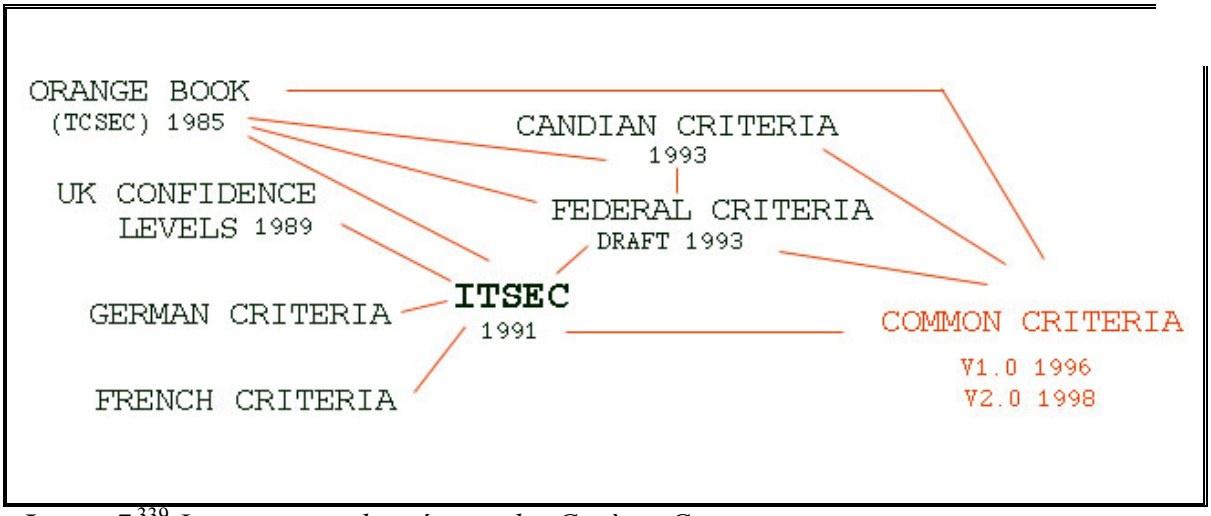


Image 7.[339] *Le processus de création des Critères Communs.*

ii. La méthode des critères communs[340]

[363] Selon la méthode des critères communs, il est nécessaire de spécifier la portée du système considéré, suivant une méthode de description partant de l'ensemble du système puis, au besoin, en décrivant progressivement les fonctions assurées par les entités de niveau inférieur. On sélectionne ensuite les « actifs » à protéger en fonction de la stratégie de l'organisation détentrice, de la valeur financière ou morale qu'ils recèlent. Il faut également prendre en considération les contrats applicables avec des tiers, de la réglementation applicable, ayant par exemple trait à la sûreté nationale, la vie privée ou la signature électronique. L'étape finale dans la description du système est l'identification de son environnement incluant les utilisateurs, personnes, systèmes annexes connectés, ainsi que leurs interactions et dépendances.

[364] De cette description, les évaluateurs déduisent et systématisent trois résultats : la définition des actifs, des menaces, des attaques et des vulnérabilités reconnues; les hypothèses sans lesquelles le système ne peut pas opérer ainsi que la politique de sécurité regroupant les règles d'administration et de conduite ou aux actifs. En d'autres mots, ces trois éléments décrivent les besoins fondamentaux en un tout complet et cohérent. À l'étape suivante tout cela est traduit en exigences sécuritaires.

[339] Critères communs, *op. cit.,* note 336
[340] Critères communs, *op. cit.,* note 335

[365] La protection des actifs ainsi circonscrits contre une menace peut être réalisée par le contrôle de l'environnement du système ou par la mise en place de techniques de sécurité au sein du système. Très souvent une combinaison entre les deux approches est utilisée.

[366] Aux termes des critères communs, après la spécification des objectifs de sécurité, il y a lieu de spécifier les fonctions de sécurité qui vont permettre de réaliser les objectifs. La méthode des critères communs propose un catalogue très complet de fonctions dans lequel le concepteur peut puiser, afin de spécifier la « cible de sécurité »[341], c'est-à-dire le système à développer et évaluer. Cependant le guide ne restreint pas les utilisateurs dans leurs choix, ils conservent la possibilité d'inventer leurs propres fonctions. Une organisation par classe, famille et composant de sécurité a été adoptée afin de décrire les fonctions proposées de manière structurée. Les classes décrivent les grands types de fonctions, comme la classe FAU, regroupant les fonctions de surveillance d'audit des activités de sécurité du système - journalisation d'événements, analyse[342]; la classe FCO, définissant les fonctions de non-répudiation - origine et réception; la classe FCS, spécifiant les algorithmes cryptographiques utilisés dans le système[343].

[367] Les familles comprennent des composants de sécurité indivisibles. Dans une classe, on place, en général, plusieurs familles correspondant à différents types de protection. Par exemple, dans la classe FDP (protection des données utilisateurs), on trouve des familles de composants telles que: Intégrité des données stockées[344] (FDP - SDI), Authentification des données[345] (FDP - DAU).

[368] La norme définit trois niveaux de potentiel d'attaque de l'agent menaçant et trois niveaux correspondants de résistance aux attaques: bas, modéré et haut, demandant un fort niveau d'expertise et des moyens très importants.

---

[341] Critères communs, « Specification of Security Targets », source: http://www.commoncriteria.org/cc/part1/part1c.html, visitée en mai 2002

[342] Critères communs, « Security Audit », source: http://www.commoncriteria.org/cc/part2/part2fau.html, visitée en mai 2002

[343] Critères communs, « Cryptographic support (FCS) » , source: http://www.commoncriteria.org/cc/part2/part2anfcs.html, visitée en mai 2002

[344] Critères communs, « Class FDP: User data protection » , source: http://www.commoncriteria.org/cc/part2/part2fdp.html, visitée en mai 2002

[345] Critères communs, « Data authentication (FDP_DAU) », source: http://www.commoncriteria.org/cc/part2/part2fdp.html#pgfId-37880, visitée en mai 2002

[369] Le grand apport de la méthode se manifeste par le fait qu'elle fixe divers niveaux de qualité et de difficulté pour évaluer chacun des sujets d'assurance décrits précédemment et qu'elle synthétise tout cela en un niveau global d'assurance.[346] Les niveaux globaux vont de EAL 1 à EAL 7, définissant un minimum à réaliser pour chaque sujet, comme suit : EAL 1 équivaut à la qualification « Testé fonctionnellement »; EAL 2 signifie « Testé structurellement » ; EAL 3 réfère à un système « Méthodiquement testé et vérifié »; EAL 4 garantie que l'objet est « Méthodiquement conçu, testé et revu »; EAL 5 est attribué aux systèmes « Semi-formellement conçu et testé »; EAL 6 - « Conception et test semi-formel »; EAL 7 désigne le système correspondant à la qualification « Conception vérifiée et tests formels ».

