LA PREUVE DU CONTRAT CONCLU PAR VOIE ÉLECTRONIQUE – CLAP 2ème *

PLAN

§ 5. Reproduction de la clause de non discrimination

CHAPITRE IV. EN GUISE DE CONCLUSION : LA DIRECTIVE SUR LE COMMERCE ÉLECTRONIQUE APPELLE UNE NOUVELLE RÉVISION DU DROIT DE LA PREUVE

Section 1. La directive sur le commerce électronique : aperçu

Section 2. La directive sur le commerce électronique et le concept d'écrit

Section 3. La directive sur le commerce électronique et les autres exigences d'ordre formel, en particulier les articles 1325 et 1326 du Code civil

INTRODUCTION

1. L'Internet, le " réseau des réseaux " , est probablement au regard de la problématique de la preuve des actes juridiques, et plus spécifiquement des contrats, " la goutte d'eau qui a fait déborder le vase ". Les questions techniques et juridiques posées par les ancêtres de la télématique (soit la combinaison des technologies de l'informatique et des télécommunications) n'étaient guère différentes - toute proportion des progrès électroniques gardée - des interrogations actuelles mais étaient le plus souvent annihilées par l'existence de conventions dérogatoires sur la preuve , possibles en réseaux fermés. C'est, en effet, la spécificité de réseau mondialement ouvert d'Internet qui cristallise le sentiment d'insécurité des relations contractuelles y nouées. Par ailleurs, l'attrait, parfois quasi-mystique, de la toile mondiale ne peut qu'être constaté, ce dont attestent d'abondantes métaphores. On parle ainsi, de façon générale, d'" espace virtuel ", de " dématérialisation du réel ", de " réseau multimédia et interactif " et, plus spécialement sur le plan commercial, de " commerce virtuel ", de " foire commerciale ", " de galeries marchandes virtuelles "… Nous préciserons encore, avec E. MONTERO , qu'il convient de distinguer, parlant de " commerce électronique ", les contrats conclus et exécutés *via* Internet, tel le téléchargement d'un logiciel, des contrats conclus sur réseaux mais exécutés en dehors de ceux-ci qui retiendront principalement notre attention.

2. Face à de tels mouvements de société, le droit se devait de réagir afin d'instaurer le climat de confiance juridique nécessaire au développement du commerce électronique, qu'il s'agisse de contrats conclus par messagerie électronique via les boîtes aux lettres électroniques ou, de façon plus aiguë encore, de contrats conclus directement – ou du moins paraissant l'être - sur tel ou tel site Web. Les incertitudes sont, en effet, multiples : comment s'assurer de l'identité de l' " autre ", ne disposant que d'une adresse e-mail ou du nom d'un site, comment garantir l'intégrité du message adressé ou reçu ou la pérennité de la page du site consultée lors de la " commande ", comment préserver l'éventuelle confidentialité de la communication, …

Dans ces perspectives, le canal utilisé par le droit, au sens large, ne devait pas, *a priori*, être nécessairement législatif, nous en reparlerons ultérieurement . Telle est bien pourtant la direction qu'emprunte le droit belge . Notre législateur, convaincu de la nécessité, prônée par nombre d'auteurs , d'une intervention législative rapide est, il est vrai, soucieux aussi de se conformer aux directives européennes. En effet, déjà, la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur a-t-elle été modifiée par une loi du 25 mai 1999 afin d'intégrer la

directive 97/7/C.E. du Parlement et du Conseil du 20 mai 1997 relative aux contrats à distance . Ainsi, au cœur de notre sujet, la loi du 20 octobre 2000, publiée au Moniteur belge du 22 décembre 2000, introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire et la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, amplement commentées ci-dessous, entendent-elles mettre en œuvre la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques adoptée le 13 décembre 1999. Enfin, et sans être exhaustif, s'agira-t-il encore d'adapter notre législation à la directive 2000/31/CE du 8 juin 2000 "sur le commerce électronique" ainsi qu'en atteste l'avant-projet de loi sur certains aspects juridiques des services de la société de l'information .

3. Pour l'heure, il convient d'appréhender, ensuite d'un bref détour du côté de la technologie (Titre II), le commerce électronique sous l'angle du droit de la preuve, tel que récemment ou prochainement modifié (Titre III), analyse qui nécessite, au préalable, un bref rappel des règles préexistant en matière de preuve mais surtout, et plus fondamentalement, des conséquences tout à fait pratiques de l'application de celles-ci au commerce électronique (Titre I).

TITRE PREMIER. LE CODE CIVIL À L'ÉPREUVE DU COMMERCE ÉLECTRONIQUE

4. Une remarque. Il ne s'agit pas de refaire, dans le cadre de la présente contribution, une description détaillée des grands principes du Code civil en matière de preuve, des modes de preuve décrits par ledit Code, de leur recevabilité ou de leur force probante. Nous renvoyons, à cet égard, le lecteur à de célèbres contributions .

CHAPITRE PREMIER. PRINCIPES ESSENTIELS RÉGISSANT LA PREUVE DES ACTES JURIDIQUES ET COMMERCE ÉLECTRONIQUE

Section 1. *Idem est non esse aut non probari*

5. Faut-il encore rappeler à l'internaute que son droit n'est rien sans la preuve de l'acte – pris ici dans son sens de *negotium* - ou du fait dont il dérive ? Probablement plus qu'à tout autre, parce qu'il évolue, selon l'expression d'Y. POULLET et M. ANTOINE , dans un monde virtuel, caractérisé par l'immatérialité et la fugacité des messages qui s'y échangent, et dont nul n'est immédiatement témoin. Seul - et à la fois partout - devant son clavier, son " bon droit " s'il est contesté ne pourra être reconnu sans la preuve qui, d'une façon ou d'une autre, le concrétise.

6. Pire encore, rappelons-le, l'existence du droit même peut être subordonnée à différents formalismes qui conditionnent la formation même de l'acte juridique. S'agissant de formalités *ad solemnitatem* dites encore *ad validatem* et non plus seulement *ad probationem*, liant indissolublement *negotium* et *instrumentum*, l'absence de ces formes, un écrit le plus souvent , est alors irrémédiable . Si la directive européenne sur un cadre communautaire pour les signatures électroniques, qui nous occupe au premier chef, paraît avoir exclu de son champ d'application les questions de validité des contrats , la question de l'adéquation d'une multitude de formalismes de validité, spécialement dans le domaine du droit de la consommation , se pose avec acuité au regard, cette fois, de la directive sur le commerce électronique .

Section 2. La portée du système de preuve légale

7. On le sait, notre droit civil de la preuve est un système de preuve légale : la loi définit, dans une perspective hiérarchique, les moyens de preuve, leur recevabilité, leur foi et force probante. Nous préciserons d'ailleurs ici, avant tout autre développement, que les termes de recevabilité, force probante ou valeur probante ont récemment

encore fait l'objet de mises au point, voire de critiques, que nous évoquerons brièvement en temps utile . Pour le reste, il existe, principalement, cinq modes de preuve, classés traditionnellement en deux groupes : d'une part, la preuve littérale, l'aveu et le serment litisdécisoire, qualifiés fréquemment de modes de preuve parfaits et, d'autre part, les témoignages et présomptions.

Il importe d'observer que les règles du Code civil relatives à la preuve ont été considérées par la Cour de cassation comme n'étant ni d'ordre public ni impératives .

8. En conséquence, premièrement, le juge ne peut soulever d'office les règles du Code civil relatives spécialement à la charge de la preuve et à l'admissibilité des modes de preuve que les parties n'invoquent point . A ce dernier égard, on précisera que le juge n'est pas cantonné dans un rôle purement passif et qu'il peut et même doit ordonner toutes les mesures d'instruction qui lui paraissent nécessaires ou souhaitables, de même qu'il lui revient de trancher le litige en appliquant le droit objectif. Certes, cette intervention doit toujours s'inscrire dans le respect du principe dispositif, en se fondant sur les seuls faits invoqués par les parties , mais l'on connaît toutes les subtilités, voire difficultés, de conciliation du principe dispositif et de l'office du juge . Faudra-t-il dès lors, pour que le juge applique le droit de la preuve, que les parties invoquent, d'une façon ou d'une autre, des prétentions factuelles d'ordre probatoire et ne placent point immédiatement et exclusivement le litige, par exemple, sur le plan de l'inexécution totale ou partielle du contrat.

9. Deuxièmement, les parties peuvent, en principe, valablement conclure des conventions dérogatoires au système de preuve légale , celles-ci supposant, d'évidence, un contact préalable et suivi entre les différents cocontractants et, dès lors, l'existence d'un réseau dit fermé. Ce principe connaît toutefois des exceptions résultant soit du caractère d'ordre public reconnu à certaines règles , soit de diverses législations spécifiques, telle la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur.

10. A cet égard, et nous permettant ainsi de nuancer les pouvoirs du juge décrits ci-dessus dans un contexte purement supplétif, nous relèverons l'article 32 de la loi sur les pratiques du commerce qui interdit toute une série de clauses abusives dans les contrats conclus entre professionnel et consommateur parmi lesquelles toute stipulation qui limiterait, de façon directe ou indirecte, les moyens de preuve que le consommateur pourrait utiliser . Nous préciserons que la nouvelle version de l'article 33 L.P.C., introduite par la loi du 7 décembre 1998 , uniformise le système de nullité des clauses abusives qu'il s'agisse des clauses visées limitativement par l'article 32 L.P.C. ou des clauses répondant à la définition générale de la clause abusive inscrite à l'article 31 L.P.C.

qui sont désormais, toutes, interdites et nulles. L'on sait, malheureusement, toute l'incertitude qui plane en doctrine quant au caractère de cette nullité et tout le doute qui entoure, spécialement, la possibilité pour le juge de soulever ce moyen d'office . Sans prétendre aucunement trancher cette délicate question, nous rappellerons l'opinion de A. MEEUS qui, dans son étude sur la notion de loi impérative et l'incidence de celle-ci sur la procédure en cassation et sur l'office du juge , considère que même en cas de dispositions simplement impératives, et donc de nullité qualifiée traditionnellement de relative, le juge doit appliquer d'office ces dispositions sauf à vérifier, au préalable, si elles n'ont pas fait l'objet d'une renonciation ultérieure ou d'une confirmation valables . On conviendra, dans cette perspective, de l'importance de la signification à donner au paragraphe 3 de l'article 33 L.P.C., qui énonce que *" le consommateur ne peut renoncer au bénéfice des droits qui lui sont conférés par la présente section "*, signification qui, semble-t-il, continue à diviser les auteurs . Nous signalerons enfin, de façon peut-être plus déterminante, un arrêt de la Cour de justice des C.E. du 27 juin 2000 qui prône un rôle actif du juge tenu d'examiner d'office le caractère abusif d'une clause d'un contrat invoqué devant lui et de choisir, eu égard au principe d'interprétation conforme, à la lumière du texte et des finalités de la directive invoquée, l'interprétation lui permettant de refuser d'office d'assumer une compétence lui attribuée par une clause abusive.

On relèvera, d'un point de vue pratique, les précisions que tentent d'apporter certains sites quant à la validité, comme mode de preuve, des " signatures électroniques " y utilisées. On peut ainsi lire, par exemple, que *" l'utilisateur accepte d'utiliser le code secret et le code d'accès comme preuve de son engagement et que cette dernière équivaut à sa signature. L'utilisateur accepte que l'utilisation du code d'accès et du code secret prouve l'existence, l'intégrité et la provenance de l'avis électronique "* . Si l'on peut considérer ce type de clauses comme des conventions relatives à la preuve permises - même entre professionnel et consommateur dans la mesure où elles pourraient être considérées comme ne limitant point, même de façon indirecte, les moyens de preuve que le consommateur peut utiliser -, faudra-t-il encore, en amont, établir que c'est effectivement la personne contre qui l'on invoque cet accord sur la preuve qui l'a signé et qui y a adhéré.

11. Parlant du commerce électronique, une précision fondamentale s'impose : le système de preuve légale évoqué ne vise, à pur et à plein, que le droit civil. En droit commercial, le régime probatoire, souvent qualifié de régime de liberté des preuves, est en réalité pareillement un système légal de preuve mais considérablement assoupli, en ce que la finale de l'article 1341 du Code civil, confirmé par l'article 25 du Code de commerce, autorise, sauf exceptions, plus largement le recours aux témoignages et présomptions. Ce régime s'applique eu égard à la nature commerciale de l'acte juridique à prouver, quelle que soit la qualité des parties, sauf à souligner l'incidence,

importante en pratique, de la notion d'acte commercial par relation à la personne (art. 2, *in fine* C. com.). Peuvent aussi exister des actes dits mixtes, c'est-à-dire présentant simultanément une double qualité, commerciale dans le chef d'une des parties et civile dans le chef de l'autre, telle, précisément, une vente réalisée entre un commerçant, dans le cadre de sa profession, et un non-commerçant. Dans cette hypothèse, on appliquera respectivement le système légal de preuve de droit civil ou, au contraire, le régime assoupli de droit commercial selon qu'il s'agira de prouver une obligation dans le chef du non-commerçant ou une obligation dans le chef du commerçant . La remarque vaut, d'évidence, tant au regard du commerce traditionnel qu'en ce qui concerne le commerce électronique.

CHAPITRE II. L'" ÉCRIT "ET LE COMMERCE ÉLECTRONIQUE

Section 1. La prééminence de l'" écrit "

12. Hormis l'aveu et le serment décisoire, recevables, en principe, en toutes matières, impliquant la déclaration ou l'affirmation solennelle de la véracité d'un fait (au sens large, par opposition à la règle de droit) et dotés d'une force probante quasi-absolue (art. 1356 et 1363 C. civ.) , notre droit de la preuve place, par rapport aux autres modes de preuve que sont la preuve testimoniale et les présomptions, sur un piédestal la preuve littérale, dans le sens restreint d'acte instrumentaire, par définition préconstituée et rédigée en un temps non suspect.

13. Cette supériorité est consacrée tant au point de vue de la recevabilité de la preuve littérale qu'en ce qui concerne sa force probante.

14. En effet, premièrement, l'article 1341 du Code civil n'admet la recevabilité, entre parties à l'acte, des présomptions et témoignages qu'en ce qui concerne les faits juridiques et les actes juridiques d'une somme ou valeur inférieure ou égale à 375 euros. Par conséquent, pour apporter la preuve d'un acte juridique d'une somme ou valeur supérieure à 375 euros, il faudra, sauf exceptions , produire un écrit (sous seing privé ou authentique). De plus, cette première règle se double d'une seconde interdisant aux parties, même en dessous de 375 euros, de prouver par témoins ou par présomptions outre ou contre le contenu de l'écrit préalablement présenté.

15. Deuxièmement, la loi attribue une force probante – soit la foi due à un acte en tant qu'il est retenu comme preuve par la loi - prédéterminée aux actes écrits signés, actes authentiques ou actes sous seing privé. Concernant essentiellement ces derniers, la disposition légale déterminante est l'article 1322 du Code civil, récemment complété, qui

énonce que *" l'acte sous seing privé, reconnu par celui auquel on l'oppose, ou légalement tenu pour reconnu, a, entre ceux qui l'ont souscrit et entre leurs héritiers et ayants cause, la même foi que l'acte authentique "*, acte authentique qui *" fait pleine foi de la convention qu'il renferme entre les parties contractantes et leurs héritiers et ayants cause "*, au terme de l'article 1319 du Code civil En réalité, l'acte authentique ne fait véritablement pleine foi que des mentions authentiques qu'il contient, spécialement l'origine de l'écriture et des signatures, et ce toujours sous réserve d'une possible contestation, par les parties ou par un tiers, par le biais d'une procédure spéciale d'inscription de faux . Quant aux mentions non couvertes par l'authenticité, elles pourront aussi être contestées, sauf, quant aux parties, à respecter l'article 1341 du Code civil . L'acte sous seing privé, lui, ne jouit pas des foi et force probante immédiates de l'origine de l'écriture et des signatures des parties, puisqu'il ne présente aucun signe d'authenticité. Il ne sera assimilé à l'acte authentique – en ce qui concerne la sincérité des déclarations des parties – que s'il est formellement reconnu ou légalement tenu pour reconnu. En pratique, aucune reconnaissance formelle ou expresse n'est exigée et il suffit que la personne à qui l'on oppose l'acte sous seing privé ne désavoue pas formellement l'écriture ou la signature de l'acte. Dès lors, de deux choses l'une. L'acte sous seing privé est reconnu, le plus souvent suite au silence du signataire. Il peut, au contraire, être formellement désavoué : l'acte sera alors légalement tenu pour reconnu si la procédure en vérification d'écritures (dont le principe est énoncé à l'article 1324 du Code civil et les modalités détaillées aux articles 883 et s. du Code judiciaire) confirme que l'acte émane bien de son signataire .

A la différence de la preuve littérale, les témoignages et présomptions n'ont pas de valeur probante déterminée : il appartient au juge d'en apprécier souverainement la valeur probante et de se forger librement sa propre conviction. On rappellera toutefois que la Cour de cassation exerce un certain contrôle portant sur la méconnaissance, la dénaturation ou la violation des notions légales de témoignages ou de présomptions du fait de l'homme. Ainsi, la Cour contrôle que le juge n'a pas déduit des faits qu'il a constatés des conséquences qui, sur le fondement de ces faits, ne sont susceptibles d'aucune justification ou encore qu'il n'adopte pas une interprétation des déclarations du témoin qui serait inconciliable avec leurs termes mêmes .

Section 2. Les exceptions à l'article 1341 du Code civil

16. Outre les limites mêmes du système décrit à l'article 1341 du Code civil, à savoir, pour ce qui nous concerne, notamment, l'incidence pratique évidente du montant plancher de 375 euros, la prééminence de l'" écrit " connaît des exceptions, générales ou particulières. Si les exceptions générales énoncées dans le Code civil, que nous allons brièvement rappeler, tendent à écorner quelque peu le quasi-monopole de la preuve

littérale, première ou deuxième règle de l'article 1341 du Code civil, en permettant exceptionnellement, le recours aux témoignages et présomptions, les exceptions particulières, disséminées dans le Code civil lui-même ou dans moult lois spécifiques, visent, au contraire, le plus souvent, à renforcer l'exigence de l'écrit – en y ajoutant parfois l'une ou l'autre formalité, telle l'exigence de mentions manuscrites – sans que l'on puisse d'ailleurs toujours déterminer s'il s'agit d'un " super " formalisme probatoire ou bien d'un formalisme de validité, entendons validité du *negotium* .

17. Au nombre des régimes exceptionnels instaurés par le Code civil, nous rappellerons, en premier lieu, la finale de l'article 1341 du Code civil, reproduite dans l'article 25 du Code de commerce, instaurant la liberté des preuves en droit commercial. Nous préciserons nos propos antérieurs en observant que si la preuve testimoniale, de même que, par analogie, la preuve par présomptions, est largement recevable, elle est entièrement subordonnée à l'autorisation du juge, qui jouit à cet égard d'un pouvoir souverain d'appréciation . Et, en pratique, l'on constate une certaine méfiance des juges quant à la possibilité de la preuve par témoins d'un contrat et, plus encore, lorsqu'il s'agit de prouver contre ou outre un écrit. En revanche, l'admission des présomptions semble plus fréquente, eu égard, probablement, au caractère parfois scientifique, et donc moins contestable, de celles-ci . Nous mentionnerons enfin la finale de l'article 25 du Code de commerce qui réserve les exceptions (à l'exception) établies pour des cas particuliers, auxquels cas la preuve de tel acte commercial devra être établie par écrit.

18. Les deux autres exceptions à l'article 1341 du Code civil, permettant dès lors la preuve par toutes voies de droit, sont davantage d'ordre factuel et reposent soit sur l'existence d'un commencement de preuve par écrit (art. 1347 C. civ.), soit sur l'impossibilité de rédiger une preuve littérale ou la perte de celle-ci (art. 1348 C. civ.).

19. Le commencement de preuve par écrit est défini, par le Code lui-même, comme tout écrit émané de celui contre lequel la demande est formée et qui rend vraisemblable le fait allégué. La définition est, en réalité, entendue très largement et vise tout document écrit, même non signé, pour autant qu'il émane effectivement de celui à qui on l'oppose , fût-ce par la voie d'une approbation ou appropriation du document d'un tiers, et conférant au fait allégué une apparence, plus que possible , de réalité.

Deux précisions. D'abord, la seule existence d'un commencement de preuve par écrit ne suffira pas. Il ne s'agit en effet, selon la formule consacrée, que d'un " adminicule " de preuve, qui doit être obligatoirement complété par des témoignages ou présomptions. Ensuite, la question se pose si le système dérogatoire de l'article 1347 du Code civil peut être utilisé lorsqu'une disposition spéciale exige, pour établir tel acte juridique, une preuve littérale préconstituée. Si une réponse négative s'impose lorsqu'il s'agit d'un

formalisme de validité du *negotium* lui-même, la controverse subsiste, en revanche, quand l'écrit signé est requis au titre d'un formalisme probatoire accru , sauf, d'évidence, si le législateur a expressément réglé ce point .

20. L'absence, *ab initio*, ou la perte de l'écrit autorisent pareillement, dès lors que l'une ou l'autre sont établies, le recours exceptionnel à la preuve par témoignages ou par présomptions. Au titre de l'absence, la doctrine et la jurisprudence, s'appuyant sur l'alinéa premier de l'article 1348 du Code civil, qui s'exprime en termes tout à fait généraux - " *toutes les fois où il n'a pas été possible au créancier de se procurer une preuve littérale de l'obligation qui a été contractée envers lui* " -, ont admis non seulement l'impossibilité matérielle, mais aussi l'impossibilité morale ou encore l'impossibilité résultant des usages . Quant à la perte, elle doit être non imputable, d'une quelconque façon, au créancier et celui-ci devra l'établir avant de pouvoir apporter, par toute voie de droit, la preuve de l'obligation qu'il invoque à son profit. Une certaine doctrine précise d'ailleurs que l'exception de l'article 1348 du Code civil vise aussi le cas d'actes juridiques dont l'écrit signé est exigé, à titre de formalisme probatoire accru ou de formalisme de validité du *negotium* .

Section 3. Application au commerce électronique

§ 1er. Position du problème et ersatz de preuve

21. Comment intégrer dans le système décrit ci-dessus les différentes " formes " électroniques utilisées pour contracter – essentiellement, pour notre propos, les courriers e-mail et les conclusions directes sur sites web -, dans quelles catégories de modes de preuve les ranger et, dès lors, quelle recevabilité et quelle force probante leur octroyer, dans quelle mesure le caractère électronique de la conclusion du contrat ouvre-t-il la voie à l'une ou l'autre exceptions précitées …? Telles sont les questions fondamentales - amplement commentées, voire disséquées, par les nombreux auteurs cités en note et bien d'autres encore, et dont nous ne ferons donc qu'une rapide synthèse - qui devaient ou doivent encore recevoir des réponses sinon certaines, du moins solides, si l'on veut assurer au commerce électronique une certaine prospérité.

22. On aura remarqué que, décrivant la recevabilité et la force probante de l'" écrit " nous avons, non contents de l'affubler de guillemets, sciemment omis de donner une quelconque définition ou même description de celui-ci. C'est que c'est là que réside l'enjeu du débat. En effet, qu'il s'agisse d'affirmer, avec l'ensemble de la doctrine , que tel " document " électronique est certainement une présomption, à l'instar de ce que la Cour de cassation énonça à propos d'un enregistrement magnétique , il faudra encore

affronter l'obstacle de la recevabilité et, ensuite, emporter la conviction du juge quant à sa valeur probante . Déciderions-nous, avec certains , que tel e-mail ou tel site web constitue un écrit au sens large , qui, s'il émane de la personne à qui on l'oppose et rend vraisemblable le fait allégué, pourra valoir comme commencement de preuve par écrit ou affirmerions-nous (avec quelle certitude ?) l'existence d'un usage dans le monde virtuel engendrant l'impossibilité de se réserver un écrit , ces positions, même consacrées légalement , ne permettront jamais que d'ouvrir la voie aux témoignages et présomptions. On le voit, toutes ces hypothèses ne constituent finalement que des pis-aller, vu la supériorité dans notre droit privé de l'acte instrumentaire.

§ 2. L'écrit instrumentaire traditionnel

23. La loi ne donne aucune définition de la preuve littérale et utilise d'ailleurs indistinctement les termes acte, titre, écrit. L'acception la plus large des termes " preuve littérale " vise la preuve par écrit, étant entendu qu'il existe des écrits signés et des écrits non signés, des écrits orignaux et des copies, des écrits non signés constituant ou non des commencements de preuve par écrit, des écrits signés qui constituent des actes instrumentaires et d'autres non, des écrits instrumentaires primordiaux et des écrits instrumentaires récognitifs ou confirmatifs, … , pléthore de concepts et de réalités distinctes qui sème le parcours de tout qui tente d'écrire sur le thème de la preuve d'innombrables et incessantes embûches. Le sort réellement favorable qui est réservé au plan probatoire à la preuve littérale ne concerne pourtant, nous l'avons vu, que certaines formes de celle-ci : l'acte authentique et l'acte sous seing privé, reconnu ou légalement tenu pour reconnu.

24. On nous permettra de délaisser présentement l'acte authentique pour les raisons suivantes. Premièrement, l'article 1322 du Code civil récemment modifié ne vise que l'acte sous seing privé . Deuxièmement, la directive sur un cadre communautaire pour les signatures électroniques ne demande point de supprimer toutes les exigences formelles relatives à la conclusion des contrats et, à cet égard, l'acte authentique suscite quelqu'interrogation . Troisièmement, parce que même la directive 2000/31/CE du 8 juin 2000 "sur le commerce électronique" , qui recommande en son article 9, paragraphe premier, aux États de veiller à ce que leur système juridique rende possible la conclusion des contrats par voie électronique permet aux États membres de ne pas appliquer le paragraphe premier de l'article 9 précité, notamment, aux contrats qui créent ou transfèrent des droits sur des biens immobiliers, à l'exception des droits de location (art. 9, § 2, a) et, plus fondamentalement encore, aux contrats pour lesquels la loi requiert l'intervention des tribunaux, des autorités publiques ou de professions exerçant une autorité publique (art. 9, § 2, b). Nous relèverons simplement que, dans son article 31,

l'avant-projet de loi appelé à transposer la directive sur le commerce électronique précise que l'acte authentique « *peut être dressé sur tout support s'il est établi et conservé dans des conditions fixées par le Roi, par arrêté délibéré en Conseil des ministres* ».

Quant à l'acte sous seing privé, nous dirons que la doctrine le définit comme l'écrit établi sans l'intervention d'un officier public agissant en cette qualité, par de simples particuliers et signé par eux . Écrit et signature sont donc les deux exigences générales minimales de l'acte sous seing privé mais, derechef, la loi ne définit ni l'un ni l'autre. Cependant, l'écrit était généralement conçu comme la représentation lisible du langage ou de la pensée au moyen de graphismes, tandis que, suite à une longue controverse, notre Cour de cassation aboutit à définir la signature – dans le cadre des testaments olographes certes mais la position peut être généralisée - de façon formaliste comme *" la marque manuscrite par laquelle le testateur révèle habituellement sa personnalité aux tiers "* . En outre, puisqu'il s'agit de pouvoir distinguer l'original de la copie dont les sorts probatoires diffèrent , notre haute Cour a précisé que *" la signature d'un acte sous seing privé doit, en règle, être tracée directement sur le document lui-même "* .

§ 3. Evolution de l'acte sous seing privé (écrit signé)

25. Les contours ainsi délimités – et limités – de l'écrit et de la signature résultent à l'évidence, et de façon inconsciente, d'une conception " papier " de l'acte instrumentaire. Comme le relève D. MOUGENOT, s'interrogeant sur la nécessité d'insérer une définition de l'écrit dans le Code civil , la nécessité de revoir la définition traditionnelle de l'écrit n'est évidemment pas neuve. Il y a quinze ans déjà, en France comme en Belgique, étaient suggérées de nouvelles formulations, tentant d'élargir les termes de lisibilité et de graphismes et, partant, d'intégrer l'écrit électronique , telles *" l'expression de la parole ou de la pensée par des signes "* ou encore *" l'expression du langage sous la forme de signes apposés sur un support. "* . Le législateur français a d'ailleurs consacré cette vision moderne de l'écrit dans le nouvel article 1316 du Code civil qui dispose : *" La preuve littérale, ou la preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles, dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission "* .

26. Pareille évolution doctrinale de la conception de l'écrit, tendant à faire du support un élément essentiellement contingent et à admettre la lisibilité par l'intermédiaire de dispositifs de lecture divers, confortèrent plus d'un à privilégier, aux fins d'assurer un avenir à l'acte sous seing privé électronique, ce que l'on nomme, traditionnellement déjà, la voie interprétative fonctionnelle. Celle-ci consistait, et consiste toujours, à déterminer avec précision les fonctions essentielles de l'écrit, afin d'analyser la mesure

dans laquelle l'écrit sous forme électronique pouvait être assimilé à l'écrit papier, doté subitement de tant de vertus. La même démarche était, dans la foulée, suggérée à l'égard, non plus de l'écrit, mais de la signature elle-même mais surgissait alors l'obstacle de la définition formaliste de celle-ci, intégrant l'exigence de son caractère *manuscrit*, prônée par notre Cour de cassation. Dès lors, la doctrine, constatant la faible quantité de décisions jurisprudentielles rendues sur ce sujet et consciente, en outre, de la nécessité, à court terme, d'un revirement de jurisprudence, s'inscrivit – du moins relativement au concept de signature - dans une perspective d'intervention législative qui consacrerait la vision fonctionnelle que nous allons brièvement rappeler.

27. Encore que les termes utilisés divergent quelque peu, on affuble généralement l'écrit de trois qualités fonctionnelles : il doit être lisible (ou encore intelligible), stable (ou encore permanent, durable) et inaltérable (ou encore irréversible ou intégral) . Derrière les mots se cachent les idées fondamentales suivantes : le document électronique doit pouvoir être lu et compris (fût-ce de façon médiate et au terme d'un décryptage) ; il doit pouvoir être fixé et conservé dans le temps; il doit enfin ne pas être susceptible de modifications, même involontaires. Si ces fonctions sont remplies presque naturellement par l'écrit papier, parce que fondamentalement le contenu de l'acte se confond avec son support – encore que l'on puisse discuter à l'infini sur le caractère compréhensif d'une écriture, la résistance du matériau papier ou encore la possibilité de modifier pareil écrit eu égard, notamment, au récent arrêt de la Cour de cassation française qui (ré)affirme qu'" *aucun principe ni aucun texte ne prohibe l'usage du crayon dans la rédaction d'un acte sous seing privé* " -, en revanche, les exigences, spécialement, de stabilité et d'inaltérabilité, ne seront remplies par le document informatique que si son créateur a pris, pour ce faire, les précautions nécessaires, tant au regard de l'obsolescence fulgurante des procédés technologiques usités qu'au niveau de l'irréversibilité immédiate et future du message, et encore concernent-elles davantage peut-être le support que l'écrit lui-même.

28. Quant à la signature, elle doit permettre, au moins , l'identification de l'auteur de l'acte – traditionnellement, l'attestation de la présence physique du scripteur - et l'adhésion - extériorisation d'une volonté interne - au contenu de celui-ci , double fonction parfois désignée par le vocable unique d'imputabilité. Telles sont les missions que devront aussi remplir nombre de techniques diverses, appelées, de façon générale " signatures électroniques " . Mais, plus fondamentalement, il est une autre fonction qui, dans le domaine virtuel, glisse du concept d'écrit à celui de signature, voire à celui d'acte sous seing privé, c'est celle d'intégrité . En effet, toutes ces interrogations plus ou moins récentes sur les contours minimaux de l'écrit semblent démontrer que c'est en réalité le support papier, parce qu'il rend facilement décelable toute tentative de falsification, qui assure l'irréversibilité du contenu du contrat. Le document électronique

lui n'est pas toujours matériellement délimité et, le plus souvent, c'est sa transformation par l'application de la signature qui en assure l'intangibilité . Cette constatation n'est évidemment pas sans incidence lorsque l'on s'interroge sur la nécessité de définir, dans la loi, l'écrit, les éléments à y inclure, l'endroit, dans l'arsenal législatif, où devrait être insérée cette définition, voire le moment d'y procéder, surtout lorsque l'on se rappelle que nombre de textes particuliers, souvent au titre d'un formalisme *ad validatem*, exigent un " écrit ", même si le législateur, peut-être dans sa grande sagesse, n'a pas expressément précisé " écrit papier " .

29. Voici le tableau dressé. Comment, dans ce contexte probatoire, le législateur belge a-t-il appréhendé ou compte-t-il appréhender le document électronique ? A-t-il intégré d'une façon ou d'une autre l'analyse fonctionnelle décrite ? Quelles sont, à cet égard, les instructions que lui a données le législateur européen et sont-elles ou seront-elles satisfaites dans un futur proche ? Il nous paraît qu'avant même d'aborder toutes ces questions, un bref, et peut-être approximatif, détour par la technologie s'impose, comme nous l'avions d'ailleurs annoncé.

TITRE II. UN COUP D'OEIL DU CÔTÉ DE LA TECHNIQUE : LES DIFFÉRENTS TYPES DE "SIGNATURES ÉLECTRONIQUES"

CHAPITRE PREMIER. PANORAMA DES PROCÉDÉS

30. Identification, manifestation du consentement, voire maintien de l'intégrité, telles sont, nous l'avons vu, les fonctions essentielles que doit pouvoir assurer, dans l'environnement électronique, le procédé qui prétendrait au statut de signature, au sens juridique du terme. Divers candidats entrent en lice. Evoquons les très brièvement avant de décrire plus amplement leur champion, soit la signature à cryptographie asymétrique.

31. Parmi ces procédés, le seul auquel le grand public soit déjà accoutumé est celui qui résulte de *l'utilisation combinée d'une carte et d'un code secret*. Si cette manipulation n'est généralement pas perçue comme une signature mais davantage comme une procédure d'accès à un réseau informatique, il reste qu'elle permet d'identifier dans une certaine mesure son auteur et, dans certaines circonstances, pourrait induire son consentement à l'opération en cours.

Certes, comme le relève notamment D. MOUGENOT , ces deux fonctions ne sont pas remplies de manière optimale. Ce succédané de signature nous paraît cependant suffisamment fiable pour une utilisation dans des réseaux fermés, non seulement, comme c'est le cas actuellement, pour opérer des retraits de fonds à des guichets automatiques ou des payements dans des terminaux-points de vente mais également dans des transactions via le *net* pour autant, alors, que la carte et le code aient été transmis préalablement par une voie traditionnelle (contact physique ou courrier postal) et que l'utilisateur possède un ordinateur équipé d'un lecteur de carte. En revanche, et contrairement à la signature numérique, le procédé semble impraticable en réseau véritablement ouvert .

32. Dans une perspective nettement plus prospective, il convient de citer les *procédés biométriques* . Ceux-ci permettent d'identifier un individu par les caractéristiques physiques uniques qu'il présente. Il peut s'agir du procédé classique de la dactyloscopie mais également de la rétinoscopie (examen des vaisseaux sanguins de la rétine de l'œil), de la manogéométrie (configuration de la main) ou de la reconnaissance vocale. Ces données peuvent, sans trop de difficultés, être numérisées et dès lors transmises et conservées par voie informatique.

Comme l'auront relevé les amateurs de polars, les procédés biométriques peuvent recevoir une foule d'applications qui ont en commun la nécessité d'identifier un individu.

Par ailleurs, si ces procédés paraissent *a priori* étrangers à l'expression du consentement à un acte juridique, il n'est en effet pas exclu qu'ils aient une telle portée, en fonction du contexte dans lequel a lieu l'identification. Il a, dès lors, été suggéré d'y recourir également à titre de signature. Néanmoins, force est d'admettre que la mise en œuvre de tels procédés suppose une infrastructure lourde et coûteuse.

33. Il est un procédé biométrique qui, en ce qui concerne notre sujet, tient une place à part : il s'agit de la *reconnaissance dynamique de la signature*. Dans ce procédé, "le scripteur signe avec un stylo spécial qui enregistre les mouvements de la main, leur vitesse, la pression exercée... et les compare avec des données en mémoire" .

Le signataire reproduisant le geste qu'il est habitué à réaliser dans l'environnement papier pour adhérer au contenu d'un document, la seconde fonction de la signature est ici assurée sans ambiguïté. En revanche, le procédé présente, par rapport aux autres procédés biométriques, une fiabilité moindre en ce qui concerne l'identification du scripteur. L'on sait notamment que la signature de tout un chacun évolue, non seulement avec le temps mais également en fonction de l'état nerveux, voire d'ébriété, du signataire.