[370] Le niveau d'assurance global fixe le niveau de maîtrise du produit ainsi que son aptitude à résister à des tests de pénétration. C'est donc un bon indicateur, mais il ne décrit pas les exigences sécuritaires du système. Ce complément sera apporté par la définition du *profil de protection* qui se fait par la construction de la cible d'évaluation

[371] Les concepteurs de systèmes ou de produits - cartes à puce, systèmes d'exploitation d'ordinateurs - doivent soumettre leurs systèmes à des évaluateurs – des spécialistes indépendants, des « centres d'évaluation de la sécurité des technologies de l'information » (CESTI). Ceux-ci évaluent la conformité du système réalisé par rapport à ces spécifications. La méthode des critères communs guide l'évaluateur dans sa tâche, en spécifiant les éléments probants qu'il doit rechercher, vérifier et analyser pour chaque composant d'assurance. Deux aspects essentiels sont examinés au cours de l'évaluation: la maîtrise de la conception du système et la politique de sécurité visant à maîtriser des risques d'environnement (complétude, qualité, cohérence) ; la résistance pratique aux tests réels de pénétration. L'évaluation, nous l'avons souligné, est un processus long et complexe, nécessitant un très haut niveau d'expertise.

[372] Un rapport est remis à la fin de l'évaluation. Il faut mentionner seuls dix CESTI sont actuellement aptes à mener des évaluations sécuritaires critères communs d'un niveau EAL 5 à travers le monde.

[373] Le certificat de conformité à un niveau d'évaluation est public, ce qui malheureusement ne décrit pas de manière détaillée le contenu sécuritaire. Pour cette raison

---

[346] EAL est une abréviation de *Evaluation Assurance Level.,* Critères communs*,* « Evaluation assurance levels », source: http://www.commoncriteria.org/cc/part3/part304.html, visitée en mai 2002

la méthode des critères communs offre l'outil du *profil de protection*[347] pour rendre publics les moyens qui ont mené à la délivrance du certificat de conformité. Le profile de protection (PP) est un concept faisant appel à un ensemble-type standardisé de capacités sécuritaires, applicable à un produit ou à un groupe de produits. Par exemple, un profil pourra être applicable aux terminaux, utilisés pour la distribution des billets de banque ou bien aux cartes à puce dédiées à la signature numérique. Il ne s'agit donc pas de cibler un produit particulier mais de brosser le tableau des menaces pour une classe de produits et donner une liste des fonctions de sécurité envisagées pour les affronter. Le profil est constitué en définissant tout d'abord le type de produit, ses fonctions de base, les actifs qu'il convient de protéger. Par exemple, dans le cas d'un circuit intégré réalisant des fonctions cryptographiques, on décrira les ressources du circuit (mémoires, registres), dans quel contexte le produit est utilisé et son cycle de vie (fabrication, programmation et exploitation). Puis on détaille l'environnement du produit : les menaces, les hypothèses et la politique de sécurité. De cette manière, on systématise les objectifs de sécurité pour le produit en question et pour son environnement.

[374] La norme des critères communs permet de mener une procédure d'audit approfondie. L'évaluation effectuée en conformité avec les critères communs renfermera en soi de sérieuses garanties de cohérence et d'exhaustivité. Il est vrai que les critères communs ne sont pas l'unique norme ayant pour objectif de spécifier et de circonscrire le cadre de l'évaluation sécuritaire des systèmes. Cependant, le standard nous offre une image du contenu de la procédure d'audit. Après les observations sur les principes de base de l'évaluation, une description du contenu même de la vérification s'imposait afin d'illustrer les démarches et les étapes nécessaires à la préparation d'une opinion sur la fiabilité. Formulés de manière à englober une grande variété de cas, les critères communs peuvent et sont déjà adaptés aux différents groupes de systèmes d'information qui peuvent s'avérer un milieu ambiant de signatures électroniques. Ceci dit, leur contenu dirigerait les procédures d'évaluation de la fiabilité des signatures à travers l'évaluation des caractéristiques des systèmes qui les réalisent.

[375] Notons que la procédure d'audit doit apporter des réponses à des interrogations précises. L'audit dont nous avons envisagé l'aspect procédural, peut déboucher sur

---

[347] Critères communs, « Specification of Protection Profiles »,
source: http://www.commoncriteria.org/cc/part1/part1b.html, visitée en mai 2002

l'émission d'un rapport, mais parfois aussi sur un audit complémentaire. Dans certaines circonstances, un certificat de conformité peut résulter de la procédure d'audit. Après l'analyse des principes généraux de l'audit et l'exposition des éléments centraux de la méthode des critères communs, il convient de nous pencher sur les résultats de l'audit.

§2. Les réponses - les résultats de l'audit

[376] Comme il a été explicité, l'audit est une procédure de cueillette et d'évaluation de données relatives à l'exactitude d'une affirmation concrète. Dans le cas d'espèce, l'évaluation porte sur l'interrogation concernant une caractéristique spécifique des systèmes d'information, à savoir sa capacité à accomplir ses fonctions avec la stabilité requise pour assurer le déroulement de processus fiables de création de signature électronique. Il est donc important de nous intéresser à la façon dont les résultats de l'audit répondent à l'interrogation sur la fiabilité d'une technologie et, par conséquent, sont rendus opérationnels.

a. La certification

[377] Un moyen de matérialiser les réponses fournies par le processus d'évaluation réfère à la certification. Pour les fins de notre étude, la définition utilisée par Bernard Brun de la certification nous paraît pertinente[348]. Parmi les nombreuses définitions de ce phénomène, l'auteur choisit la suivante :

> *« La certification est une procédure par laquelle une tierce partie donne une assurance écrite qu'un produit, un service, un système qualité, un organisme est conforme à des exigences spécifiées. »*

[378] La certification n'est pas apparue avec le commerce électronique. Elle a une histoire relativement longue. Un exemple ancien de certification réfère aux activités des

[348] B. BRUN, *loc. cit.*, note 274

Underwriters Laboratories[349]. Les laboratoires sont un organisme indépendant de vérification et de certification d'une ample gamme de produits. L'organisation a été mise sur pied en 1893 par William Henry Merrill qui a été chargé de découvrir pourquoi le Palais de l'électricité à l'Exposition colombienne à Chicago avait été aussi souvent sinistré par des incendies. C'est de cette manière que le modèle d'entreprise a été conçu. Le but initial des *Underwriters Laboratories* était de tester l'équipement électrique des entreprises et leur mission était de servir aux intérêts des compagnies d'assurance. Les attestations de qualité de l'équipement électrique délivrées par le certificateur se sont transformées en prérequis de la conclusion d'un contrat d'assurance pour l'entreprise qui utilisait l'équipement électrique certifié.

[379] La certification en matière de systèmes d'information peut s'avérer un des moyens de matérialiser les conclusions de l'évaluation des capacités desdits systèmes. Les marques de certification sont, quant à elles, les moyens de publiciser la certification. La certification peut varier par sa nature, son ampleur, son niveau, ses auteurs. La portée de la certification dépend des standards utilisés, du mode d'évaluation, de la manière de traitement de l'information, du mécanisme contractuel sur la base duquel elle s'effectue, du statut du certificateur. Un facteur exerçant un impact profond sur la portée de la certification est le degré de sa reconnaissance de l'agent certificateur. Dans le cas où celui-ci est reconnu par les industries d'un secteur d'activité donné, ou encore par un gouvernement, la valeur de la certification alors émise s'en verra grandement augmentée. Dans d'autres situations, la reconnaissance par le gouvernement est obligatoire. Tel est le cas de l'attribution des EAL conformément au standard des *critères communs*, lorsque seuls des organismes accrédités sont autorisés à octroyer certains certificats. La nature et la portée de la certification sont sans doute des facteurs majeurs de l'autorité du certificat.

[380] En tant que processus, la certification se situe logiquement après la vérification effectuée au cours de l'audit. En se basant sur les constats de l'évaluation, elle est gouvernée par un contrat entre le certificateur et l'entité certifiée. Bien que la certification comporte les caractéristiques d'un acte unilatéral, il n'en demeure pas moins qu'elle s'inscrit dans un cadre contractuel précis, le certificateur ne jouissant pas d'un pouvoir arbitraire. La certification est une reconnaissance de conformité relativement à des

---

[349] Bruce SCHNEIER, «Cyber UL ?», *Counterpane Internet Security*, *Crypto-gram Newsletter*, 15 janvier 2001, source: http://www.counterpane.com/crypto-gram-0101.html, visitée en mars 2001

paramètres déterminés. Le certificateur doit se baser sur ces paramètres pour déterminer s'il l'octroie ou non. L'encadrement contractuel de la certification est aussi déterminant pour établir le poids à accorder aux affirmations dont elle fait état.

[381] La dernière étape de la certification est l'attribution de la marque de certification qui peut être sous la forme de sceau, certificat ou toute autre marque matérialisant les résultats de la décision du certificateur. Dans le cas de la certification, c'est cette marque qui rend tangibles les affirmations sur les aspects de l'entité certifiée qui font l'objet de la certification.

[382] La certification est susceptible de jouer un rôle majeur dans le cas de la signature électronique. Elle facilite la prise de décisions concernant les caractéristiques des méthodes de signature. Comme nous l'avons explicité, l'octroi des attestations de conformité aux termes des Critères communs représente une certification. La qualification et l'accréditation des PSC selon la Directive européenne[350] et La Loi concernant le cadre juridique des technologies de l'information du Québec[351], de par leur nature, sont des formes de certification des prestataires. Tenons compte, tout de même, que la certification n'est pas l'unique moyen de matérialiser les résultats de l'évaluation des capacités d'un objet. De plus, même si le certificat existe pour attester de certaines capacités de la signature électronique ou du système à l'aide duquel elle a été apposée, ceci ne devrait pas obligatoirement emporter la conviction sur ces capacités. Notons que cet outil facilite et guide les appréciations sur les qualités de l'objet certifié mais la prise en considération des affirmations du certificat se fera toujours sous le jour des particularités du processus de certification que nous venons d'exposer.

b. L'adéquation des moyens d'évaluation possibles dans le cyberespace

[383] L'évaluation des qualités des produits est un processus ancien. Aussi, son application dans le cyberespace ne surprend pas. Le développement du processus d'évaluation des capacités de l'environnement virtuel, à partir des standards qui en fournissent la base et à travers de la procédure de vérification, est enfin bâti pour permettre

[350] Directive européenne, préambule (11), article 3 (3), précitée, note 9
[351] L.C.C.J.T.I ., article 53, précitée, note 10

de trouver la réponse à notre question initiale. C'est ce schéma que nous appliquons pour remédier à l'interrogation sur les capacités d'un système d'information et qui nous fournira un résultat concret sur l'aptitude du système examiné d'être le théâtre de processus fiables de réalisation de signatures électroniques.

[384] Tout de même, l'évaluation des produits, comme terme générique, dans le cyberespace doit être appropriée à ses modalités. À l'heure actuelle la société ne pourrait se vanter d'un schéma efficace pour juger les capacités des phénomènes virtuels. Selon Schneier, la cotation et le classement des éléments du cyberespace selon leurs qualités sont des mécanismes inappropriés, au moins de nos jours[352].