34. La signature dynamique ne doit pas être confondue avec le procédé consistant simplement à *numériser une signature manuscrite au moyen d'un scanner*. Ce procédé, qui permet de reproduire à l'infini le graphisme d'une signature manuscrite, ne diffère finalement de la reproduction par photographie que par son degré de perfection. Il ne présente aucune garantie quant à l'identité de la personne qui a opéré la reproduction. Le document qui porte une telle signature n'a pas plus de valeur qu'une simple photocopie.

La difficulté de distinguer une signature manuscrite originale de sa reproduction réalisée par un procédé numérique montre cependant combien la première n'assure que de manière précaire la fonction d'identification qu'on lui prête traditionnellement. L'avenir du procédé de signature dont il est question ci-après n'en est que plus radieux.

CHAPITRE II. LA SIGNATURE BASÉE SUR LA CRYPTOGRAPHIE ASYMÉTRIQUE

35. La signature dite digitale, ou numérique, basée sur la cryptographie asymétrique, semble constituer la seule technique qui, à l'heure actuelle, permette d'assurer dans l'environnement télématique avec un degré élevé de fiabilité les fonctions d'identification, de non-répudiation et de maintien de l'intégrité. Il n'est dès lors pas étonnant que ce soit sur ce procédé que s'est focalisée l'attention des pouvoirs normatifs.

Et si, contrairement à d'autres textes , la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques a vocation à s'appliquer à d'autres types de signatures électroniques , il ne fait nul doute que la signature numérique constitue le modèle sur lequel ont été façonnés les principes de la directive. Celle-ci est, pour ce motif, difficilement compréhensible à qui ne maîtrise pas un minimum de notions à propos de la cryptographie asymétrique. C'est pourquoi, à l'instar de la plupart des auteurs qui traitent du sujet, nous nous risquerons à donner un aperçu du procédé . Nous espérons que les hommes de science sous les yeux desquels échouerait par mégarde la présente contribution voudront bien pardonner aux pauvres juristes que nous sommes les éventuelles incohérences, imprécisions ou erreurs qui se seront immanquablement glissées dans les lignes qui suivent.

Comme l'indique l'étymologie hellénique de son nom, la cryptographie a pour objet premier d'assurer le caractère secret de communications. De manière logique, son usage, qui remonte à l'antiquité, a longtemps été cantonné au domaine militaire. L'utilisation des procédés cryptographiques n'a d'ailleurs été libéralisée en Belgique, de manière progressive, que récemment .

L'ère de la télématique a vu se développer des procédés de cryptographie basés sur l'utilisation d'*algorithmes* et de "*clés*". Un algorithme est une fonction mathématique qui, de manière imagée, peut être comparée à une moulinette. Son effet est de transformer, au terme d'une opération dite de *chiffrement*, une séquence donnée de *bits* (*binary units* soit une suite de 0 et 1) en une séquence différente. L'opération inverse est le *déchiffrement*. On notera que si les algorithmes eux-mêmes appartiennent au domaine public, les opérations de chiffrement et de déchiffrement ne peuvent être réalisées qu'au moyen de *paramètres* que sont les clés de chiffrement et de déchiffrement. Ces clés, qui, comme les données à chiffrer, ne sont autres qu'une suite de bits, sont, en principe, secrètes et ont une longueur variable. La fiabilité de l'opération dépend, d'une part, de la longueur de la clé utilisée et, d'autre part, de la "robustesse" de l'algorithme.

Trois types d'algorithmes sont utilisés en cryptographie : algorithmes symétriques, algorithmes asymétriques et algorithmes de hachage.

36. Comme on le sait, la communication à distance par l'internet implique que les données échangées transitent par une série de relais (serveurs, routeurs...). Il existe dès lors un risque qu'une personne mal intentionnée intercepte les données lors de leur transfert, en prenne connaissance et, le cas échéant, les modifie à l'insu de l'expéditeur. La cryptographie symétrique a pour principal avantage de pallier ce danger. Sachant que tout texte qui apparaît en clair sur l'écran d'un ordinateur est stocké et transmis sous forme de *bits*, suivant une sorte d'alphabet universel , il est possible de chiffrer la

séquence initiale de bits au moyen d'un algorithme symétrique et d'une clé secrète préalablement à son envoi . Le message, incompréhensible par les tiers, sera "déchiffré" par son destinataire au moyen de la même clé.

Remarquons que si ce système assure la confidentialité du message, il présente néanmoins des inconvénients. Il suppose d'abord que tout intervenant partage avec chacun de ses correspondants une clé secrète distincte. La gestion de ces clés est dès lors malaisée. Mais, surtout, ce problème paraît impraticable dans un réseau ouvert où une communication préalable des clés n'a pu avoir lieu de manière sécurisée. Enfin, on relèvera que la fonction d'identification inhérente au concept de signature n'est pas assurée de manière totale, dès lors qu'il est impossible de savoir lequel des correspondants détenant la clé a chiffré un message donné.

37. La solution à ces problèmes réside dans le recours à un cryptosystème asymétrique . Ce dernier repose sur l'utilisation d'une paire de clés différentes. L'une des clés est une fonction irréversible de l'autre. Ce qui est chiffré au moyen d'une de ces clés ne peut être déchiffré qu'en appliquant l'autre clé, et inversement. Dans la pratique, une des clés - dite *privée ou secrète* - ne sera connue que du titulaire du "bi-clé", tandis que l'autre sera divulguée publiquement, d'où son nom de *clé publique*. Vu que la clé publique est une fonction irréversible de la clé privée, il est impossible, dans un temps raisonnable , de connaître la clé privée au départ de la clé publique.

38. Notons dès à présent que le cryptosystème asymétrique présente l'inconvénient d'être nettement moins performant en termes de rapidité que le modèle symétrique . Pour pallier cet inconvénient, le troisième type d'algorithme mentionné ci-dessus, *l'algorithme de hachage* est combiné à l'algorithme de chiffrement asymétrique. Cet algorithme présente la propriété de convertir un texte (séquence de bits) d'une longueur quelconque en un message d'une longueur fixe, en l'espèce nettement inférieure à celle du message originaire. L'avantage est que, malgré cette réduction, le hachage de messages distincts ne donnera jamais un résultat identique. Le résultat de l'opération représente en quelque sorte *l'empreinte digitale* du message originaire (*digest* en anglais) . Ainsi, en chiffrant, au moyen de l'algorithme asymétrique et d'une de ses clés, cette empreinte plutôt que le message lui-même, un temps considérable peut être gagné et le système devient suffisamment performant pour être appliqué à des messages d'une certaine longueur.

39. Le cryptosystème asymétrique permet deux applications principales. D'abord, il permet d'assurer la *confidentialité* d'un message. Si l'expéditeur du message chiffre celui-ci au moyen de la clé publique de son destinataire, il est en effet assuré que seul ce dernier sera en mesure de le déchiffrer et, partant, d'en prendre connaissance, à

l'exclusion de toute autre personne. L'autre application - qui seule retiendra notre attention dans la suite de l'exposé - est celle qui permet de *signer* un message. Pour ce faire, l'expéditeur applique à son message, après l'avoir "haché", sa propre clé privée. Il obtient ainsi une version "chiffrée" de ce message, qui n'est autre que sa signature numérique. Il envoie ensuite à son correspondant le message lui-même, en clair, joint à cette signature. Comme le relève H. BITAN, " la signature électronique contrairement à la signature manuscrite n'a pas d'autonomie. La signature électronique dépend de l'acte ou du message auquel elle est associée. Il y aura donc autant de signatures électroniques distinctes que d'actes ou de messages différents transmis par une même personne" . Précisons cependant que le dispositif de création de signature d'une personne, soit l'algorithme de chiffrement et la clé privée, sont, eux, constants pour la durée de validité de la clé.

Une fois le message et sa signature parvenus à leur destinataire, celui-ci va procéder à la comparaison entre le message lui-même - ou l'empreinte de ce message qu'il obtient en le hachant – et le résultat du déchiffrement de la signature au moyen de la clé publique. S'il y a correspondance parfaite, il aura la certitude que le message a été expédié par la personne qui détient la clé privée correspondant à la clé publique qu'il a utilisée pour le déchiffrement et n'a pas été modifié au cours de la transmission. Reste à s'assurer de l'identité du titulaire de la paire de clés.

40. C'est ici qu'entre en jeu le *tiers certificateur* . Celui-ci assure la mission fondamentale de certifier au destinataire que la clé publique que ce dernier a utilisée appartient bien à telle personne déterminée et est bien la fonction irréversible d'une clé privée qui n'est, en principe, connue que de cette personne. Ces renseignements sont contenus dans un *certificat* délivré par le tiers certificateur au titulaire du "bi-clé". Ce certificat, qui s'apparente à une *carte d'identité électronique*, pourra être joint par l'expéditeur aux messages signés qu'il envoie. Il sera, en outre, consultable dans un *annuaire électronique* tenu par le certificateur. La norme Iso X. 509 définit le contenu standard d'un certificat. Il contient notamment le nom de l'autorité qui a généré le certificat, le nom du propriétaire de celui-ci, sa période de validité, la clé publique du titulaire et l'algorithme avec lequel sera utilisée cette clé. Le certificat, enfin, porte la signature numérique du certificateur lui-même .

41. Ainsi, la cryptographie asymétrique, jointe à l'intervention d'un tiers certificateur, remplit avec un haut degré de fiabilité les fonctions analysées comme étant celles d'une signature. L'identification d'abord, comme nous l'avons montré, est assurée. La non-répudiation également, dans la mesure où une personne n'utilisera sa clé privée que pour signer des messages ou des actes auxquels elle souhaitera marquer son consentement. L'intégrité du message, enfin, peut être aisément vérifiée. En effet, s'il

vient au destinataire ou à un tiers l'idée de le modifier, cette modification apparaîtra immédiatement, dès lors que le message haché ne correspondra plus au résultat du déchiffrement de la signature numérique au moyen de la clé publique de l'expéditeur et dès lors que le destinataire ou le tiers, parce qu'il ne connaît pas la clé privée de l'expéditeur, n'a pas la possibilité de créer une fausse signature en chiffrant le message qu'il a modifié.

Notons encore que les fonctions de signature et de confidentialité peuvent être cumulées en appliquant au message, d'une part, la clé publique du destinataire et, d'autre part, la clé privée de l'expéditeur.

42. La complexité du mécanisme décrit ci-dessus pourrait, à juste titre, rebuter les esprits les mieux disposés. Qu'ils se rassurent. Les différentes opérations décrites ci-dessus se déroulent en pratique de manière presque automatique et à l'insu des intervenants . L'exemple qui suit tente de le montrer.

Supposons que *Primus* souhaite adresser un message signé numériquement à *Secundus*. Ceci suppose bien sûr que l'un et l'autre soient équipés, non seulement du matériel permettant la navigation sur le web, mais également d'un logiciel de courrier électronique permettant la signature numérique . Il est également requis que *Primus*, préalablement à l'envoi de son premier message, ait généré sur internet une paire de clés asymétriques ou ait demandé au certificateur de lui en fournir une. Dans les deux cas, *Primus* demande à *Tertius*, le certificateur, de lui délivrer un certificat. Ce certificat atteste, d'une part, que *Primus* est bien titulaire de la clé publique qui y est mentionnée et, d'autre part, qu'il y a correspondance entre cette clé et la clé privée que *Primus*, au terme de l'opération initiale, est le seul à connaître. Concrètement, cette clé privée sera stockée sur le disque dur de l'ordinateur de *Primus* ou, mieux, sur un support externe. Le support idéal semble, à l'heure actuelle, être une carte à puce qui est alors insérée, au moment de la signature, dans un lecteur spécifique raccordé à l'ordinateur . L'introduction d'un code "PIN" est, en outre, généralement requise pour l'activation de la carte. Ce code ne doit pas être confondu avec la clé privée elle-même, qui est contenue dans la puce de la carte et qui est d'ailleurs bien trop complexe pour être mémorisée par l'utilisateur.

Primus est alors en mesure d'envoyer des messages signés de manière fiable. Pour ce faire, il insère sa carte à puce dans le lecteur prévu à cet effet, rédige son message ("Veux-tu acheter mon char pour mille sesterces ?), indique l'adresse e-mail de son destinataire puis clique sur l'icône "*signer*". Ce faisant, et sans que rien n'apparaisse à l'écran, le message qui, supposons-le, se lit en binaire "11000101000011111000101010011" est automatiquement haché pour devenir

"11001001" puis "chiffré", au moyen de la clé privée de *Primus*, en "01011100". Cette dernière séquence, qui constitue la signature du message, est envoyée à *Secundus* avec le message en clair. La confidentialité peut aussi être assurée par le seul fait de "cliquer" sur une seconde icône prévue à cet effet, appliquant au message la clé publique de *Secundus* et rendant le message illisible pour tout qui ne détient pas la clé privée de *Secundus* .

Parvenue dans l'ordinateur de *Secundus*, la signature (01011100) est déchiffrée (en 11001001) au moyen de la clé publique de *Primus* que le logiciel de *Secundus* a découvert dans le certificat . Par ailleurs, le message lui même (11000101000011110001010100011) se voit appliquer l'algorithme de hachage. L'empreinte obtenue (en principe 11001001) est comparée à celle obtenue au terme du déchiffrement de la signature . Si les deux empreintes coïncident, *Secundus* est simplement informé de ce qu'il a reçu de *Primus* un message signé et du contenu de ce message. Si les empreintes ne coïncident pas ou si le certificat de *Tertius* ne figure pas parmi les certificats d'autorités de certification que contient le logiciel de *Secundus*, celui-ci est informé de ce qu'il a reçu un message dont l'intégrité et l'origine ne sont pas assurées.

43. Ainsi, le procédé de la signature numérique, quoique fort complexe dans ses rouages, se manipule relativement aisément en pratique. Il faut bien reconnaître cependant que, à l'heure actuelle, il n'est utilisé que par une fraction extrêmement limitée des "internautes", principalement des sociétés commerciales de grande envergure. Si l'on rencontre assez fréquemment des *sites* dits *sécurisés* , c'est-à-dire dont le certificat assure l'identité du titulaire du site et la propriété du nom de domaine , il paraît malaisé de découvrir des sites de vente permettant au consommateur, lorsqu'il accepte une offre, d'apposer à un endroit ou à un autre sa *signature numérique* si d'aventure il en possède une. Cependant, on peut supposer que de tels systèmes se développeront à moyen voire à court terme. Le coût de l'émission d'un certificat peut en effet être jugé raisonnable (environ 50 euros pour une personne physique) et les ordinateurs personnels devraient à l'avenir être de plus en plus régulièrement équipés de lecteurs de cartes à puce. La directive 1999/93/CE et ses mesures d'exécution nationales sont de nature, comme nous allons le voir, à accélérer et encourager une telle évolution.

TITRE III. Le mouvement lÉgislatif

CHAPITRE PREMIER. LES TEXTES PERTINENTS

44. Les incertitudes concernant le statut des éléments probatoires dans l'environnement électronique ne sont évidemment pas propres à notre petit pays. On ne s'étonnera dès lors pas de constater aux quatre coins du globe une certaine frénésie législative en la matière . Le caractère mondial de l'internet a également conduit diverses organisations internationales à s'intéresser au sujet . Nous nous limiterons pour notre part à présenter la directive du 13 décembre 1999 créant un cadre communautaire pour les signatures électroniques et les dispositions légales qui ont été récemment adoptées en Belgique en vue de mettre en œuvre cette directive.

Section 1. La directive sur la " signature électronique "

45. C'est le 13 décembre 1999 que fut adoptée, au terme de la procédure de co-décision , la directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques. L'objectif spécifique de la directive est "de faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique" (art. 1er). Au delà, la directive est motivée par l'objectif premier des Communautés : le bon fonctionnement du marché intérieur et, partant, l'élimination de toute entrave à la libre circulation des marchandises et des services au sein de celui-ci. La Commission avait en effet relevé que divers Etats membres avaient adopté ou s'apprêtaient à adopter des règles particulières en matière de signature électronique, le cas échéant selon des approches divergentes, alors que d'autres Etats n'avaient pris aucune initiative en la matière . Une harmonisation s'avérait dès lors nécessaire pour éviter tout obstacle au développement du commerce électronique intra-communautaire. Cette harmonisation, classiquement, est couplée au principe de la reconnaissance mutuelle. Il est évident, par ailleurs, que la directive 1999/93 constitue une des pièces du *corpus* législatif européen émergeant relatif à la "Société de l'Information" .

Le cadre juridique mis en place par la directive est double. Il concerne, d'une part, les services de certification et les prestataires de ceux-ci, dont nous avons laissé entrevoir le rôle au numéro 40 de ce rapport. Nous présenterons ci-dessous les grandes lignes de ce régime (Chapitre II). La directive fixe, d'autre part, les effets juridiques des signatures électroniques. C'est ce second aspect qui retiendra principalement notre attention (Chapitre III).

Section 2. L'article 1322, al. 2, nouveau du Code civil et la loi du 9 juillet 2001 sur les signatures électroniques et les services de certification

46. Les Etats membres étaient priés de mettre en vigueur avant le 19 juillet 2001 les dispositions de droit national nécessaires pour se conformer à la directive. En Belgique, deux textes doivent, à cet égard, être pris en compte. Le premier, déposé sous la législature précédente sous l'intitulé de "*projet de loi visant à modifier certaines dispositions du Code civil relatives à la preuve des obligations*" a, après un avis très critique du Conseil d'Etat et un élagage sérieux , été joint à une proposition de loi de G. BOURGEOIS, "*introduisant de nouveaux moyens de télécommunication dans la procédure judiciaire et extrajudiciaire*" , pour devenir la proposition de loi *" introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire "* .

Ce texte, adopté par la Chambre des représentants en séance plénière le 6 juillet 2000 et non évoqué par le Sénat, a été sanctionné et promulgué le 20 octobre 2000 et publié au Moniteur du 22 décembre 2000 . Comme son intitulé nouveau le laisse pressentir, il contient deux chapitres, l'un introduisant des modifications dans le Code civil, l'autre dans le Code judiciaire. Les modifications du Code civil, entrées en vigueur dix jours après leur publication, soit le 1er janvier 2001, sont au nombre de deux. D'une part, l'article 1322 du Code est complété d'un second alinéa. Il sera examiné ci-après. D'autre part, l'article 2281, réglant autrefois l'application dans le temps des lois relatives à la prescription et abrogé depuis 1949, est rétabli dans un titre XXI intitulé "De la notification". Cette disposition précise les différentes manières dont pourra désormais être accomplie une notification, acte juridique unilatéral exigé à diverses reprises dans le Code . Il est ainsi fait place - comme en matière judiciaire d'ailleurs - aux techniques du télégramme, du télex, de la télécopie et du courrier électronique. L'article 2281, al. 3, nouveau précise qu'*" à défaut de signature au sens de l'article 1322, le destinataire peut, sans retard injustifié, demander au notifiant de lui fournir un exemplaire original signé. S'il ne le demande pas sans retard injustifié ou si, sans retard injustifié, le notifiant fait droit à cette demande, le destinataire ne peut invoquer l'absence de signature "*. En dépit de cette référence à la notion de signature, nous n'examinerons pas l'article 2281 nouveau, notre propos étant limité à la preuve, dans l'environnement informatique, des obligations contractuelles .