[385] Selon l'auteur plusieurs facteurs empêchent la cotation graduelle des produits et des systèmes d'information dans l'espace informatique. En premier lieu, la sécurité du cyberespace est toujours en mouvance, le rythme auquel de nouvelles vulnérabilités et de contre-mesures correspondantes font leur apparition est extrêmement rapide. La vérification des capacités des systèmes virtuels d'information est, selon l'auteur une tâche ambitieuse caractérisée par une grande complexité. La relativité de la fiabilité d'un processus est d'autre part l'obstacle qui entrave le classement graduel de ses caractéristiques. Nous ne saurions prétendre que les procédures d'évaluations disponibles peuvent donner du sens à une grille d'évaluation selon laquelle les capacités d'un phénomène pourraient être typées[353]. De surcroît, les défaillances des systèmes d'information ne sont pas dans tous les cas, évidentes, contrairement à la majorité des hypothèses dans le monde réel. La prise en considération du contexte et des pratiques reliées à la sécurité virtuelle rendent encore plus complexe l'évaluation et l'octroi de labels de qualité dans l'examen des propriétés d'un système d'information fonctionnant dans le cyberespace.

[386] Tout en adhérant sans réserve à ce que l'auteur écrit, nous estimons important de souligner que les difficultés d'évaluer les systèmes d'information virtuels sont provoquées par l'état actuel de l'architecture. Cet état nous empêche d'évaluer efficacement ses propriétés. Il serait légitime de soutenir que dans un avenir prochain la donne serait changée. Sans vouloir décrier les appels optimistes tournés vers l'avenir, notre but est uniquement de démontrer que nos recherches sur les interrogations concernant l'approprié

---

[352] B. SCHNEIER, *op. cit.,* note 349

[353] Comme le soutient Schneier, si un serveur peut être classé à l'intérieur d'une grille de 1 à 10, il serait difficile d'attribuer un sens à chacun des grades : « *What does a 9 mean?* », *Id.*

et l'inapproprié, le possible est l'impossible, sont contingentées par le cyberespace d'aujourd'hui, variable se modifiant avec une vélocité remarquable.

Conclusion partielle – L'aspiration à une connaissance de l'environnement

[387] Il est impossible d'appréhender le phénomène de la signature informatique en faisant abstraction de son environnement qu'est le cyberespace. Tout au contraire, la nouveauté des moyens d'authentification virtuels et les conséquences en découlant devraient être considérées comme un résultat de cette appartenance. Nous avons démontré que le standard de fiabilité, une règle juridique, possède un contenu technique est sa substance est essentiellement déterminée par les propriétés de l'architecture du cyberespace. Ainsi, si l'interrogation sur la fiabilité des procédés virtuels d'authentification traduit un manque de maîtrise de l'environnement, l'évaluation de ses caractéristiques par les mécanismes développés à cet effet peut permettre de combler cette ignorance.

[388] L'évaluation des caractéristiques des systèmes d'information bise à fournir des certitudes. Si le droit se tourne, à plusieurs occasions, vers le concept de fiabilité de la signature électronique sous la forme d'exigences ou de critères d'application de ses normes, le besoin se fait ressentir d'apporter les réponses à la question de la fiabilité dans chaque situation concrète. Dans ce contexte, l'appréciation des éléments qui en forment le contenu est une étape essentielle. Le jugement de la fiabilité s'inscrit dans un cadre institué à cet effet. Il est basé sur des standards établis et alimentés par une procédure d'audit. Le jugement sur les caractéristiques déterminées d'un système d'information nous fournit des conclusions sur la manière dont ce système d'information accomplit ses fonctions, parmi lesquelles, pour notre étude, se situe le processus de création de signature.

[389] Selon nous, le schéma mis en place pour fournir la base de l'évaluation en matière de signature électronique présente, en partie, le désir, plus général encore, de se doter d'une connaissance de l'environnement dans lequel elle existe. Enfin la connaissance et la maîtrise du cyberespace ne font que leurs premiers pas et s'inscrivent dans une évolution dont nous ne saurions ignorer les effets. L'architecture du monde virtuel est aussi en voie de développement incessant. À notre avis ce sont les deux processus parallèles, le

développement de l'architecture d'une part et l'amplification de nos connaissances et nos expériences dans le cyberespace d'une autre qui définiront les besoins en droit, comme ils le font à l'étape actuelle. C'est en tenant compte de ces deux processus parallèles qu'une démarche juridique prospective pourra être adoptée.

Conclusion

[390] Notre étude a été consacrée à un phénomène juridique – l'institution de la signature. D'autre part, cette étude s'est intéressée aux réalités auxquelles cette institution juridique se rapporte – la signature manuscrite et la signature électronique. Comme nous l'avons démontré, il existe une chaîne logique entre ces trois réalités. L'institution de signature a été la sanction du droit de l'avènement du seing manuel. La signature électronique est, à la différence de la signature traditionnelle, une réalité survenue postérieurement à l'existence de l'institution de signature en droit.

[391] Dans les rapports sociaux, le besoin d'identifier les auteurs des actes, ainsi que de démontrer leur attitude envers ces actes a toujours été une nécessité impérieuse pour le droit. Parmi les nombreux moyens destinés à servir cette fin, la signature manuscrite s'est distinguée et s'est imposée comme le moyen le plus efficace. Cette imposition de la signature traditionnelle a eu pour résultat la création de l'institution de signature en droit – un ensemble de règles juridiques consacrant les conséquences liées à l'usage du seing manuel. Ainsi, inspirée par la réalité physique qu'est la signature manuscrite, le droit a sanctionné son usage en lui attribuant des conséquences juridiques que représente l'institution de signature. L'autre facette de ce processus est la détermination du contenu de l'institution de signature par les particularités de la signature manuscrite. Lorsque les règles du droit se modelaient, le seul moyen possible de signer était le seing manuel. De ce point de vue, il serait légitime de soutenir que l'institution juridique de signature représente en effet la sanction légale de la signature manuscrite.

[392] De nos jours la donne est changée. L'institution de signature n'est plus un ensemble de normes régissant l'usage de signature manuscrites, son emprise étant étendue sur d'autres phénomènes. Le droit a reconnu l'appellation de signature à une grande variété de formes du cyberespace. Les conditions pour cette reconnaissance sont clairement définies – pour avoir les conséquences juridiques prescrites par l'institution de signature, tout moyen doit accomplir les fonctions de la signature manuscrite (l'identification du signataire et son adhésion au contenu de l'acte signé). Cette condition est une règle de droit s'appliquant à toute forme de signature autre que la signature manuscrite. Cependant, en dehors de ce

préalable à l'admission des procédés électroniques en droit, le contenu de l'institution de signature demeure inchangé.

[393] Dans ce contexte, nous nous retrouvons devant une réalité dont les effets ont fait l'objet de notre étude. Le droit a étendu son emprise sur des phénomènes différant de la signature manuscrite grâce à des normes procédurales, c'est-à-dire, sans modifier substantiellement ses règles. Par conséquent, bâtie et modelée selon les particularités du seing manuel, l'institution juridique de signature s'est avérée forcément inadaptée aux à l'usage des signatures électroniques. Pour remédier à cette inadaptation, le droit a recouru à l'application du *standard de fiabilité* des signatures électroniques. Afin de s'ajuster aux utilisations des signatures modernes sur le plan probatoire, l'institution juridique de signature s'est tournée vers ce standard qui se décompose en des garanties d'un lien fiable entre la signature et son auteur et entre la signature et le contenu de l'acte signé. L'exigence de fiabilité, une règle juridique de par ses conséquences, possède un contenu qui fait appel à un ensemble de règles techniques liées à la signature électronique.

[394] Ces règles techniques dépendent à leur tour des propriétés de l'environnement dans lequel se situe le procédé de signature électronique. C'est dans les propriétés de l'architecture du cyberespace que le standard de fiabilité trouve son contenu. Tout élément de l'architecture, est susceptible d'influencer la fiabilité du procédé électronique de signature qui résulte d'un processus mis en oeuvre au sein d'un ensemble hétéroclite de machines, logiciels, données. Ainsi, le standard de fiabilité se décompose en un grand nombre de règles techniques associées à chaque élément du milieu ambiant de la signature électronique. Il est alors légitime de conclure que le droit appréhende les nouveaux moyens d'authentification cybernétiques à travers des particularités de leur environnement.

[395] Force est aussi de conclure que le standard de fiabilité est un ensemble de règles juridiques, possédant un contenu technique, qui ne concernent que les signatures électroniques. Les interrogations du droit sur la fiabilité de l'environnement des procédés d'authentification ne se manifestent que sur le plan des signatures électroniques. C'est uniquement en matière d'authentification électronique que l'institution juridique de signature nécessite un ajustement. Ce constat illustre un des éléments centraux de ce travail quant aux phénomènes liés au fait que la signature manuscrite est une réalité précédant la création de l'institution juridique de signature, alors que la signature électronique lui est postérieure.

[396] L'intérêt porté par le droit aux particularités de l'environnement de la signature électronique est susceptible de porter à confusion lorsque l'on envisage les concepts de signatures manuscrite et celui de signature électronique. Nous avons soutenu l'affirmation que la signature électronique est considérée comme étant un processus intimement liée à son environnement. En revanche, en matière d'authentification traditionnelle, à cause du désintéressement du droit de la fiabilité du procédé manuscrit de signature et des particularités de son environnement, on risque d'être porté à croire que le seing manuel est un procédé qui n'implique que « *la main de quelqu'un qui puisse écrire avec une plume ou quelque chose de similaire* »[354]. Ceci fonde souvent une opposition entre la signature manuscrite, un procédé simple d'authentification d'une part et sa contrepartie électronique qui représente un processus complexe situé dans le cyberespace, et réalisé grâce à l'ensemble d'éléments formant sa morphologie, d'une autre. Est-ce que ceci voudrait dire que la signature électronique est essentiellement définie par le cyberespace alors que la signature manuscrite ne subit aucunement les effets des propriétés de son environnement?

[397] Il est vrai que le droit s'intéresse peu à l'architecture du monde réel en tant qu'environnement de la signature manuscrite. Cependant, ceci ne veut pas dire que le seing manuel n'est pas dépendant de cette architecture au même degré que l'est la signature électronique de l'architecture du cyberespace. Au contraire, la signature manuscrite est aussi indissociablement liée à son milieu– le mode réel que l'est la signature électronique au cyberespace. Par ailleurs, l'attitude du droit envers la signature manuscrite est tout autant conditionnée par son environnement.

[398] La différence entre les deux réalités pour le droit ne consiste pas dans les rôles respectifs que jouent les environnements réel et virtuel pour la signature manuscrite et les procédés électroniques. La distinction se manifeste sur un autre plan, qui est, selon nous, le degré de maîtrise de ces deux environnements. Si le contrôle du monde réel a été le résultat d'un long processus pour devenir un acquis au sens d'un ensemble de connaissances, d'expériences et de possibilités, tel n'est pas le cas de la maîtrise du cyberespace. Les aptitudes de la société dans le cyberespace ne font que leurs premiers pas. Il est tout de même facile de dépister des mouvements de l'inconnu vers le connu, de l'impossible vers le possible, de l'hasardeux vers la sécuritaire, tous ces mouvements représentant des étapes

[354] D. SYX, *loc. cit.* note 35, 137

du trajet allant de l'absence de contrôle vers la maîtrise. Si aujourd'hui nous avons besoin de signatures électroniques fiables, cette exigence ne serait-elle superflue dans l'éventualité d'un cyberespace globalement empreint de fiabilité? Ce n'est qu'une question parmi le grand nombre de questions qui surgissent dans tous les domaines du droit à l'aube d'un cyberespace de sécurité et de contrôle.

Bibliographie

LÉGISLATION :

Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation, J.O. Numéro 132 du 8 Juin 2002

Code civil belge

Code civil du Québec, source http://www.canlii.org/qc/loi/ccq/tout.html

Code civil français

Code de procédure civile belge

Code de procédure civile du Québec, source http://www.canlii.org/qc/loi/c25/tout.html

Code de procédure civile français

Décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, J.O. Numéro 77 du 31 Mars 2001, page 5070

Décret no 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information , J.O. Numéro 92 du 19 Avril 2002, page 6944

Directive 1999/93/ce du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, L13/12, JOCE, 19 janvier 2000

Federal Rules of Evidence

Loi concernant le cadre juridique des technologies de l'information, L.Q. 2001, c.32

Loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, Moniteur belge, 9 Juillet 2001

Loi introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, Moniteur belge, 20 Octobre 2000

Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, J.O. Numéro 62 du 14 Mars 2000, page 3968