47. Le second texte belge à prendre en considération est la récente loi du 9 juillet 2001 "*fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification*" (ci-après "la loi du 9 juillet 2001"). Comme le précise son article 2, al. 1er, cette loi a pour objet explicite de transposer la directive 1999/93/CE. A l'instar de cette dernière, elle régit tant l'activité des prestataires de service de certification que

les effets de la signature électronique. On relèvera au passage le caractère mouvementé de la gestation législative de ce texte .

La circonstance que deux lois distinctes traitent l'une et l'autre pour partie des signatures électroniques en matière de preuve est évidemment de nature à susciter des difficultés, en particulier à propos de l'articulation des textes entre eux.

Section 3. Définitions liminaires et neutralité technologique

48. Avant d'examiner les deux groupes de dispositions matérielles relatives, d'une part, aux prestataires de services de certification et, d'autre part, au régime juridique de la signature électronique, il paraît indispensable de s'arrêter quelques instants sur les articles 2 de la directive et de la loi du 9 juillet 2001. Ceux-ci définissent une série de notions utilisées dans la suite des textes.

Ces notions apparaissent au premier abord quelque peu déconcertantes, non seulement pour le juriste auquel elles sembleront éminemment techniques, mais paradoxalement aussi pour le scientifique rompu au fonctionnement de la cryptographie asymétrique, qui ne retrouvera pas les termes qu'il utilise quotidiennement. Cette dernière constatation s'explique par le souci des autorités européennes d'adopter un texte *neutre du point de vue technologique* . Si la cryptographie asymétrique occupe aujourd'hui les devants de la scène, rien n'exclut que, à terme, une autre technique assure de manière plus efficace et plus sûre les fonctions d'identification, d'adhésion et d'intégrité. Il convenait dès lors de recourir à des termes suffisamment souples pour ne pas exclure les techniques d'authentification qui pourraient se développer dans le futur. Ainsi, plutôt que d'utiliser les mots "clé privée" et "clé publique", les articles 2 de la directive et de la loi utilisent ceux de "données afférentes à la création de signature" et de "données afférentes à la vérification de signature", ces données étant mises en oeuvre par un "dispositif (logiciel ou matériel) de création - ou de vérification - de signature". De même, l'adjectif "électronique" a été substitué, pour qualifier la signature, à ceux de "numérique" et de "digitale" qui apparaissaient à différentes reprises dans le texte de la proposition initiale de directive et dans l'avant-projet de loi .

Le souci d'éviter l'obsolescence de la directive est également rencontré par la mission de suivi confiée à la Commission. Celle-ci devra rendre compte au Parlement européen et au Conseil de la mise en oeuvre de la directive dans les deux ans de la date de transposition et, à cette occasion, "*déterminer s'il convient de modifier le champ d'application de la (…) directive pour tenir compte de l'évolution des technologies, du marché et du contexte juridique et, le cas échéant, formuler des propositions législatives*" (art. 12).

49. On relèvera par ailleurs dans les articles 2 de la directive et de la loi du 9 juillet 2001 un dédoublement de plusieurs définitions. Ainsi, à côté de la "signature électronique" figure la "signature électronique *avancée*"; on distingue, à côté du "dispositif de création de signature", le "dispositif *sécurisé* de création de signature"; le "certificat", défini comme "l'attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne", peut dans certains cas accéder au statut de "certificat *qualifié*". La distinction entre ces faux jumeaux dépend généralement de la question s'ils satisfont ou non à une série de conditions. Les exigences prescrites pour les signatures électroniques avancées sont stipulées dans l'article 2 lui-même tandis que celles concernant les certificats qualifiés et les dispositifs sécurisés de création des signatures électroniques se trouvent dans les annexes de la directive . Cette même structure a été adoptée dans la loi du 9 juillet 2001 .

Chapitre II. Les services de certification, leurs prestataires, LES CERTIFICATS ET LEURS TITULAIRES

Section 1. Liberté d'accès au marché et régimes volontaires d'accréditation

50. Le premier principe consacré par la directive est celui de la *liberté d'accès au marché* : selon l'article 3.1 de la directive, les Etats membres ne soumettent la fourniture de services de certification à *aucune autorisation préalable*. Ce principe est repris à l'article 4, § 2, de la loi du 9 juillet 2001 qui enjoint toutefois à tout prestataire émettant des certificats qualifiés de communiquer certaines informations à l'administration.

51. L'interdiction de subordonner la fourniture de services de certification à une autorisation préalable ne signifie évidemment pas que les Etats membres ne peuvent réglementer l'*activité* des prestataires de tels services. La directive fixe à cet égard des exigences minimales qu'il appartient aux Etats membres de transposer dans leur droit interne.

52. Quant au principe du libre accès, il est tempéré par l'article 3.2 de la directive : "sans préjudice des dispositions du paragraphe 1, les Etats membres *peuvent* instaurer ou maintenir des *régimes volontaires d'accréditation* visant à améliorer le niveau du service de certification fourni". En vertu de l'article 11, les Etats membres doivent informer la Commission et les autres Etats membres des régimes volontaires d'accréditation qu'ils mettent en place et communiquer les nom et adresse des organismes nationaux responsables de l'accréditation ainsi que de tous les prestataires de service de certification accrédités.

La loi du 9 juillet 2001 confie la tâche d'octroyer et de retirer les accréditations à l'administration du Ministère des Affaires économiques (art. 2, 12° et art. 17). Le Roi est invité à fixer, notamment, la procédure de délivrance, de suspension et de retrait de l'accréditation ainsi que les modalités du contrôle des prestataires accrédités. L'article 17, § 3, confirme que le choix de recourir à un prestataire de services de certification accrédité est libre . La qualité de prestataire accrédité est protégée pénalement (art. 21).

Nous relèverons que le régime de faveur réservé aux prestataires de service de certification accrédités n'a cessé d'être rétréci au fil du mûrissement du projet. Alors que le projet de loi initial semblait établir un lien nécessaire entre l'accréditation et le caractère qualifié du certificat , la loi autorise sans nul doute, dans sa version définitive, l'émission de certificats qualifiés par des prestataires non accrédités. C'est au niveau des effets juridiques reconnus à la signature électronique que l'accréditation présentera des avantages . L'accréditation est en outre particulièrement utile aux certificateurs établis en dehors de la Communauté . Soulignons que, dès lors qu'ils émettent des certificats qualifiés, les prestataires de service de certification, accrédités ou non, sont soumis aux mêmes obligations , des différences pouvant éventuellement exister au niveau du contrôle .

Section 2. Philosophie de la directive : harmonisation et reconnaissance mutuelle, traitement national et libre prestation

53. La directive 1999/93/CE est une directive d'harmonisation. C'est en vue de rapprocher les législations des Etats membres qu'elle définit, respectivement dans ses annexes I et II, les exigences auxquelles devront satisfaire les certificats qualifiés et les prestataires de service de certification délivrant de tels certificats. La directive pose également des règles minimales en matière de responsabilité des prestataires de service de certification qui délivrent à l'attention du public un certificat présenté comme qualifié ou qui garantit au public un tel certificat. Quelques principes en matière de protection des données à caractère personnel sont également précisés. Quant à l'annexe III, elle énonce les exigences minimales pour les dispositifs sécurisés de création de signature électronique. L'annexe IV, enfin, contient des recommandations pour la vérification sécurisée de la signature. Tous ces points seront examinés en temps utile.

54. Selon la méthode habituelle, l'harmonisation minimale organisée par la directive entraîne la reconnaissance mutuelle des mesures adoptées par les autres Etats membres. L'article 3.4 de la directive illustre ce principe : "*La conformité des dispositifs sécurisés de création de signature aux conditions posées à l'annexe III est déterminée par les organismes*

compétents, publics ou privés, désignés par les Etats membres (…) La conformité aux exigences de l'annexe III qui a été établie par les organismes visés au premier alinéa est reconnue par l'ensemble des Etats membres" .

55. L'article 4 de la directive 1999/93 confirme par ailleurs que les principes fondateurs du marché intérieur - traitement national et libre prestation de services - sont applicables aux services de certification. Aux termes de cette disposition, "chaque Etat membre applique les dispositions nationales qu'il adopte conformément à la présente directive *aux prestataires de service de certification établis sur son territoire* et aux services qu'ils fournissent. Les Etats membres *ne peuvent imposer de restriction* à la fourniture de services de certification provenant d'un autre Etat membre dans les domaines couverts par la présente directive".

Ainsi, chaque prestataire de service de certification doit satisfaire aux exigences de l'Etat membre dans lequel il est établi - au sens de l'article 43 (ex. art. 52) du Traité de Rome – et pourra dès lors prester ses services dans chacun des autres Etats membres. La libre prestation de service est rendue praticable par l'harmonisation minimale et la reconnaissance mutuelle qui en est le corollaire.

L'article 16, § 1, de la loi du 9 juillet 2001 fait application des principes de reconnaissance mutuelle et de libre prestation en énonçant qu' « *un certificat qualifié délivré à l'intention du public par un prestataire de service de certification qui est établi dans un Etat membre de l'Espace Economique européen est assimilé aux certificats qualifiés délivrés par un prestataire de service de certification établi en Belgique* ».

56. Ces principes, de manière logique, sont complétés par celui du *"home country control*" : aux termes de l'article 3.3 de la directive, « *chaque Etat membre veille à instaurer un système adéquat permettant de contrôler les prestataires de service de certification établis sur son territoire et délivrant des certificats qualifiés au public* » .

57. Quel est, dans ce modèle, le sort des prestataires de service de certification établis en dehors de la Communauté ? Selon l'article 7 de la directive, relayé par l'article 16, § 2, de la loi du 9 juillet 2001, les certificats qualifiés émis par les prestataires de pays tiers devront être reconnus équivalents aux certificats délivrés par un prestataire établi dans la Communauté dans trois hypothèses. Deux d'entre elles sont classiques. Il y aura d'abord équivalence lorsque le prestataire remplit les conditions visées dans la directive (l'annexe II) *et* a été accrédité dans le cadre d'un régime volontaire d'accréditation établi dans un Etat membre. Cette dernière précision révèle sans conteste l'un des avantages de l'accréditation. Ensuite, l'équivalence est également acquise lorsque le prestataire est reconnu en application d'un accord bilatéral ou multilatéral entre la Communauté et des

pays tiers ou des organisations internationales .

Enfin, la troisième hypothèse dans laquelle l'équivalence sera reconnue est plus spécifique et repose sur le mécanisme même de la certification : il y aura équivalence lorsqu'un prestataire de service de certification établi dans la Communauté et qui satisfait aux exigences de la directive garantit lui-même le certificat émis par le prestataire établi dans le pays tiers. Ne pourrait-il suffire, à cet égard, que le prestataire communautaire ait accepté d'émettre un certificat au nom du prestataire tiers et certifiant la signature électronique de celui-ci ? Dès lors, tous les certificats délivrés à des personnes physiques ou morales par le prestataire tiers et signés par lui seraient indirectement garantis par le prestataire communautaire.

Section 3. Obligations et responsabilité des prestataires de service de certification délivrant des certificats qualifiés

58. C'est un régime à deux vitesses que met en place la directive 1999/93 : selon que les prestataires de service de certification présentent les certificats qu'ils délivrent comme qualifiés ou non, ils devront répondre à une série d'exigences strictes ou pourront se borner à respecter quelques dispositions en matière de protection des données à caractère personnel . Rappelons que le législateur belge, dans la loi du 9 juillet 2001, fait usage de la possibilité réservée par la directive d'ajouter une "troisième vitesse" au système en permettant aux prestataires délivrant des certificats qualifiés de demander une accréditation .

C'est essentiellement par les annexes I et II, d'une part, et par la disposition relative à la responsabilité des prestataires délivrant des certificats qualifiés, d'autre part, que la directive évoque les obligations mises à charge des prestataires émettant des certificats qualifiés. Quant à la loi du 9 juillet 2001 elle-même, son article 11 procède également par renvoi à des annexes I et II reproduisant celles de la directive. D'autres obligations relatives aux prestataires délivrant des certificats qualifiés découlent de dispositions diverses concernant soit " les missions " de ces prestataires, soit leur responsabilité, soit encore la révocation des certificats qualifiés. Nous nous proposons d'étudier ces différents thèmes.

§ 1. « Des missions »

59. Aux termes des articles 8 et 9 de la loi du 9 juillet 2001, trois obligations essentielles sont imposées au certificateur lors de la délivrance d'un certificat qualifié.

L'article 10, par ailleurs, prévoit que le certificateur "conserve un *annuaire électronique* comprenant les certificats qu'il délivre et le moment de leur expiration". Il s'agit en réalité d'une redondance par rapport aux points b) et c) de l'annexe II. Cet annuaire devra être consultable "*on line*" par le destinataire de messages signés et tenu à jour, afin que le destinataire d'un message signé sur base d'un certificat révoqué puisse s'en apercevoir en temps utile .

60. Lors de l'émission d'un certificat qualifié, le prestataire de service de certification doit en premier lieu "*vérifier la complémentarité des données afférentes à la création et à la vérification de signature*" (art. 8, § 1er) . Cette obligation semble imposée au certificateur sans qu'il faille distinguer selon qu'il a généré lui-même ces données ou que le demandeur de certificat les lui a communiquées. Toutefois, l'article 14 relatif à la responsabilité du prestataire paraît limiter la présomption de responsabilité qu'il énonce au prestataire générant lui-même les clés .

61. Le certificateur doit en second lieu vérifier l'identité et, le cas échéant, les qualités spécifiques de la personne pour laquelle le certificat est émis (art. 8, § 2, disposition qui fait double emploi avec le point d) de l'annexe II). Pour éviter d'engager ultérieurement sa responsabilité, le certificateur sera bien avisé, lors de l'enregistrement, d'exiger la présentation d'éléments suffisamment probants. Lorsqu'une personne physique demande au prestataire de lui délivrer un certificat qualifié, il nous semble que le prestataire devrait, par mesure de prudence, exiger la comparution personnelle du candidat muni de sa carte d'identité . Comme nous le verrons ultérieurement, un certificat peut également être délivré à une personne morale, qui aura dès lors une signature électronique propre. S'il s'agit d'une société commerciale, le certificateur devrait, d'une part, exiger ses statuts et, d'autre part, vérifier, selon les règles du Code des sociétés, si la personne physique qui introduit la demande au nom de la personne morale a bien le pouvoir - conventionnel ou légal - de la représenter à cet effet . La délivrance d'un certificat est sans conteste un acte grave qui excède la gestion journalière d'une société. Les problèmes suscités par la signature des personnes morales seront évoqués plus loin, de même que l'examen de l'article 8, § 3, de la loi, apportant quelques précisions sur ce point. L'indication de qualités spécifiques dans le certificat ne doit également être réalisée qu'avec prudence . Ainsi, l'indication d'un titre professionnel protégé par la loi ne devrait être faite que sur présentation d'une attestation de l'ordre professionnel concerné.

Il semble être de pratique fréquente pour les prestataires de service de certification de confier à un organisme *ad hoc*, généralement appelé *autorité d'enregistrement*, la tâche de procéder à l'enregistrement des candidats à la délivrance d'un certificat, le prestataire se limitant à émettre ce certificat sur base des données fournies par cette autorité . Pour la

signature de personnes exerçant une profession réglementée, l'enregistrement peut être le fait des autorités de l'ordre professionnel, spécialement lorsque le certificat, outre l'identité du signataire, atteste de sa qualification professionnelle . Il eut également été imaginable, de manière générale, de confier la tâche de l'enregistrement aux administrations communales pour les personnes physiques et aux greffes des tribunaux de commerce pour les sociétés commerciales. Manifestement, les dispositions légales ne mentionnent pas ces autorités situées en amont du certificateur. Qui plus est la question se pose si l'article 8, § 2, en imposant au certificateur de vérifier l'identité du demandeur, ne rend pas illégale la pratique consistant pour le certificateur à recourir à une ou plusieurs autorités d'enregistrement indépendantes. Nous ne le pensons pas. Néanmoins, il faudra à notre sens considérer que l'autorité d'enregistrement reste tiers par rapport au contrat ayant pour objet l'émission du certificat et n'est que le sous-traitant du certificateur . Ceci a des conséquences évidentes en matière de responsabilité.

62. La troisième obligation du prestataire lors de l'émission d'un certificat qualifié est de fournir un exemplaire de celui-ci au candidat titulaire (art. 9 de la loi).

§ 2. Exigences des annexes I et II

63. Comme nous l'avons laissé entendre, c'est à l'annexe II, relative aux exigences concernant les prestataires de service de certification délivrant des certificats qualifiés, que sont inscrites les principales obligations de ceux-ci. L'annexe I est également capitale, dès lors qu'elle définit les mentions que doit nécessairement contenir tout certificat qualifié. Le renvoi à ces deux annexes est opéré par l'article 11 de la loi.

64. Aux termes de l'annexe II, les certificateurs visés doivent :
- faire la preuve qu'ils sont suffisamment fiables pour fournir des services de certification (a) ;
- assurer le fonctionnement d'un service d'annuaire et de révocation (b);
- veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision (c);
- vérifier, par des moyens appropriés, l'identité et, le cas échéant, les qualités spécifiques de la personne à laquelle un certificat qualifié est délivré (d);
- employer du personnel ayant les connaissances spécifiques, l'expérience et les qualifications nécessaires (e);
- utiliser des systèmes et des produits fiables (f);
- prendre des mesures contre la contrefaçon des certificats et garantir, lors de la génération des clés, la confidentialité de celles-ci (g);

- disposer de ressources financières suffisantes, la loi suggérant à cet égard de contracter une assurance de responsabilité (h);
- enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant 30 ans (i) ;
- ne pas stocker ni copier les données afférentes à la création de signature (j) ;
- fournir à toute personne demandant un certificat, avant d'accéder à cette demande, une série d'informations, dans une langue compréhensible par cette personne (k) ;
- utiliser des systèmes fiables pour stocker les certificats (l).