Uniform Commercial Code, Projet proposé le 1er février 1999, source : http://www.law.upenn.edu/bll/ulc/ulc.htm, visité en mai 2002

Uniform Computer Information Transactions Act, Approuvé et recommandé à l'adoption par la Conférence Nationale des commissaires du droit étatique uniforme, Conférence Annuelle Denver, Colorado, Juillet 1999

Uniform Electronic Transaction Act, Approuvé et recommandé à l'adoption par la Conférence Nationale des commissaires du droit étatique uniforme, Conférence Annuelle Denver, Colorado, Juillet 1999

DOCUMENTS OFFICIELS

Avant-projet de convention sur les contrats électroniques, Commission des Nations Unies pour le droit commercial international, A/CN.9/WG.IV/WP.95, Trente-neuvième session New York, 11-15 mars 2002

Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social et au Comité des régions - Sécurité des réseaux et de l'information: Proposition pour une approche politique européenne Journal officiel n° C 048 du 21/02/2002 p. 0033 - 0041

Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation 1996

Loi type sur les signatures électroniques, adopté par la Commission des Nations Unies pour le droit commercial international le 5 juillet 2001

Projet de loi type sur certains aspects juridiques de l'échange de données informatisées (EDI) et des moyens connexes de communication des données, Commission des Nations Unies pour le droit commercial international, A/CN.9/409/ADD.1 27 février 1995

JURIDPURDENCE:

Armand v. Checotel Finance Corp., [1985] Q.J. No. 40

Bolduc c. Talbot, QCCQ, 25 octobre 2001, Source : http://www.canlii.org/qc/jug/qccq/2001/2001qccq1827.html

Cass. fr. (com.), 2 déc. 1997

Cass., 7 janv. 1955, Pas., 1955, I

Central Pontiac Buick Ltée c. Poirier, [1997] A.Q. no 709

Chalets Boisson S.A.R.L. c. Gros, Appel Besançon (Ch. sociale), 20 octobre 2000

Daubert v. Merrell Dow Pharmaceutical Inc., 113 C. St. 2786, p. 2797 (1993)

Digital Equipment Corporation v. Alta Vista Technology Inc., 960 F. Supp. 456 (1997)

Frye c. U.S, 293 F. 1013 (D.C. Cir. 1923)

Hassentaler v. Farzin, 388 Pa. Super. 37, 564 A. 2d 990 (1989)

Interstate United Corp. v. White, 388 F. 2d 5 (10th Cir 1967)

Joseph Denunzio Fruit Co. v. Crane, 79 F. Supp. 117 (S.D. Cal. 1948)

Kahn c. Toronto Dominion Bank, [1997] A.Q. no 61

Kumho Tire Co. v. Caramichael, 526 U.S. 137 (1999)

La Reine c. Mohan, (1994) 2 R.C.S., 9

Olmstead v. United States, 277 U.S. 438 (1928) (USSC+)

Parma Tile Mosaic & marble Co. v. Estate of Short, 590 N.Y.S. 2d 1019 (Sup. Ct. 1992)

Perma Research and Development v. Singer Co., (2nd Cir) 542 F2d 111, 121 (1976)

Reno v. ACLU, 521 U.S. 844 (1997)

State v. Bond, 12 Idaho 424, 86 P. 43 (1906)

State v. Estill, 13 Kan App 2d 111, 764 p2d 455 (1988).

U.S. v. Thomas, 74 F. 3d. 701 (6th cir. 1996)

United States v. Liebert (ED Pa) 383 F Supp 1060 (1974)

Yaggy v. B.V.D. Co., 173 S.E. 2d 496 (N.C. Ct. App. 1970)

LIVRES:

ANDERSON R., Security Engineering, A Comprehensive Guide to Building dependable Distributed Systems, John Wiley and Sons, 2001

BENSOUSSAN A., Internet, aspects juridiques, Ed. Hermes, Paris, 1996

BIEGEL S., Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace, Cambridge, MIT Press, 2001

BRIN D., The Transparent Society : Will Technology Force Us to Choose Between Privacy and Freedom, Cambridge, Mass., Perseus Books, 1998

BUQUET A., La signature du sceau à la clé numérique, histoire, expertise, interprétation, Paris, Édition Service Gutenberg XXIème siècle, 2000

BUQUET, A., Les documents contestes et leur expertise, Editions Yvon Blais Inc., Cowansville, Quebec, Canada, 1997

COLLMANN D., Computer Security, John Wiley and Sons, 1999

DAVID R., D. PUGSLEY, Les contrats en droit anglais, L.G.D.J., 2 ed., Paris, 1985

DENNING D., Cryptography and Data Security, Addison-Wesley, 1982

DENNING D., Information Warfare and Security, Addison-Wesley, 1999

Dr. PERIOT M., BROSSON P., Morpho-physiologie de l'ecriture, Paris, Payot, 1957

ENGEL P., Traite des obligations en droit suisse, Ed Ides et Calendes, Neuchatel, 1973

FAUSSE A.-F., La signature électronique, Paris, Dunod, 2001

FRAENKEL B., La signatrure, genese d'un signe, Paris, NRF, Gallimard, 1992

GUIGUE M.C., De l'origine de la signature et de son emploi au Moyen-Age, Paris, Dumoulin, 1873

HARRISON W., Suspect documents, their scientific examination, Londres, Sweet and Maxwell limited, 1958

KATSH E., The electronic Media and the Transformation of Law, New York/Oxford, Oxford University Press, 1989

LAMÈTHE D., La signature dans les actes sous seing privé, Th. Paris II, 1975

LESSIG L., Code and Other Laws of Cyberspace, New York, Basic Books, 1999

LESSIG L., The Future of Ideas: The Fate of the Commons in a Connected World, New York, Random House, Incorporated, 2001

LILLY G. C., An Introduction to the Law of Evidence, 3ème Édition, St Paul, West Group, 1996

MAJDANSKI D., La signature et les mentions manuscrites dans les contrats, Bordeaux, 2000

NEUMANN P., Computer-Related Risks, Addison-Wesley, 1995

PARISIEN S., P. TRUDEL, L'identification et la certification dans le commerce électronique, Cowansville, Yvon Blais, 1996

RUVIN A., D. GEER, M. RANUM, Web Security Sourcebook, John Wiley and Sons, 1997

SCHNEIER B., Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2 ed. New York, Wiley, 1996

SCHNEIER B., Secrets and Lies: Digital Security in a Networked World, NY, John Wiley & Sons, 2000

TRUDEL P., F. ABRAN, K. BENYEKHLEF, S. HEIN, Droit du cyberespace, Montréal, Thémis, 1997

TRUDEL P., G. LEFEBVRE, S. PARISIEN, La preuve et la signature dans l'échange de documents informatisés au Québec, Québec, Publications du Québec, 1993

WÉRY E., T. VERBIEST, Le droit de l'Internet et de la société de l'information: droits européen, belge et français, Bruxelles, Larcier, 2001

WHITTEN J. L., L. D. BENTLEY, K. C. DITTMAN, System Analysis and Design Methods, 5ème Édition, Boston, McGraw-Hill, 2001

WRIGHT B., The Law of Electronic Commerce, EDI, Fax, and E-mail: Technology, Proof, and Liability, Boston, Little, Brown & Co., 1991

YOURDON E., Modern Structured Analysis, NJ, Englewood Cliffs, 1989

YOURDON E., Modern Structured Analysis, NJ, Englewood Cliffs, 1989

ARTICLES:

ANTOINE M., M. ELOY, J.-F. BRAKELAND, « Droit de la preuve face aux nouvelles technologies de l'information », *CRID*, Namur, 1992

BARLOW J. P., « A Declaration of the Independence of Cyberspace », *Electronic Frontier Foundation*, source http://www.eff.org/~barlow/Declaration-Final.html, visité en mai 2002

BHANSALI B.B., « Man-In-the-Middle Attack - A Brief », *System Administration, Networking, and Security Institute, Reading Room*, 16 février 2001, source: http://rr.sans.org/threats/middle.php, visité en mai 2002

BOSS A. H., « Searching for Security in the Law of Electronic Commerce » 588 *Practising Law Institute*, 1999

BOSS A. H., « The Uniform Electronic Transactions Act in a Global Environment», 37 *Idaho Law Review* 2001

BRUN B., « Nature et impact juridique de la certification dans le commerce électronique sur Internet », *Lex Electronica*, 2000, source : http://www.lex-electronica.org/articles/v7-1/Brun.pdf, visité en mai 2002

CAPRIOLLI, É. A., Preuve et signature dans le commerce électronique*, Droit et patrimoine* 1997, n. 55

COOL Y., « Signature électronique et signature manuscrite : sœurs ennemies ou sœurs jumelles? », *CRID, Droit des technologies de l'information*, Namur 1999

COVIELLO A., « Identity Management: An Important Enabler of E-Government », *Conférence Managing Identity and Authentication on the Internet*, le 11 mars 2002, source: http://www.csis.org/tech/events/020311event/coviello/index.htm, visité en mai 2002

CROZE H., Informatique, preuve et securite, D. 1987. chr.

DAVIO É., « Questions de certification, signature et cryptographie », *CRID, Internet face au droit*, Namur, 1997

DAVIS G. B., « Knowing the Knowledge Workers: A Look at the People Who Work with Knowledge and the Technology That Will Make Them Better », *ICP Software Review*, 1982

DUNBERRY É., «L'archivage des documents électroniques», dans Vincent GAUTRAIS (dir.), Droit du commerce électronique, Montréal, Éditions Thémis, 2002, 124

EUBANKS G., « Identity Management: A Key Element of Critical Infrastructure Assurance », *Conférence Managing Identity and Authentication on the Internet*, le 11 mars 2002, source: http://www.csis.org/tech/events/020311event/eubanks/index.htm, visité en mai 2002

FENWICK W., DAVIDSON G., « Admissibility of Computerized Business Records », 14 *Am. Jur. Proof of Facts* 2d 173, 2000

FISHER D, « Gates : Security over Features », *eWeek, News and Analysis*, 21 Janvier 2002, source : http://www.eweek.com/article/0,3658,s=701&a=21528,00.asp, visité en mai 2002

FONTAINE M., La preuve des actes juridiques et les technologies nouvelles, dans *La Preuve*, Colloque, U.C.L.,, 1987

FULLER L., Consideration and Form, 1941 41 *Columbia Law Review* 799

GARRETSON G., « Industry examines government role in digital Ids », *InfoWorld*, le 11 Mars 2002, source: http://ww1.infoworld.com/cgi-bin/fixup.pl?story=http://www.infoworld.com/articles/hn/xml/02/03/11/020311hndigitalid.xml&dctag=onlinecommunities, visité en mai 2002

GATES B., « Why we're Building .NET Technology », 18 juin 2001, source: http://www.microsoft.com/presspass/misc/06-18BillGNet.asp, visité en mai 2002

GAUTRAIS V., « Les aspects relatifs à la sécurité » , *Juris International, Commerce Électronique, Guide juridique du commerçant électronique*, source : http://www.jurisint.org/pub/05/fr/index.htm, visité en mai 2002

GAUTRAIS V., «Le contrat électronique au regard de la Loi concernant le cadre juridique des technologies de l'information», dans Vincent GAUTRAIS (dir.), Droit du commerce électronique, Montréal, Éditions Thémis, 2002

GEYER A., « MEDePASS Healthcare Checklist », *ANSI*, source: http://www.ansi.org/rooms/room_41/public/ppt/hisb184.ppt

GLISSEN J., « Le preuve en Europe (XVI – XIXe siècles) », *Recueils de la Société Jean Bodin*

GOBERT D., É. MONTERO, « La signature dans les contrats et les paiements électroniques: l'approche fonctionnelle », *CRID, Commerce électronique*, Namur 2000

HOWARD G., « Ethernet », *Yale University, PC Lube and Tune*, source http://www.yale.edu/pclt/COMM/ETHER.HTM, visité en mai 2002

ITEANU O., Internet et le droit, Ed. Eyrolles, Paris, 1996

JACCARD M., « Problèmes juridiques liés à la sécurité des transactions sur le réseau », *Signelec.com, Signature électronique et droit de la preuve*, 2000, source : http://www.signelec.com/content/se/articles/article_michel_jaccard_html , visité en mai 2002