65. Aux termes de l'annexe I, tout certificat qualifié doit comporter :
a) une mention indiquant que le certificat est délivré à titre de certificat *qualifié* ;
b) l'identification du *prestataire* de service de certification ainsi que le pays dans lequel il est établi;
c) le nom du *signataire* ou un pseudonyme qui est identifié comme tel ;
d) la possibilité d'inclure, le cas échéant, une *qualité spécifique* du signataire, en fonction de l'usage auquel le certificat est destiné ;
e) des données afférentes à la vérification de signature qui correspondent aux données pour la création de signature sous le contrôle du signataire ;
f) l'indication du début et de la fin de la *période de validité* du certificat;
g) le code d'identité du certificat;
h) la *signature électronique* avancée *du prestataire* de service de certification qui délivre le certificat ;
i) les *limites* à l'utilisation du certificat, le cas échéant ;
j) les limites à la valeur des transactions pour lesquelles le certificat peut être utilisé, le cas échéant.

§ 3. De la révocation des certificats qualifiés

66. Les certificats de signatures électroniques ont normalement une durée de validité limitée. Comme nous venons de le voir, les certificats qualifiés doivent d'ailleurs nécessairement en faire mention. Le certificateur doit par ailleurs avertir le titulaire un mois avant cette expiration (art. 12, § 2, al. 2). Il est cependant des circonstances dans lesquelles il y a lieu de procéder à la révocation du certificat avant l'échéance de la date d'expiration. Les cas de révocation sont énoncés à l'article 12 de la loi. Le certificateur doit révoquer le certificat soit sur demande du titulaire du certificat (art. 12, § 1), soit d'office dans quatre hypothèses.

67. La principale est celle où il apparaît que la signature électronique ne peut plus assurer de manière fiable les fonctions qui sont les siennes. Tel sera le cas lorsque "*la*

confidentialité des données afférentes à la création de signature a été violée" (divulgation, perte ou vol de la clé privée, voire déduction de la clé secrète par un tiers au départ de la clé publique). Tel sera également le cas lorsqu'il apparaîtra que le certificat a été délivré sur base d'informations erronées ou falsifiées ou que les informations contenues dans le certificat ne sont plus conformes à la réalité (le titulaire, par exemple, a été radié de l'ordre professionnel auquel le certificat atteste qu'il appartient) .

Deux autres hypothèses sont liées à la situation du certificateur : il y aura révocation lorsque celui-ci aura reçu une injonction judiciaire de cesser ses activités pour avoir manqué à ses obligations (art. 12, § 2, 2°, renvoyant à l'art 20, § 4, b) ou lorsqu'il cessera ses activités sans qu'il n'y ait reprise par un autre prestataire garantissant un même niveau de qualité et de sécurité . La dernière hypothèse est celle du décès ou de la dissolution du titulaire du certificat .

68. Il est évidemment capital que les tiers soient avertis de la révocation d'un certificat . Le prestataire doit dès lors répondre sans délai à une demande de révocation (art. 13, § 1er) et, immédiatement après la décision de révocation, mentionner celle-ci dans l'annuaire électronique dont l'article 10 impose la tenue (art 13, § 2). C'est à partir de cette inscription que la révocation est opposable aux tiers (art. 13, § 3).

§ 4. Responsabilité des prestataires de service de certification

69. L'article 6 de la directive détermine des exigences minimales en ce qui concerne la responsabilité des prestataires de service de certification délivrant ou garantissant des certificats présentés comme qualifiés . Cette disposition est reproduite quasiment à la lettre à l'article 14 de la loi du 9 juillet 2001.

A notre sens, cet article 14 règle la responsabilité des prestataires de service de certification à l'égard des *destinataires* de messages signés de manière électronique ("tout organisme ou personne physique ou morale qui se fie raisonnablement au certificat ") . C'est dès lors la responsabilité *extracontractuelle* des certificateurs qui est en cause. Plus précisément, l'article 6 nous paraît imposer aux Etats membres d'introduire dans leur législation une *présomption de responsabilité* des certificateurs visés. Si le bénéficiaire de cette présomption doit établir positivement son dommage, la faute du certificateur sera par contre présumée dans diverses hypothèses :

1°) La faute est d'abord présumée lorsqu'il s'avère que les informations contenues dans le certificat qualifié étaient, à la date où ce certificat a été délivré, inexactes. C'est principalement une identification erronée du signataire qui pourrait être préjudiciable au

destinataire du message signé ;

2°) La faute du certificateur est également présumée lorsque les données prescrites pour un certificat qualifié ne sont pas toutes présentes, faute que le certificateur peut aisément éviter ;

3°) Le tiers certificateur pourrait également voir sa responsabilité engagée lorsque, au moment de la délivrance du certificat, le signataire ne détenait pas les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat ;

4°) La faute du prestataire de service de certification devra encore être présumée lorsqu'il apparaîtra que les données afférentes à la création de la signature et celles afférentes à sa vérification ne peuvent être utilisées de manière complémentaire. Conformément à la directive, la loi belge ne retient toutefois cette présomption de faute que dans l'hypothèse où le certificateur a lui-même généré les données afférentes à la création et à la vérification de signature, ce qui, comme nous l'avons vu, n'est pas toujours le cas, le demandeur de certificat pouvant présenter au certificateur une paire de clés qu'il a lui-même générée .

5°) Le certificateur sera enfin présumé en faute lorsqu'il aura omis de faire enregistrer la révocation du certificat.

70. Ces présomptions de faute sont réfragables : le prestataire de service de certification cesse d'être responsable "*s(’il) prouve qu’il n’a commis aucune négligence*". Le renversement de la présomption ne suppose donc pas nécessairement la preuve d'une cause étrangère libératoire .

La première présomption énoncée ci-dessus sera, par exemple, renversée s'il appert que le certificat a été délivré sur la présentation de documents d'identité falsifiés mais dont la falsification n'apparaissait qu’au terme d’un examen complexe. En ce qui concerne le défaut d'avoir procédé à l'enregistrement de la révocation du certificat, il convient de distinguer le motif de la révocation. Ainsi, on aperçoit mal comment le tiers certificateur pourrait établir qu'il a pu sans négligence omettre d'accéder à la demande de révocation du titulaire ou de l'autorité judiciaire. En revanche, les autres hypothèses de révocation appellent des distinctions. Ainsi, en cas de compromission des données afférentes à la création de signature, il conviendra de rechercher la cause de celle-ci.

71. Le prestataire de service de certification peut, en outre, limiter sa responsabilité à l'égard des personnes qui se fient aux certificats qu'il émet , en indiquant dans ceux-ci

(annexe I, i, j), soit les limites fixées à leur utilisation , soit la valeur limite des transactions pour lesquelles le certificat peut être utilisé. Les deux mentions pourraient le cas échéant être cumulées. Il est exigé que ces mentions soient "*discernables par les tiers*".

Entendons-nous bien : ces mentions ne signifient pas que la signature utilisée pour un usage exclu par le certificat ou pour une transaction d'un montant excédant la valeur limite y mentionnée n'est pas valable et, partant, que le signataire pourrait ne pas être valablement engagé . Mais, dès lors que le destinataire du message signé établit l'existence d'une des causes de responsabilité de l'article 14, §§ 1 et 2, les mentions précitées permettent au tiers certificateur de limiter le montant des dommages et intérêts réclamés à la valeur maximale indiquée dans le certificat ou de dégager sa responsabilité.

72. Notons encore que l'efficience de la mise en cause de la responsabilité des prestataires émettant des certificats qualifiés devrait en pratique être garantie par l'obligation faite à ceux-ci de disposer de ressources financières suffisantes (annexe II, h). Nous rappellerons que le législateur n'a malheureusement que suggéré et non imposé la souscription d'une assurance de responsabilité, encore que, comme le soulignent certains auteurs, « (…) le contrat d'assurance n'est pas le seul outil disponible qui permette d'offrir la garantie de ressources financières suffisantes » .

Section 4. Protection des données

73. Nous venons d'analyser les obligations imposées aux seuls prestataires délivrant des certificats qualifiés. L'article 5 de la loi du 9 juillet 2001 (art. 8 de la directive) relatif à la protection des données requiert par contre des Etats membres qu'ils imposent diverses obligations à tous les prestataires de service de certification, sans distinguer selon que ces prestataires émettent des certificats qualifiés ou non .

74. Se conformant à l'article 8.1 de la directive, l'article 5, § 1, de la loi commence par réserver l'application de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Elle prévoit ensuite qu'un prestataire de service de certification ne pourra recueillir des données personnelles "*que directement auprès de la personne concernée ou avec le consentement explicite de celle-ci et uniquement dans la mesure où cela est nécessaire à la délivrance et à la conservation du certificat*" et ajoute que "*les données ne peuvent être recueillies ni traitées à d'autres fins sans le consentement explicite de la personne intéressée*".

75. Toujours dans un souci de protection de la vie privée, l'article 8.3 de la directive

interdit aux Etats membres d'empêcher le prestataire de service de certification d'indiquer dans le certificat un *pseudonyme* au lieu du nom du signataire. Le préambule précise cependant que les dispositions relatives à l'utilisation de pseudonymes dans des certificats n'empêche pas les Etats membres de réclamer l'identification des personnes conformément au droit national ou communautaire. En Belgique, c'est seulement dans l'hypothèse où les nécessités d'une *instruction pénale* l'exigent que le certificateur sera tenu de communiquer l'identité du titulaire du certificat (art. 5, § 2). Ceci implique évidemment que toute personne souhaitant se voir délivrer un certificat sous un pseudonyme doit communiquer au certificateur son identité réelle et que ce dernier doit conserver celle-ci. Il est renvoyé, pour les conditions et les modalités de la divulgation aux autorités judiciaires, aux articles 90 *bis* à 90 *decies* du Code d'instruction criminelle, relatifs aux écoutes et à l'enregistrement des (télé)communications privées. Précisons enfin que lorsqu'un pseudonyme est utilisé, il doit être identifié comme tel en vertu de l'annexe I, c) de la loi .

Section 5. Contrôle des prestataires de service de certification

76. Le projet de loi initial n'organisait le contrôle que des seuls certificateurs accrédités, ce qui était logique dès lors qu'eux seuls pouvaient émettre des certificats qualifiés. Vu la suppression du lien, contraire à la directive, entre accréditation et caractère qualifié du certificat, le contrôle a été étendu *rationae personae.* Il pourrait même concerner tout prestataire de service de certification, vu l'habilitation donnée au Roi par l'article 20, § 1er. Le contrôle des prestataires n'émettant pas des certificats qualifiés - s'il s'en trouve – ne pourrait probablement porter que sur le respect des dispositions relatives à la protection des données à caractère personnel.

77. L'article 20 de la loi, en ses §§ 3, 4 et 5, prévoit une procédure particulière en cas de manquement aux prescriptions de la loi par un prestataire délivrant des certificats qualifiés. L'administration doit d'abord le mettre en demeure de prendre les mesures nécessaires afin de se conformer à ses obligations. Un délai raisonnable, qui sera fixé par l'administration en fonction de la nature du manquement constaté, lui est imparti à cet effet. Si à l'expiration de ce délai le prestataire n'a pas mis fin à l'infraction, l'administration pourra saisir les tribunaux. Si le prestataire est accrédité, elle pourra également lui retirer son accréditation et lui enjoindre de mentionner ce retrait dans son annuaire. Seuls les tribunaux pourront en revanche faire défense au contrevenant de continuer à émettre des certificats qualifiés. On peut s'étonner qu'une modification du Code judiciaire n'ait pas été envisagée pour donner au Président du tribunal de commerce statuant comme en référé la compétence spéciale de connaître de cette action.

78. Il ressort de l'article 17, § 2, 4°, de la loi que le Roi pourrait soumettre les prestataires accrédités à un contrôle plus rigoureux que ceux qui, sans être accrédités, délivrent des certificats qualifiés. Mais, dès à présent, une différence substantielle existe, dès lors que les prestataires ne reçoivent leur accréditation qu'après avoir été soumis à une évaluation par une "entité" visée à l'article 2, 13° du projet, laquelle va s'assurer du respect des annexes I, II et III (art. 17, § 1er). Il existe donc, dans le cas des prestataires accrédités, un contrôle systématique *a priori.*

Section 6. " Obligations " des titulaires de certificats

79. La loi du 9 juillet 2001 contient aussi l'une ou l'autre dispositions relatives aux " obligations " du titulaire de certificat. L'article 3 de la loi énonce ainsi de façon générale qu'elle « *fixe (…) les règles à respecter par (…) les titulaires de certificats, sans préjudice des dispositions légales concernant les règles de représentation des personnes morales* ". Plus spécialement, l'article 19 de la loi instaure le principe selon lequel le titulaire du certificat est seul responsable de la confidentialité de sa clé secrète dès le moment de la création de celle-ci . Concrètement, il est conseillé de stocker la clé privée de signature sur une carte à puce ou sur un *token*, plutôt que sur le disque dur d'un ordinateur ; en outre, un système de verrouillage par code « pin » est souhaitable, dans l'attente d'éventuels systèmes permettant de protéger l'accès à la clé privée par des moyens « biométriques », tels une reconnaissance de l'iris ou des empreintes digitales du titulaire du certificat .

En cas de doute sur le maintien de la confidentialité des données afférentes à la création de signature, mais aussi lorsque les informations contenues dans le certificat ne sont plus conformes à la réalité, l'article 19 de la loi enjoint au titulaire de procéder à la révocation du certificat . Enfin, le dernier paragraphe de cet article 19 interdit au titulaire (sous quelle sanction ?) d'utiliser sa clé secrète lorsque le certificat est arrivé à échéance ou est révoqué ; il ne peut pas non plus d'ailleurs faire certifier son " ancienne " clé secrète par un autre prestataire de service de certification.

Chapitre III. les effets de la signature Électronique

Section 1. La directive 1999/93/CE

80. C'est à l'article 5 de la directive que sont déterminés les effets juridiques que les Etats membres sont tenus de conférer aux signatures électroniques. Cette disposition opère une *summa divisio* entre, d'une part, ce que nous appellerons pour faire bref *les*

signatures électroniques parfaites et, d'autre part, *les autres signatures électroniques*. Les effets des premières sont régis par l'article 5.1, ceux des secondes par l'article 5.2.

§ 1er. Champ d'application de l'article 5

81. La présente contribution est consacrée au problème de la preuve des conventions conclues par voie électronique. Il est cependant capital de noter que le champ d'application de la directive 1999/93, et spécialement de son article 5 relatif aux effets juridiques des signatures électroniques, déborde largement ce sujet. Si la signature est un élément essentiel de l'écrit probatoire, il ne s'agit pas d'un concept propre au droit de la preuve. La signature est une exigence qui émerge dans un nombre appréciable de dispositions légales dans des disciplines aussi diverses que le droit civil , le droit judiciaire , le droit fiscal ou le droit social . *A priori*, l'article 5 a pour vocation à s'appliquer à ces différents domaines . Le 19ème considérant de la directive annonce en effet que "*les signatures électroniques seront utilisées dans le secteur public au sein des administrations nationales et communautaires et dans les communications entre lesdites administrations ainsi qu'avec les citoyens et les opérateurs économiques, par exemple dans le cadre des marchés publics, de la fiscalité, de la sécurité sociale, de la santé et du système judiciaire*". Ce champ d'application large est confirmé dans l'Exposé des motifs de la loi du 9 juillet 2001 . Si le séisme est d'une magnitude aussi étendue, il est vrai que la matière de la preuve en constitue l'épicentre. En attestent notamment le 21ème considérant et les références expresses à la notion de recevabilité comme preuve en justice dans les deux paragraphes de l'article 5.

82. Il convient également de rappeler les termes de l'article 1er de la directive, relatif au champ d'application de celle-ci : "*l'objectif de la présente directive est de faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique (...)* ". Ce premier alinéa est complété d'un second alinéa formulé, lui, en des termes négatifs : "(La directive) ne couvre pas les aspects liés à la conclusion et à la *validité des contrats* ou *d'autres obligations légales* lorsque des *exigences d'ordre formel* sont prescrites par la législation nationale ou communautaire (...) ". Cette restriction, éclairée par le 17ème considérant, nous paraît devoir être interprétée comme suit : la directive 1999/93 n'a pas pour objet de permettre la conclusion de tout contrat "*on line*" ni l'accomplissement par voie électronique de tout acte juridique quelconque. La seule portée de l'article 5 de la directive est de faire une place, lorsqu'une signature est exigée, à la version électronique de celle-ci. Toute autre disposition légale qui, en posant des exigences d'ordre formel, constitue une entrave à l'accomplissement d'un acte par voie électronique n'est pas remise en question par cette disposition. Il en résulte que si l'article 5 déborde largement le droit de la preuve, il ne l'épuise pas. Notre droit de la preuve pose en effet

certaines exigences d'ordre formel autres que la présence d'une signature. Si la subsistance de ces exigences n'est pas remise en cause par la directive sur la signature électronique, elle l'est en revanche par la directive 2000/31 sur le commerce électronique .

§ 2. Les signatures électroniques "parfaites" et la clause d'assimilation

83. L'article 5.1 vise les signatures :
- électroniques
- avancées
- basées sur un certificat qualifié et
- créées par un dispositif sécurisé de création de signature.

Chacun de ces éléments est défini à l'article 2 de la directive.

La signature électronique est "*une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification*" (art. 2.1). La comparaison de cette définition avec celle que la doctrine dite de l'approche fonctionnelle a proposé de la signature révèle que deux des fonctions évoquées par cette doctrine sont ici à première vue absentes : l'adhésion et l'intégrité. Le terme d'authentification, tel qu'il est utilisé dans cette disposition, nous paraît en outre déborder la fonction d'identification, dans la mesure où il ne se rapporte pas nécessairement à une personne. L'authentification consiste à notre sens dans la détermination de l'origine des données . Cette origine peut être une personne mais aussi une machine à partir de laquelle ont été envoyées les données, telle un télex, un télécopieur ou un ordinateur. Quant aux données authentifiées, elles ne consistent pas nécessairement en l'expression d'une volonté dans le but de créer des effets juridiques : il peut tout aussi bien s'agir d'un logiciel, des pages d'un site *web*, voire d'une œuvre littéraire ou artistique .

Pour être "avancée", la signature doit :
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.