JOHNSON D. R., D. G. POST, « Law and Borders: The rise of Law in Cyberspace », *Stanford Law Review* 48, (1996), 1403, 1407

KENNEDY J. B., M. WONG, «Recent Developments in U.S. Privacy Law», *Practising Law Institute, Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series,* PLI Order No. G0-00ZQ novembre, 2001

LAMETHE, D., Reflexions sur la signature, GP 1976, I

LARRIEU J., Les nouveaux moyens de de preuve : pour ou contre l'identification des documents informatiques a des ecrits sous seing prive? *Cahiers Lamy*, nov. 1988, (H), p.8, et dec. 1988 (I)

LECLERCQ P., Faut-il reformer le droit de la preuve?, *Droit de l'informatique et des télécommunications*, 1991, 1, p.5

LESSIG L., « Surveying Law and Borders: the Zones of Cyberspace », *Stanford Law Review* 48 (1996), 1367

LESSIG L., « Reading the Constitution in Cyberspace », *Emory Law Journal*, 45 (1996)

MAHER M., « An Analysis of Internet Standardization », 3 *Va. J.L. & Tech*. 5, Spring 1998 source: http://scs.student.virginia.edu/~vjolt/graphics/vol3/home_art5.html visité en mai 2002

MASSE D.G., « L'autoroute de l'information : convergence du droit et de la technologie », *Colloque Faire des affaires en toute sécurité sur les autoroutes de l'information*, 10 novembre 1995

MCCARTHY M., « Security Woe: Computer-Screen Spies », *ZDNET, ZDNET Technology News*, 6 Août 2000, source: http://zdnet.com.com/2100-11-502732.html?legacy=zdnn, visité en mai 2002

MORRIS C., C. FERGUSON, How Architecture Wins Technology Wars, *Harvard Business Law Review*, March-April, 1993, 86

MUNDIE K., «Keynote Address», *Conférence Managing Identity and Authentication on the Internet*, le 11 mars 2002, source: http://www.csis.org/tech/events/020311event/Mundie/index.htm, visité en mai 2002

PATENAUDE P., « De l'expertise judiciaire dans le cadre du procès criminel et de la recherche de la vérité : quelques réflexions », *Revue de Droit*, Université de Sherbrooke, (1) 1997

REED C., « What is a Signature? », *The Journal of Information, Law and Technology* (3), 2000

SCHNEIER B, , «Cyber UL ?», *Counterpane Internet Security, Crypto-gram Newsletter*, 15 janvier 2001, source: http://www.counterpane.com/crypto-gram-0101.html, visité en mai 2001

SCHNEIER B., « Security » , *Counterpane Internet Security, Crypto-gram Newsletter*, 15 mars 2001, source: http://www.counterpane.com/crypto-gram-0103.html , visité en mai 2002

SCHNEIER B., «The Blowfish Encryption Algorithm», *Counterpane Internet Security, Counterpane Labs*, 2002 , source: http://www.counterpane.com/blowfish.html, visité en mai 2002

SYX D., « Vers de nouvelles formes de signature? », (1986) 3 *Droit de l'informatique*, 133, 135

The Economist, « Mach 1 at Microsoft », *The Economist Technology Quarterly*, 33 – 34, 16 Mars 2002

TUERKHEIMER F., « The Daubert Case and Its Aftermath : A Shot-gun wedding of Technology and Law in the Supreme Court», 51 *Syracuse Law Review* 2001

VAN QUICKENBORNE M., « Quelques réflexions sur la signature des actes sous seing privé », *R.C.J.B*., 1985

VICTOR L., MULHERN J., « Sending E-mail: Selecting & Configuring Your SMTP Server », *University of Pennsylvania, University of Pennsylvania Computer Center*, source : http://www.upenn.edu/computing/help/doc/email/smtp.html, visité en mai 2002

VOLOKH E., « Technology and the Future of Law », *Stanford Law Review*, 47 (1995), 1375

WÉRY E., « Microsoft « Passport » et « .net », la FTC transige, mais l'Europe poursuit l'enquête», *Droit des nouvelles technologies, Actualités*, le 3 septembre 2002

WÉRY E., « Surfer anonymement devient illégal en Belgique », *Droit des nouvelles technologies, Actualités*, le 18 Mars 2002

WINN J. K., « Open Systems, Free Markets, and Regulation of Internet Commerce », *Tulane Law Review* 72 (1998), 1177

ZACHMAN J. A., « A Framework for Information System Architecture », *IBM Systems Journal* 26, No. 3, (1987)

RESSOURCES INTERNET:

About.com, Learn the Net Glossary, source: http://www.learnthenet.com

Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de

Common Criteria for Information Technology Security Evaluation, http://www.commoncriteria.org

Conseil stratégique des technologies de l'information, http://www.csti.pm.gouv.fr/home_fr.htm

Des informations sont disponibles sur http://www.cenorm.be/aboutcen/aboutcen.htm, visité en mai 2002

Marx Software Security, News, source: http://www.marx.com

Microsoft, http://www.microsoft.com

Ministère de la culture et des communications, Autoroute de l'information, Loi concernant le cadre juridique des technologies de l'information (L.Q.2001, c.32), Texte annoté par article, source : http://www.autoroute.gouv.qc.ca/loi_en_ligne/loi/annindex.html, visité en mai 2002

Passeport .NET, http://passport.com/Consumer/default.asp?lc=3084

RSA Security, http://www.rsasecurity.com

Service central de la sécurité des systèmes d'informations, http://www.scssi.gouv.fr

The American National Standards Institute, http://www.ansi.org

The Center for Strategic and International Studies, http://www.csis.org

The International Telecommunication Union, http://www.itu.int

The Internet Architecture Board, http://www.iab.org

The Internet Engineering Steering Group, http://iesg.org

The Internet Engineering Task Force, http://ietf.org

The Internet Research Task Force, http://irtf.org/

The Internet Society, http://www.isoc.org

The National Computer Security Center, http://csrc.nist.gov

The National Institute of Standards and Technology, http://www.nist.gov

The World Wide Web Consortium, http://www.w3.org

U.S. Department of Defense Trusted Computer System evaluation Criteria, http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

US Government Export Portal, Market Access and Compliance, http://www.mac.doc.gov