Comme le relèvent M. ANTOINE et D. GOBERT , on reconnaît dans cette définition les fonctions d'identification (b) et d'intégrité (d). Force est dès lors de constater un porte-à-faux entre les définitions de la directive et celles proposées par la doctrine

"fonctionnaliste". Ce que la première nomme signature avancée se rapproche de ce que la seconde considère comme une signature pure et simple, la signature électronique non avancée étant une technique qui, dans la doctrine fonctionnaliste, ne pourrait être qualifiée de signature, à défaut d'identifier une personne et d'assurer la fonction de maintien de l'intégrité. Il nous semble même pouvoir être soutenu que la signature avancée de la directive est une notion plus compréhensive que la signature fonctionnelle classique puisque, si elle doit identifier son auteur, elle n'a pas nécessairement pour but de manifester l'adhésion de celui-ci au contenu d'un acte juridique.

La notion de certificat qualifié a été rencontrée au numéro 65. Rappelons également qu'un dispositif de création de signature est un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature (soit, en matière de cryptographie asymétrique, la clé privée) et qu'il est sécurisé lorsqu'il satisfait aux exigences prévues à l'annexe III de la directive (art. 2.5 et 2.6).

84. L'article 5.1 de la directive oblige les Etats membres à veiller à ce que les signatures électroniques " parfaites " :

a) *"répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier*

et

b) soient recevables comme preuves en justice".

85. Le point b) n'appelle que de brèves observations. Nous relèverons que, dans notre droit de la preuve, la notion de recevabilité concerne le mode de preuve et non la signature en tant que telle. On peut cependant considérer que le texte réalise une ellipse et que devront être recevables les documents "revêtus" d'une signature électronique parfaite.

86. Le point a) revêt en revanche un caractère quelque peu ésotérique. On pourrait en effet penser, à première lecture, qu'il énonce des conditions de validité supplémentaires auxquelles devraient satisfaire les signatures électroniques visées. Tel n'est pas le cas. L'énoncé des conditions de validité est l'objet, nous l'avons vu, de l'article 2 et des annexes auxquelles celui-ci renvoie. L'article 5, comme son intitulé l'indique, règle les *effets* juridiques des signatures électroniques. Le texte signifie en réalité que lorsqu'une disposition légale exige que des données soient accompagnées d'une signature, cette exigence, dès l'instant où les données sont fournies par la voie électronique, devra pouvoir être satisfaite par l'apposition d'une signature électronique "parfaite". C'est principalement l'emploi du pluriel ("aux" exigences, "ces" exigences) qui trouble la compréhension correcte du texte. Ce pluriel s'explique toutefois par la

multiplicité de dispositions légales qui, dans les législations des Etats membres, requièrent l'apposition d'une signature .

En bref, l'article 5.1, b), oblige les Etats membres à assimiler les données électroniques liées à une signature électronique parfaite à des données manuscrites ou imprimées revêtue d'une signature manuscrite. La doctrine retient dès lors, pour désigner l'article 5.1, l'expression de *clause d'assimilation* .

Comme nous l'avons dit ci-avant, l'assimilation est obligatoire chaque fois qu'une disposition légale interne pose l'exigence d'une signature et lui confère un effet de droit, peu importe que cette exigence soit de nature probatoire ou autre. Il y a lieu, en outre, de garder à l'esprit la notion très large de signature électronique avancée donnée par la directive. Toutefois, en droit belge, la portée effective de la clause d'assimilation nous paraît restreinte aux signatures par lesquelles une personne marque son adhésion à un acte juridique ; les signatures de sites ou de logiciels, en revanche, ne nous semblent pas pouvoir faire l'objet d'une assimilation à la « signature manuscrite », à défaut précisément de connaître un équivalent manuscrit auquel la loi attacherait des effets de droit.

Dans la matière de la preuve, la clause d'assimilation a pour effet qu'un document électronique auquel est lié une signature électronique parfaite sera assimilé à un document papier revêtu d'une signature manuscrite. La valeur probante qui sera attribuée à ce document dépend cependant de la législation interne de chaque Etat membre. Le 21ème considérant de la directive précise du reste que "*la présente directive n'affecte en rien la capacité d'une juridiction nationale de statuer sur la conformité aux exigences de la présente directive ni les règles nationales relatives à la libre appréciation judiciaire des preuves*". Ainsi, l'"écrit électronique parfait" ne fera pleine foi que lorsque l'écrit traditionnel a lui-même cet effet. Aucune atteinte n'est portée au régime de la liberté de la preuve dans les domaines ou dans les ordres juridiques où ce régime prévaut.

§ 3. La clause de non-discrimination

87. L'article 5.2 est relatif aux effets des signatures électroniques qui ne rencontrent pas les exigences permettant de les faire bénéficier de la clause d'assimilation. Aux termes de cette disposition, "*les Etats membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique 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 accrédité de service de certification
ou
- qu'elle n'est pas créée par un dispositif sécurisé de création de signature".

On aura constaté d'emblée la formulation négative utilisée. La doctrine qualifie d'ailleurs l'article 5.2 de *clause de non discrimination.*

Deux effets sont visés dans cette disposition : ce qui ne peut être refusé pour certains motifs aux signatures électroniques, c'est, d'une part, l'efficacité juridique et, d'autre part, la recevabilité comme preuve en justice.

88. Que faut-il entendre par l'"*efficacité juridique*" d'une signature électronique ?

Ne cachons pas qu'en posant la question de cette façon, nous écartons une des lectures possibles du texte de l'article 5.2 suivant laquelle l'efficacité juridique ne serait que l'efficacité juridique comme preuve en justice, lecture qui rendrait d'ailleurs quelque peu surabondant l'adjectif " juridique ".
A notre sens, la notion d'efficacité juridique de la signature ne peut être appréhendée qu'eu égard au champ d'application très large de l'article 5 . Certes, derechef, à l'égard des signatures de sites ou de logiciels, il ne pourrait être question de discrimination qu'à la condition de découvrir un texte qui accorde une efficacité juridique à des équivalents de ces procédés dans le monde papier. Quant aux signatures de personnes, l'efficacité dont question devra se manifester certainement dans le domaine du droit de la preuve mais aussi en dehors de celui-ci. Ainsi, par exemple, l'article 5.2 interdirait aux Etats membres de refuser la recevabilité d'une action en justice pour le seul motif que la requête serait signée électroniquement.

L'efficacité est *aussi* l'efficacité en matière de preuve. Ceci implique que les Etats membres devront veiller à ce que les motifs énumérés par l'article 5.2 ne puissent être invoqués pour refuser à la signature électronique toute valeur probante . Il n'est évidemment pas question d'imposer aux Etats membres de donner une force probante déterminée à ladite signature, résultat auquel même la clause d'assimilation n'aboutit pas, mais seulement d'empêcher que la non discrimination relative à la recevabilité - examinée ci-dessous - reste purement théorique en déniant systématiquement, et dans un second temps, toute valeur probante à la preuve reçue.

89. Quant à l'interdiction de refuser la recevabilité comme preuve en justice des signatures électroniques pour les motifs énumérés, elle soulève la question suivante : les Etats membres doivent-ils, comme dans l'article 5.1, assurer la recevabilité généralisée de l'écrit signé électroniquement ou bien peuvent-ils se limiter à veiller à ce que cet écrit soit recevable dans certaines hypothèses ? Comme on le sait, notre Code civil limite la recevabilité des présomptions de l'homme et des témoignages (art. 1341), tandis que l'écrit est en toute hypothèse recevable comme mode de preuve. Ne pourrait-on soutenir que, l'écrit électronique étant à tout le moins assimilable à une présomption de l'homme, la clause de non discrimination était déjà satisfaite par notre législation préalablement à l'introduction de l'article 1322, al. 2, dans notre Code civil ? La réponse à cette question découle en réalité de l'examen des motifs pour lesquels il est interdit de refuser la recevabilité – notamment - de la signature électronique.

90. Le premier motif prohibé est sans nul doute le plus important : l'efficacité juridique et la recevabilité comme preuve en justice ne peuvent être refusées à une signature électronique au seul motif que celle-ci se présente sous forme électronique. En d'autres termes, le caractère manuscrit de la signature, ou toute autre exigence équivalente, ne peut être imposé.

Il en résulte que notre droit de la preuve, tel qu'il existait avant sa récente modification, enfreignait la clause de non discrimination. Non pas parce que le document revêtu d'une signature électronique ne pouvait être reçu que dans les hypothèses où la preuve est libre mais parce que son irrecevabilité dans les autres hypothèses résultait de l'exigence - certes jurisprudentielle mais dirimante - du caractère manuscrit de la signature de l'acte sous seing privé .

Ainsi, c'est au premier chef au regard de la signature manuscrite que la signature électronique ne peut être discriminée. Les autres motifs pour lesquels il est interdit de refuser de recevoir une signature électronique en justice ou de lui prêter une efficacité juridique - absence de certificat qualifié, non délivrance du certificat qualifié par une autorité accréditée, non recours à un dispositif sécurisé de création de signature - sont secondaires. Bien plus, il nous semble que c'est l'absence d'un autre motif qui mérite d'être soulignée : l'article 5.2 n'interdit en effet pas aux Etats-membres de dénier à une signature électronique toute efficacité juridique ou de refuser de la recevoir comme preuve en justice au motif qu'elle n'est *pas avancée.* La signature électronique - au sens de l'article 2. 1) de la directive – pourrait ainsi se voir privée d'efficacité juridique et ne pas être reçue comme mode de preuve, non pas pour le seul motif qu'elle est électronique, mais parce qu'elle n'assurerait pas des fonctions considérées comme essentielles à la signature par tel ou tel ordre juridique, à savoir les fonctions

d'identification et d'adhésion, voire d'intégrité .

§ 4. Quelques remarques légistiques au sujet de l'article 5

91. Diverses critiques d'ordre légistique peuvent être formulées à l'égard de l'article 5. D'abord, comme nous l'avons dit plus haut, la formulation de l'article 5.1, a), est d'une compréhension malaisée, tandis que la portée du terme "efficacité juridique " de la signature utilisé à l'article 5.2 est controversée.

92. L'on constatera aussi que ce sont les seules signatures électroniques qui cumulent les caractéristiques d'être avancées, de reposer sur un certificat qualifié et d'être créées par un dispositif sécurisé de création de signature qui doivent être assimilées à des signatures manuscrites. A défaut de rencontrer une seule de ces exigences, la signature électronique ne jouira que de la clause de non-discrimination. En d'autres termes, alors que la directive paraît distinguer quatre types de signatures électroniques - "simple", "avancée", "avancée avec certificat qualifié" et "avancée avec certificat qualifié et créée par un dispositif sécurisé" -, seule la dernière (que nous avons qualifiée de " signature électronique parfaite ") est privilégiée quant à ses effets. Ne retenant que deux degrés dans les effets, il eut été préférable, à notre sens, que la directive distingue deux types de signatures seulement - avancée et simple, par exemple -, ce qui n'empêchait pas d'énoncer dans une disposition liminaire ou une annexe les multiples exigences auxquelles devait satisfaire la signature qui bénéficierait de l'assimilation. La formulation de la clause d'assimilation eut ainsi gagné en légèreté et partant en lisibilité.

Section 2. Le nouvel article 1322, al. 2, du Code civil

§ 1er. Le texte

93. La loi du 20 octobre 2000, comme nous l'avons annoncé, a notamment complété l'article 1322 du Code civil d'un nouvel alinéa. Rappelons que l'article 1322, devenant 1322, alinéa 1er, dispose que : "*l'acte sous seing privé, reconnu par celui auquel on l'oppose, ou légalement tenu pour reconnu, a, entre ceux qui l'ont souscrit et entre leurs héritiers et ayants cause, la même foi que l'acte authentique*", lequel, comme le stipule l'article 1319 dudit Code, "*fait pleine foi*" entre ces parties .

94. L'alinéa nouveau de l'article 1322 ajoute que "*peut satisfaire à l'exigence d'une signature, pour l'application du présent article, un ensemble de données électroniques pouvant être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu de*

l'acte".

§ 2. Effets conférés par l'article 1322, al. 2, du Code civil

95. Par cette disposition nouvelle, le législateur belge met, à tout le moins dans le domaine probatoire , en œuvre la clause de non-discrimination de l'article 5.2 de la directive 1999/93 . Il résulte en effet de cette disposition notamment qu'un document électronique signé ne pourra plus être rejeté au seul motif qu'il se présente sous forme électronique.

96. L'opinion a été émise selon laquelle l'article 1322, al. 2, nouveau aurait seulement pour effet de rendre *recevable* la signature électronique, et que le juge serait libre de lui attribuer la valeur probante qu'il souhaite . Nous ne pouvons souscrire à cette interprétation. L'article 1322, al. 2, signifie selon nous que, pour autant que la signature électronique assure les fonctions d'imputabilité et d'intégrité énoncées au texte, le document électronique auquel est lié cette signature accède au statut d'acte sous seing privé. Il en résulte, certes, que ce document est recevable (art. 1341 C. civ.) mais également qu'il fait pleine foi de son contenu (art. 1319, 1320 et 1322 C. civ.). La loi du 20 octobre 2000 n'a, à proprement parler, modifié ni les règles relatives à la recevabilité de l'écrit, ni celles qui concernent sa force probante ; elle a seulement élargi la définition de la signature au sens de l'article 1322 du Code civil et, partant, celle de l'acte sous seing privé, avec les conséquences qui en découlent quant à la recevabilité et la valeur probante. En synthèse, l'article 1322, al. 2, du Code civil intervient au seul stade, préalable à tout autre, de la qualification du mode de preuve .

Cette possibilité de conférer à l'écrit électronique la force probante de l'acte sous seing privé ne dépasse pas, à notre sens, la transposition de la clause européenne de non discrimination. Comme nous l'avons vu, c'est en effet tant la recevabilité comme preuve en justice que l'efficacité juridique qui ne peuvent être déniées aux signatures électroniques pour le seul motif, notamment, qu'elles sont électroniques.

§ 3. Conditions devant être rencontrées

97. Deux conditions doivent être rencontrées pour qu'un ensemble de données électroniques puisse satisfaire à l'exigence d'une signature au sens de l'article 1322 du Code civil. Ces données doivent, d'une part, pouvoir être *imputées* à une personne déterminée et, d'autre part, établir le *maintien de l'intégrité* de l'acte.

La fonction de maintien de l'intégrité n'étonne pas : la doctrine a souvent souligné que c'est la signature qui, dans l'environnement électronique, permet de s'assurer que le contenu d'un document n'a pas été modifié postérieurement à son approbation. En matière de cryptographie asymétrique, toute altération devrait être repérable par la dissemblance qu'elle entraînerait entre la signature numérique déchiffrée et l'empreinte du message lui-même .

Le terme d'*imputabilité*, en revanche, n'apparaît généralement pas dans la définition fonctionnelle que la doctrine donne de la signature et l'on peut regretter son usage qui, traditionnellement, se réfère à l'aptitude d'une personne à rendre compte d'un fait ou d'un acte, spécialement en matière pénale . Toutefois, il ne fait pas de doute que l'imputabilité recouvre ici les deux fonctions traditionnelles de l'identification du signataire et de son adhésion au contenu du message. L'exposé des motifs du premier projet "preuve" est tout à fait univoque à cet égard .

98. La double exigence de l'imputabilité et de l'intégrité nous semble dès lors conforme aux enseignements et aux souhaits de la doctrine. On relèvera seulement que la loi nouvelle ne donne pas une définition fonctionnelle de la signature en général mais se borne à formuler des exigences à l'égard de la signature électronique. Pour D. GOBERT et E. MONTERO , cette approche présente l'avantage de ne pas faire table rase de l'important acquis jurisprudentiel relatif à la signature manuscrite. Cette dernière devra continuer à satisfaire aux exigences mises à jour par le passé , tant en ce qui concerne son contenu (apposition du nom patronymique ou à tout le moins d'un nom par lequel le scripteur révèle habituellement sa personnalité aux tiers) que sa forme (apposition au pied de l'acte, recours à un graphisme particulier...). Les signatures au timbre humide, par griffe ou par cachet restent également bannies, sauf exceptions légales .

Il y a également lieu de s'interroger sur la compatibilité des exigences d'imputabilité et de maintien de l'intégrité au regard de la clause de non discrimination de la directive 1999/93. La signature électronique est en effet définie dans la directive de manière très large; en particulier, elle ne doit pas nécessairement permettre d'imputer le message signé à une personne, ni en assurer l'intégrité. Néanmoins, comme nous l'avons dit, l'article 5.2 de la directive n'interdit pas de discriminer une signature électronique au motif, notamment, qu'elle ne permet pas d'identifier le signataire ou qu'elle n'est pas " liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable ". L'article 1322, al. 2, nouveau de notre Code civil ne nous semble en conséquence pas contraire à la directive sur la signature électronique .

§ 4. Pouvoir d'appréciation du juge du fond

99. En ce qui concerne la formulation du texte nouveau, on aura remarqué que le verbe "pouvoir" est utilisé à deux reprises : "*Peut* satisfaire à l'exigence d'une signature, pour l'application du présent article, un ensemble de données électroniques *pouvant* être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu de l'acte".

L'expression "peut satisfaire" n'emporte pas, selon nous, de conséquences particulières. Elle résulte seulement de l'évolution du texte au fil de sa gestation législative et il nous semble que l'on peut, sans méconnaître la volonté du législateur, la lire comme signifiant "satisfait" .

Quant à la seconde utilisation du verbe pouvoir ("pouvant être imputé"), elle a sans aucun doute pour objet de conférer au juge du fond un pouvoir d'appréciation élargi . Les travaux préparatoires le confirment . Il faut cependant se garder de croire que le juge aurait le pouvoir arbitraire de rejeter pour n'importe quel motif la signature électronique ou de lui conférer le statut qui lui plaît. D'abord le juge doit motiver sa décision au regard des critères d'imputabilité et de maintien de l'intégrité. Ensuite son choix se limite, comme nous l'avons vu, soit à assimiler le document électronique à un acte sous seing privé et dès lors à lui accorder pleine foi, soit à lui refuser cette qualification, avec les conséquences qui en résultent. Le juge ne pourrait, selon nous, sans encourir la censure de la Cour de cassation constater qu'un ensemble de données électroniques assure effectivement les fonctions susdites et refuser néanmoins de recevoir l'acte dont ces données maintiennent l'intégrité ou encore ne le considérer que comme présomption de l'homme. Il ne pourrait non plus, sauf bien sûr lorsque la preuve est libre et à moins de recourir au concept de commencement de preuve par écrit, recevoir une "signature" électronique tout en constatant que les fonctions d'imputabilité et d'intégrité ne sont pas remplies. La marge de manœuvre du juge du fond réside dans la seule appréciation du *degré* d'imputabilité et de garantie d'intégrité dont il se satisfait.

§ 5. Dénégation de signature ?

100. Quelle est enfin, dans l'hypothèse où l'acte sous seing privé se présente sous forme électronique, la place des articles 1323 et 1324 du Code civil, relatifs à la dénégation de signature et à la vérification d'écritures ? *A priori*, ces dispositions continuent à s'appliquer. L'exposé des motifs du premier projet preuve le confirmait

expressément . Néanmoins, il nous semble que dans la pratique cette vérification d'écritures *se confondra* le plus souvent avec l'opération consistant à vérifier l'imputabilité de l'acte. En vidant, éventuellement, au terme d'une expertise, la question si le message qui lui est soumis est bien imputable à l'une des parties au procès, le juge aura *ipso facto* procédé à une vérification d'écritures.

101. Nous rappellerons que si la charge de cette preuve repose sur la partie qui invoque l'acte, celle-ci ne devra pas - et la chose est heureuse - systématiquement apporter cette preuve. Les règles relatives à la preuve sont en effet supplétives si bien que, dans l'hypothèse où l'auteur prétendu de l'acte ne conteste pas sa paternité, fût-ce par son silence, le juge n'a pas à vérifier d'office si la fonction d'imputabilité est remplie (il en va de même en ce qui concerne l'intégrité), pas plus qu'il n'a, face à un *instrumentum*-papier, le droit de procéder à une vérification d'écritures en l'absence de toute dénégation. Bien plus, dans une multitude de procès, de simples copies sont produites en justice sans qu'aucune objection ne soit soulevée ; de même, l'écrit électronique, même non signé, sera pleinement recevable et fera pleine foi tant que son auteur n'aura soulevé aucune exception sur le terrain de la preuve.

§ 6. Quels sont, concrètement, les procédés susceptibles de rencontrer les exigences de l'article 1322, al. 2, du Code civil ?

102. Avant de passer à l'examen de la disposition réglant les effets des signatures électroniques "parfaites", il nous reste à nous interroger sur les procédés de signature qui très concrètement, dans le commerce électronique d'aujourd'hui, pourraient prétendre assurer les fonctions d'imputabilité et de maintien de l'intégrité au sens de l'article 1322, al. 2, du Code civil.

En dehors des signatures biométriques et dynamiques, qui ne se rencontrent apparemment *jamais* dans le commerce sur le *net* pour diverses raisons parmi lesquelles l'absence d'équipement pour leur mise en œuvre, la première candidate nous paraît résolument être la signature à cryptographie asymétrique, dont l'usage reste à l'heure actuelle cantonné à un nombre très restreint d'opérateurs commerciaux mais qui pourrait se généraliser à court ou moyen terme. Certes, lorsque celle-ci satisfera aux conditions de perfection énoncées par la loi du 9 juillet 2001, elle bénéficiera du régime de faveur prévu par l'article 4, § 4, de cette loi ; mais il est précisément des hypothèses où elle ne sera pas « parfaite », par exemple parce que le certificat auquel elle est liée n'est pas « qualifié ». Dans cette hypothèse, cette signature numérique pourra éventuellement satisfaire au test judiciaire « imputabilité-intégrité ».

Pour le reste, une inquisition empirique superficielle révèle que l'identification des partenaires sur le web s'effectue la plupart du temps soit par l'indication du nom de l'expéditeur d'un e-mail, soit par la communication d'un numéro de carte de crédit , soit par l'indication d'un code d'identification qui a été conféré par un vendeur à son client au terme d'une procédure d'enregistrement *on line* .

103. Force est de constater que les modes d'identification précités sont généralement très peu fiables : il est extrêmement aisé pour une personne mal intentionnée de créer une adresse électronique au nom d'autrui ou d'intercepter le numéro de la carte de crédit d'une personne, soit à l'occasion d'une présentation physique de la carte, soit que son titulaire l'ait utilisée sur un site non sécurisé, l'interception supposant alors, certes, certaines compétences informatiques. Dans la majorité des cas, dès lors, le juge sera amené à constater que la fonction d'imputabilité n'est pas assurée de manière suffisamment fiable et qu'il n'y a, partant, ni signature électronique ni acte sous seing privé. En d'autres termes, la contestation de la recevabilité même du document électronique ou la dénégation de signature aboutiront fréquemment et la partie qui invoquait le document électronique sera déboutée de sa demande .

Néanmoins, il ne nous paraît pas exclu que, dans certaines hypothèses, le juge se satisfasse de ces procédés non totalement fiables. On pourrait ainsi songer au cas où l'adresse e-mail ou le code d'identification n'ont été délivrés que moyennant la communication de renseignements précis et personnels à l'intéressé, auxquels un tiers aurait difficilement pu avoir accès. Rappelons en effet que le juge jouit d'un large pouvoir d'appréciation et qu'il peut qualifier de signature électronique un procédé qui assure avec une fiabilité suffisante les fonctions exigées à l'article 1322, al. 2, du Code civil. Nous relèverons toutefois que si pareille identification pourrait être estimée suffisante par le juge, la question de l'intégrité du document produit pourrait, si du moins elle est soulevée, engendrer davantage de difficultés en pratique . Ici peut être pourrait intervenir le concept de commencement de preuve par écrit, pour autant que, à l'estime du juge, le document produit émane bien de la partie contre laquelle il est invoqué et qu'il rende vraisemblable le fait allégué. Resterait alors à trouver des indices propres à compléter adéquatement le commencement de preuve par écrit, de manière à emporter la conviction du magistrat.

Section 3. La loi du 9 juillet 2001 sur les signatures électroniques et les services de certification

§1er. Le principe de l'assimilation "automatique"

104. L'article 4, § 4, de la loi du 9 juillet 2001 s'énonce comme suit : "*Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, est assimilée à une signature manuscrite, qu'elle soit réalisée par une personne physique ou morale*" .

Il résulte de ce texte que lorsque le juge est confronté à une signature électronique "parfaite" , il n'a pas à rechercher si celle-ci assure les fonctions d'imputabilité et de maintien de l'intégrité. Sous réserve d'une procédure en vérification d'écritures , le document auquel est liée ladite signature est considéré de plein droit comme un acte sous seing privé, par principe recevable et faisant pleine foi de ce qui est contenu au titre.

105. La principale difficulté suscitée par cette disposition est, selon nous, de déterminer l'ampleur des vérifications auxquelles doit se livrer le juge pour considérer que la signature électronique est "parfaite". Nous avons vu, en effet, que pour être "avancée" la signature électronique doit remplir quatre fonctions dont deux sont essentielles, que le certificat qualifié doit contenir entre 8 et 10 mentions (annexe I), que les prestataires délivrant de tels certificats doivent satisfaire aux 12 exigences énumérées à l'annexe II et que les dispositifs sécurisés de création de signature doivent rencontrer les 4 exigences de l'annexe III . Précisons qu'il est extrêmement malaisé pour un juge de contrôler le respect de la plupart de ces points. Ainsi, si l'on devait considérer que la présence de chacun des éléments de la signature électronique parfaite doit faire l'objet d'une démonstration par celui qui s'en prévaut, une expertise longue et malaisée s'en suivrait systématiquement et l'assimilation n'aurait d'automatique que le nom. Qui plus est, l'article 4, § 4, mettrait la partie qui invoque la signature dans une position nettement plus défavorable que celle de l'article 1322, al. 2, imposant de démontrer les seules conditions d'imputabilité et de maintien de l'intégrité. Cette interprétation, certes plausible, enlève au système une bonne part de son efficacité .

Selon nous, les vérifications à opérer par le juge devraient être limitées. Leur nature différerait selon que le prestataire de service de certification qui a émis le certificat est accrédité ou non.

106. Si la signature électronique est basée sur un certificat délivré par un prestataire *accrédité*, le juge ne devrait procéder, à notre avis, à aucune autre vérification que celle de cette accréditation et de son maintien (en réservant toujours l'application des articles 1323 et 1324 du Code civil). L'accréditation du prestataire *suppose* en effet que celui-ci ait satisfait aux exigences de l'annexe II, que ses certificats soient conformes à l'annexe I et que les dispositifs de création de signature utilisés répondent à l'annexe III (art. 17,

§1er) . L'accréditation n'est octroyée par l'administration qu'après qu'une entité indépendante ait vérifié le respect des exigences posées par ces diverses annexes (art. 17, § 1er, al. 2) et au terme d'une évaluation que l'expert qui serait mandaté par le juge ne serait peut être pas à même de réaliser. En outre, les prestataires accrédités sont soumis à un contrôle de l'administration et l'accréditation peut être retirée (art. 18 et 20, § 5) lorsque le respect des exigences légales cesse d'être établi .

On pourrait nous objecter que parmi les exigences dont le respect est vérifié par l'entité d'évaluation et sanctionné par l'administration ne figure pas celle que la signature électronique soit "avancée". Il nous semble cependant que lorsque les exigences des annexes I, II et III sont rencontrées, la signature qui sera créée est *nécessairement* avancée .

107. Comme nous l'avons indiqué précédemment, une des modifications majeures apportées au projet de loi par l'amendement dicté par la Commission européenne consistait à permettre à des prestataires non accrédités de délivrer des certificats qualifiés . Il en résulte que l'assimilation réalisée par l'article 4, § 4, de la loi du 9 juillet 2001 s'applique également à des signatures électroniques "parfaites" qui reposent sur des certificats qualifiés délivrés par des prestataires non accrédités. Celui qui se prévaut de l'écrit électronique revêtu d'une telle signature doit-il, dans cette hypothèse, apporter la preuve, le cas échéant par expert, que les exigences des annexes I, II et III ont été rencontrées et que la signature remplit les conditions pour être avancée ? Répétons-le, cette solution, quoique défendable, ne nous paraît pas opportune. Nous pensons au contraire que la partie sur laquelle repose la charge de la preuve pourra recourir à diverses présomptions.

En ce qui concerne le caractère "qualifié" du certificat, le problème doit être nettement relativisé, dès lors que l'annexe I de la directive et de la loi se borne en définitive à édicter les différentes mentions que doit comporter un tel certificat. La vérification du respect de ces exigences est une opération purement matérielle à laquelle le juge peut procéder lui-même sans la moindre difficulté. Quant au caractère "sécurisé" du dispositif de création de signature utilisé - soit sa conformité aux exigences de l'annexe III -, il pourra être établi, *prima facie*, par une attestation délivrée par des organismes compétents désignés par l'administration (art. 7, § 2 de la loi) . Il nous semble également que le juge devra considérer que le respect par le prestataire des exigences stipulées à l'annexe II résulte du contrôle administratif auquel sont soumis ceux-ci en vertu de l'article 20 de la loi . Il sera possible à cet égard de demander à l'administration si le certificateur concerné a récemment fait l'objet d'une mise en demeure de se conformer à la loi, voire d'une procédure judiciaire visant à lui interdire de délivrer des certificats qualifiés. Enfin, dès lors que le respect des annexes I, II et III aura été établi,

principalement par attestations, la signature sera *a fortiori* considérée comme avancée . En conclusion, la preuve de la perfection de la signature électronique pourrait être, dans cette analyse, moins aléatoire qu'il n'y paraît au premier abord.

§ 2. La signature des personnes morales

108. L'article 4, § 4, de la loi du 9 juillet 2001 évoque la possibilité qu'une signature électronique soit réalisée par une *personne morale* . Il pourra s'agir tant d'une personne morale de droit privé que de droit public. Les groupements dénués de personnalité juridique (société de droit commun, sociétés internes ou momentanées,...) sont bien évidemment exclus. Techniquement, le prestataire de service de certification délivrera le certificat au nom de la personne morale elle-même, plutôt qu'au nom d'un de ses organes de représentation.

L'apparence selon laquelle la signature électronique exclurait l'intervention de toute personne physique est trompeuse. Si le certificat est émis au nom de la personne morale, c'est évidemment un être de chair et d'os qui détient le dispositif de création de la signature et qui l'applique aux messages qui doivent être signés. Cette personne physique, que nous dénommerons l'"utilisateur" de la signature, sera normalement un organe de représentation de la personne morale, le gérant unique d'une S.P.R.L. par exemple . Cet utilisateur pourra le cas échéant confier, sous sa propre responsabilité, le support de la clé privée à un mandataire ou programmer un « agent électronique » pour la conclusion automatique d'actes sur le net.

La loi prévoit, en son article 8, § 3, que *"le prestataire de services de certification tient un registre contenant le nom et la qualité de la personne physique qui représente la personne morale et qui fait usage de la signature liée au certificat, de telle manière qu'à chaque utilisation de cette signature, on puisse établir l'identité de la personne physique"*. L'existence de ce registre devra permettre la mise en cause ultérieure de la responsabilité de l'utilisateur, en cas d'excès de pouvoir notamment . En revanche, les tiers ne nous paraissent pas tenus, lorsqu'ils reçoivent un acte électronique signé par la personne morale, de consulter systématiquement ledit registre et de prendre en considération les éventuelles limitations de pouvoirs de l'utilisateur, que celles-ci soient statutaires (répartition de pouvoirs entre administrateurs, par exemple) ou légales (notion de gestion journalière notamment). A leur égard, l'acte est signé par la personne morale elle-même, de sorte que celle-ci est, à tout le moins sur le plan du droit des personnes morales, irrévocablement engagée.

Soulignons enfin que la démarche initiale, soit la demande même de délivrance d'un

certificat, est un acte important qui nécessite des pouvoirs de représentation les plus étendus. Ainsi, pour une société anonyme, le certificat ne devrait être émis qu'à la demande du conseil d'administration ou des administrateurs pouvant se prévaloir d'une clause de double signature, voire d'une personne spécialement mandatée à cet effet par les organes précités. Si la demande n'émane pas de ces derniers, le certificateur devra, sous peine d'engager sa responsabilité, refuser de délivrer le certificat.

§ 3. Quelle place pour la dénégation de signature et la vérification d'écritures ?

109. L'article 4, § 4, de la loi du 9 juillet 2001 réserve de manière expresse la possibilité d'un désaveu de signature. Ainsi, le texte permet au juge, qui aurait dans un premier temps constaté - de la manière que nous avons précédemment, suggérée - que la signature électronique qui lui est présentée est "parfaite", d'ordonner, pour peu que cette signature soit déniée, une vérification d'écritures selon la procédure des articles 883 et suivants du Code judiciaire.

Outre que cette procédure paraît peu adaptée à l'environnement électronique, l'application pure et dure du régime des articles 1323 et suivants du Code civil nous semble, *a priori*, défavorable au développement de l'acte sous seing privé électronique. Elle implique en effet que, conformément au droit commun, la partie qui invoque l'acte a la charge de prouver qu'il émane bien de celle à laquelle il entend l'opposer. Est-il raisonnable de lui imposer ce fardeau dès lors que la signature électronique parfaite présente un degré de fiabilité nettement supérieur à celui d'une signature manuscrite ? Pour répondre à cette question, il n'est pas inopportun de s'interroger sur la notion, au plan civil, de *faux électronique.* C'est, en effet, cette accusation que le signataire apparent lance à l'encontre de la partie qui invoque l'acte.

Le faux électronique nous paraît recouvrir deux situations distinctes. Comme le relève le Conseil d'Etat à la suite d'E. DAVIO , "*le titulaire d'une clé privée est en fait soumis à un double risque, la divulgation accidentelle de sa clé et le déchiffrement frauduleux de celle-ci (…)*". Ces deux risques constituent selon nous les deux hypothèses de faux électronique.

110. La première hypothèse - divulgation accidentelle du dispositif de création de signature - nous paraît devoir être appréciée à la lumière de l'article 19 de la loi du 9 juillet 2001 : "*dès le moment de la création des donnés afférentes à la création de signature, le titulaire du certificat est seul responsable de la confidentialité de ces données. En cas de doute (...) le titulaire est tenu de faire révoquer le certificat*". Il en résulte que, si même le titulaire a désavoué victorieusement sa signature au sens de l'article 1323 et si dès lors, à défaut d'avoir prouvé comme il se doit l'existence du contrat, la partie qui invoquait l'acte doit

être déboutée de sa demande initiale, elle pourra mettre en cause la responsabilité aquilienne du titulaire fautif et lui réclamer une indemnisation équivalente au dommage résultant de la non conclusion du contrat . Si le titulaire du certificat a effectivement demandé la révocation de celui-ci en raison de la perte du support de sa clé privée mais que cette révocation n'a pas été enregistrée dans son annuaire par le certificateur, il est évident que c'est ce dernier qui sera responsable envers le cocontractant débouté . Enfin, si la révocation du certificat a été enregistrée mais que le cocontractant a négligé de vérifier que tel n'était pas le cas, il ne disposera d'aucun recours .

111. Quel sort faut-il réserver à l'autre hypothèse, soit celle dans laquelle le titulaire du certificat invoquerait qu'un tiers est parvenu à déduire sa clé privée de sa clé publique et s'en est ainsi servi à son insu, autrement dit lorsque la fiabilité du mécanisme de création de signature est mise en question ? La partie qui invoque l'acte signé doit-elle dans cette hypothèse, parce qu'elle supporte la charge de la preuve, établir que cet acte de piratage n'a pu avoir lieu ? Ne s'agit-il pas d'une preuve négative indéfinie impossible à apporter ? Et dans ce cas, n'est-ce pas un moyen commode, pour un cocontractant peu scrupuleux, de pouvoir toujours revenir sur son engagement ?

Il nous semble qu'il faille ici raison garder, si l'on ne veut paralyser le système au moment même où il voit le jour. Rien n'interdit au juge de se contenter d'une vraisemblance sérieuse de fiabilité en lieu et place d'une certitude . Il pourra ainsi interroger un expert pour savoir si, à sa connaissance, la clé utilisée a pu, étant précisé l'algorithme auquel elle était liée, être "cassée" moyennant la mise en œuvre de moyens raisonnables . Si la réponse de l'expert est négative, la partie qui invoque l'acte aura, *prima facie*, apporté la preuve qui lui incombait. Il appartiendra alors au signataire apparent de prouver positivement que sa clé a effectivement été cassée, ce qui sera, il faut l'admettre, malaisé .

112. Mentionnons l'existence d'une position plus favorable encore à la signature électronique "parfaite ". Selon D. GOBERT et E. MONTERO, cette signature bénéficie d'une présomption réfragable selon laquelle les fonctions d'imputabilité et d'intégrité sont remplies. Ils en déduisent que " (…) un signataire peut toujours, comme pour la signature manuscrite, contester sa signature puisque la présomption est réfragable, avec néanmoins la différence fondamentale qu'il ne lui suffit plus de désavouer sa signature mais qu'il doit renverser la présomption " .

§ 4. Le champ d'application de l'article 4, § 4, de la loi du 9 juillet 2001

113. La matière de la preuve des obligations n'est de toute évidence pas la seule où

émerge la notion de signature. Au contraire, une grande variété de normes imposent, souvent à peine de nullité, la signature d'un document . La question se pose dès lors si l'équivalence fonctionnelle entre la signature électronique et la signature manuscrite, consacrée par l'article 4, § 4, de la loi du 9 juillet 2001, ne concerne que la question probatoire - et encore relativement au seul acte sous seing privé - ou doit au contraire être étendue en toute matière.

Divers arguments militent en faveur d'une interprétation large. D'abord, la clause d'assimilation de l'article 4, § 4, est formulée en termes généraux . Il nous paraît, à cet égard, que la subsistance des seuls termes "*sans préjudice des articles 1323 et suivants du Code civil*" a pour seul objet de confirmer que la partie à laquelle on oppose un acte sous-seing privé électronique peut toujours dénier sa signature et non d'empêcher l'application du texte en dehors de l'acte sous seing privé. Ensuite, le titre de cette loi et le fait qu'elle ne soit pas insérée dans le Code civil indiquent son émancipation par rapport à la matière de la preuve des obligations. Enfin, et surtout, la directive sur la signature électronique, et plus particulièrement son article 5, n'est, comme nous l'avons indiqué , pas limitée au domaine de la preuve, même si celui-ci constitue son terrain de prédilection. Or, le droit national doit, lorsque ses termes le permettent, être interprété en conformité avec le droit communautaire . En conclusion, face à toute disposition légale exigeant la signature d'un acte, il nous parait que le juge est tenu d'accorder une efficacité juridique audit acte signé électroniquement.

114. Notons encore que, dans au moins deux domaines, des clauses d'assimilation et de non discrimination à portée limitée avaient déjà été introduites avant la loi du 9 juillet 2001. Un arrêté royal du 16 octobre 1998, d'une part, avait permis à la signature électronique de faire une première apparition dans l'ordre juridique belge. Il avait en effet introduit dans la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque-carrefour de la sécurité sociale un article 16 *bis* aux termes duquel "*dans les cas fixés par le Roi, en ce qui concerne l'application de la sécurité sociale, vaut également signature, outre la signature manuscrite, le résultat découlant d'une transformation asymétrique et cryptographique d'un ensemble des données électroniques, pour autant qu'une autorité de certification agréée par la Banque-carrefour ait certifié que cette transformation permet de déterminer, avec un degré de certitude raisonnable, l'identité de l'auteur et son accord avec le contenu de l'ensemble des données, ainsi que l'intégrité de l'ensemble des données*" . L'article 863, al.2, nouveau, du Code judiciaire, d'autre part, dispose que "*l'exigence de la signature n'empêche pas que l'acte puisse également être accompli valablement par télécopie ou par courrier électronique. Si une partie qui y a intérêt le demande, le juge peut toutefois ordonner à l'auteur de l'acte de confirmer sa signature*" . On relèvera le fossé qui sépare ces deux textes, le premier étant orienté d'un point de vue technologique et relativement exigeant, le second très peu formaliste.

On relèvera également, dans le droit fil de notre conception large du champ d'application de la loi du 9 juillet 2001, la possibilité offerte pratiquement depuis le 11 février 2002 par le Ministère des Finances d'introduire des déclarations à la T.V.A. par la voie d'internet (système dit « Intervat ») .

115. Précisons enfin qu'il n'est pas question, en conférant un champ d'application large à l'article 4, § 4, de la loi du 9 juillet 2001, de permettre l'accomplissement par voie électronique de tout acte juridique quelconque. La directive 1999/93/CE concerne en effet la seule signature électronique. Elle n'oblige pas les Etats membres à supprimer d'autres exigences d'ordre formel telles que celles que l'acte soit entièrement rédigé "de la main" de l'auteur de l'acte ou encore en présence d'un officier public. Ainsi, par exemple, les craintes exprimées par le Conseil d'Etat de voir apparaître des testaments olographes électroniques nous paraissent non fondées. De même, le formalisme probatoire de l'article 1326 du Code civil continuerait-il à empêcher qu'un acte de cautionnement, par exemple, puisse être prouvé par un "écrit électronique", sauf, d'évidence, recours au concept de commencement de preuve par écrit, voire à l'aveu ou au serment.

Néanmoins, le maintien de telles exigences devra être remis en question, en raison non de la directive sur la signature électronique mais bien d'une autre directive, d'une envergure nettement plus étendue que la première, la directive 2000/31/CE sur le commerce électronique. Cette question est évoquée au chapitre IV de la présente contribution.

§ 5. Reproduction de la clause de non discrimination

116. Suite à un amendement déposé au Sénat, un cinquième paragraphe, reproduisant presque littéralement la clause de non-discrimination énoncée à l'article 5.2 de la directive , a été ajouté à l'article 4 de la loi du 9 juillet 2001. Aux termes de cet ajout, "*Une signature électronique ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice 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 accrédité de service de certification ou
- qu'elle n'est pas créée par un dispositif sécurisé de création de signature".

117. Si la justification donnée à l'amendement sénatorial nous laisse perplexes, nous pensons toutefois que celui-ci se justifie par la circonstance que l'article 1322, al. 2, du Code civil, dont l'effet est également de supprimer la discrimination antérieure entre signatures manuscrite et électronique, est une disposition dont l'application devait, du vœu du législateur, être restreinte à la matière de la preuve des obligations . Or, c'est en toutes matières que l'article 5.2 de la directive interdit les discriminations .

118. Si nous approuvons l'insertion, dans la loi du 9 juillet 2001, d'une clause de non discrimination à portée générale, la formulation de celle-ci nous incite à émettre quelques observations.

Premièrement, l'on peut regretter que cette disposition vise, outre l'efficacité juridique des signatures électroniques, leur recevabilité comme preuve en justice. Cette question est en effet épuisée par l'article 1322, al. 2, du Code civil, quelle que soit d'ailleurs l'interprétation que l'on donne à ce dernier .

Deuxièmement, la formulation négative du texte, justifiée dans une directive qui s'adresse aux Etats-législateurs en leur enjoignant de supprimer certaines discriminations pouvant figurer dans leur ordre juridique interne, ne laisse pas de susciter des interrogations lorsqu'elle apparaît dans la loi elle-même.

L'injonction négative est, certes, partiellement justifiée dès lors que parmi les destinataires du texte figurent les pouvoirs normatifs inférieurs. Si ceux-ci adoptaient des dispositions comportant une exigence de signature, ils devraient veiller à éviter les discriminations interdites par l'article 4, § 5, de la loi du 9 juillet 2001. Rappelons toutefois qu'aux termes de l'article 4, § 3, « *le Roi peut, par arrêté délibéré en Conseil des ministres, soumettre l'usage des signatures électroniques dans le secteur public à des exigences supplémentaires éventuelles* » . Une disposition réglementaire ayant la même portée que l'article 16 bis de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque-carrefour de la sécurité sociale pourrait par contre s'avérer illégale si elle était appelée à régir des relations de pur droit privé.

119. En revanche, à l'égard des particuliers, d'une part, du juge, d'autre part, cette simple reproduction du vœu européen présente, nous semble-t-il, des difficultés d'application . La clause belge de non discrimination interdit certes au juge de considérer le document comme non valide au seul motif que la signature dont ce document est revêtu se présente sous la forme électronique ou, par exemple, n'a pas été réalisée sur base d'un certificat qualifié. Mais ce magistrat ne dispose en réalité d'aucun *critère positif* à l'aune duquel apprécier la validité de la signature électronique. Dans le silence de la loi, il nous paraît que les critères d'identification, d'adhésion et de maintien

de l'intégrité dégagés par la doctrine fonctionnaliste et consacrés en matière d'acte sous seing privé par l'article 1322, al. 2, du Code civil, pourraient être généralisés .

De même, en l'absence d'indication et dans la loi et dans les travaux parlementaires, la clause de non discrimination ne nous paraît pas devoir s'interpréter comme interdisant désormais aux particuliers d'exclure conventionnellement l'usage, dans leur relations réciproques, de signatures électroniques ou d'exiger que celles-ci reposent, par exemple, sur un certificat émis par un certificateur accrédité.

CHAPITRE IV. EN GUISE DE CONCLUSION : LA DIRECTIVE SUR LE COMMERCE ÉLECTRONIQUE APPELLE UNE NOUVELLE RÉVISION DU DROIT DE LA PREUVE

Section 1. La directive sur le commerce électronique : aperçu

120. La directive du 8 juin 2000 sur le commerce électronique ne constitue pas l'objet spécifique de notre article mais n'y est pas non plus étrangère, dès lors qu'elle appelle, parmi bien d'autres réformes, de nouvelles modifications des dispositions légales sur la preuve. Précisons dès à présent que la date prévue pour sa transposition était fixée au 17 janvier 2002 (art. 22). A l'heure actuelle existe un avant-projet de loi « sur certains aspects juridiques des services de la société de l'information », disponible sur le site du Ministère des Affaires économiques .

L'objet de la directive sur le commerce électronique est très vaste puisque, en vue d'assurer la libre circulation des services de la société de l'information entre les Etats membres (art. 1.1), elle rapproche les dispositions nationales applicables à ces services qui concernent respectivement le marché intérieur, l'établissement des prestataires, les communications commerciales, les contrats par voie électronique, la responsabilité des intermédiaires, les codes de conduite, le règlement extrajudiciaire des litiges et la coopération entre Etats membres (art. 1.2).

121. Aux termes de l'article 9.1 de la directive, *"les États membres veillent à ce que leur système juridique rende possible la conclusion des contrats par voie électronique. Les États membres veillent notamment à ce que le régime juridique applicable au processus contractuel ne fasse pas obstacle à l'utilisation des contrats électroniques ni ne conduise à priver d'effet et de validité juridiques de tels contrats pour le motif qu'ils sont passés par voie électronique"*. La portée de cet article est précisée par le considérant n° 34 : " *Chaque Etat membre doit ajuster sa législation qui contient des exigences, notamment de forme, susceptibles de gêner le recours à des contrats par voie électronique. Il convient que l'examen des législations nécessitant*

cet ajustement se fasse systématiquement et porte sur l'ensemble des étapes et des actes nécessaires au processus contractuel, y compris l'archivage du contrat. Il convient que le résultat de cet ajustement soit de rendre réalisables les contrats conclus par voie électronique (…)".

Il convient cependant de noter que le second paragraphe de l'article 9 de la directive autorise les États membres à maintenir, pour quatre catégories de contrats, des dispositions faisant obstacle à leur conclusion par voie électronique. Il s'agit :
a) des contrats qui créent ou transfèrent des droits sur des biens immobiliers, à l'exception des droits de location;
b) des contrats pour lesquels la loi requiert l'intervention des tribunaux, des autorités publiques ou de professions exerçant une autorité publique;
c) des contrats de sûretés et garanties fournis par des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle ou commerciale;
d) des contrats relevant du droit de la famille ou du droit des successions.

122. Dans l'avant-projet de loi précité, trois mesures ont été adoptées afin d'assurer le respect de l'article 9, § 1er, de la directive. D'abord, une clause consacre, de façon tout à fait générale, la théorie des équivalents fonctionnels en ces termes : « *Toute exigence légale ou réglementaire de forme relative au processus contractuel est réputée satisfaite à l'égard d'un contrat par voie électronique lorsque les qualités fonctionnelles de cette exigence sont préservées* » (art. 17, § 1er). Ensuite, le paragraphe 2 fait une application de cette théorie à l'égard de trois concepts récurrents en matière de formalisme, à savoir l'écrit, la signature – en se référant pour celle-ci, d'évidence, à l'article 1322, al. 2, du Code civil et à l'article 4, § 4, de la loi du 9 juillet 2001 - et la mention écrite de la main. Enfin, le Roi est habilité, dans un délai donné, à « *adapter toute disposition législative ou réglementaire qui constituerait un obstacle à la conclusion de contrats par voie électronique* » (art. 17, § 3).

Section 2. La directive sur le commerce électronique et le concept d'écrit

123. La première question à envisager est certainement celle de la nécessité d'insérer dans l'arsenal législatif belge une définition de l'écrit. C'est que, lors de la récente révision du droit de la preuve, notre législateur s'est limité à retoucher la notion de la signature dans le cadre de l'acte sous seing privé, cette retouche s'avérant indispensable en raison de la définition formaliste donnée, *in tempore non suspecto*, de la signature par la Cour de cassation . Or, l'acte sous seing privé, rappelons-le, consiste en un écrit signé. En conséquence, certains auteurs, ne se satisfaisant point de la voie interprétative fonctionnelle de la notion d'écrit , requièrent une définition légale de celui-ci. A notre

sens, la circonstance que le législateur n'ait pas jugé nécessaire d'introduire également une définition fonctionnelle de l'écrit indique qu'une telle définition est par lui *supposée*. Dans le cas contraire, en effet, l'introduction de la signature électronique serait totalement inefficiente. A quoi bon préciser que la signature que doit revêtir l'écrit pour accéder au statut d'acte sous seing privé peut être électronique si l'écrit lui-même ne peut présenter une telle nature ? Le postulat de rationalité du législateur implique donc que ce législateur ait retenu, dans le cadre de la récente réforme, une conception fonctionnelle de l'écrit.

124. Au delà, lorsque la loi exige à titre de preuve, par dérogation au système de l'article 1341 du Code civil, un acte sous seing privé même pour un acte juridique de moins de 375 euros, cet écrit pourrait aussi se présenter sous la forme électronique, pour autant que les conditions énoncées à l'article 1322, al. 2, du Code civil – ou à l'article 4, § 4, de la loi du 9 juillet 2001 - soient satisfaites. Ainsi, en va-t-il, par exemple, pour la preuve du contrat d'assurance terrestre régie par l'article 10, § 1er, de la loi du 25 juin 1992 .

125. Mais il nous semble aussi que la cohésion impose que la notion d'écrit ne varie pas selon que celui-ci est exigé *ad probationem* ou *ad validitatem.* Dès lors, quand un texte subordonne la validité d'un *negotium* quelconque à sa constatation par *écrit*, ce dernier pourrait, dans l'état actuel des textes déjà, prendre la forme électronique. Ainsi, pourrait-on admettre que se conclue par internet un contrat d'intermédiaire de voyage, la législation relative à celui-ci, à savoir la loi du 16 février 1994, spécialement en son article 23, exigeant, sans autre précision, un contrat écrit contenant certaines mentions certes obligatoires mais non point manuscrites.

Cependant, le point névralgique de l'adaptation en droit belge de l'article 9 de la directive sur le commerce électronique est probablement de déterminer ce que telle ou telle disposition légale vise par l'emploi du mot " écrit ", à savoir l'écrit dans sa conception fonctionnelle d'acte sous seing privé ou l'écrit papier, ce dernier présentant peut-être aux yeux du législateur, du moins quand il s'agit de conditionner la validité même du contrat, des vertus supplémentaires. Plus fondamentalement encore, l'idée n'est-elle pas que lorsque le législateur impose un écrit pour la formation même du contrat, dans le but non seulement de susciter la réflexion de la partie protégée au moment de la conclusion du contrat mais encore de lui permettre d'accéder, ultérieurement, aux informations utiles, il désire, idéalement, que chacune des parties dispose du même document, quel que soit son support, signé par toutes les parties ou du moins par la partie à laquelle on voudrait l'opposer. Cette idée nous paraît d'ailleurs corroborée par le fait que, le plus souvent, le législateur impose expressément qu'un exemplaire dudit contrat soit remis à la partie cocontractante dite faible . On rejoint ici il

est vrai, ne fût-ce que partiellement, la problématique du support durable, concept affleurant dans diverses réglementations européennes ou belges, tel l'article 79 de la loi du 14 juillet 1991 sur les pratiques du commerce - issu de la transposition de l'article 5 de la directive 97/7 - dans le cadre de la réglementation des contrats à distance à l'égard des consommateurs .

126. Quoiqu'il en soit, on observera que le gouvernement, comme l'avait préconisé D. MOUGENOT pour des raisons de sécurité juridique, semble avoir opté pour l'insertion d'un texte exprès consacrant la notion d'écrit. L'article 17, § 2, de l'avant-projet « commerce électronique » énonce en effet : « *L'exigence d'un écrit est satisfaite par une suite de signes intelligibles et accessibles pour être consultés ultérieurement, quels que soient leur support et leurs modalités de transmission* ».

Section 3. La directive sur le commerce électronique et les autres exigences d'ordre formel, en particulier les articles 1325 et 1326 du Code civil

127. Le droit belge impose à l'égard de nombreux contrats des exigences de forme qui ne paraissent en aucun cas pouvoir être respectées en cas de conclusion par voie télématique. Il en va ainsi, dès lors que le législateur n'a, à ce jour, point encore consacré le concept d'acte authentique électronique , des dispositions qui exigent que certains contrats soient constatés dans la forme authentique, soit pour leur validité (tels, par exemple, l'article 66 du Code des sociétés ou l'article 76 de la loi hypothécaire), soit pour leur opposabilité (art. 2 de la loi hypothécaire). De nombreux contrats de consommation figurent également parmi les conventions qui ne peuvent, dans l'état actuel des textes, être conclues par voie électronique : l'exigence de mentions manuscrites (par exemple, l'article 17 de la loi du 12 juin 1991 relative au crédit à la consommation ou l'article 7, § 2, de la récente loi du 11 avril 1999 relative aux contrats portant sur l'acquisition d'un droit d'utilisation d'immeubles à temps partagé) s'y oppose indiscutablement .

128. On rappellera toutefois, que le paragraphe 2 de l'article 9 de la directive sur le commerce électronique autorise exceptionnellement les Etats membres pour certaines catégories de contrats, et notamment ceux pour lesquels la loi requiert l'intervention des tribunaux, des autorités publiques ou de professions exerçant une autorité publique (art. 9, § 2, b), à maintenir des exigences rendant impossible la conclusion desdits contrats par voie électronique . Précisons toutefois que le maintien par les Etats membres de l'exception prévue sous ce point b de l'article 9, § 2, doit faire l'objet d'une justification envers la Commission, laquelle justification doit être renouvelée tous les cinq ans. A cet égard, il sera aisé de justifier, par exemple, l'impossibilité de conclure un "cybermariage". En revanche, l'on peut s'interroger sur la pertinence des motifs qui justifient

l'impossibilité actuelle de conclure un acte notarié par internet alors même que chacune des parties au contrat serait mise en présence physique de son notaire respectif .

On aura relevé, par ailleurs, que les contrats de consommation ne figurent pas tels quels parmi les exceptions énumérées par l'article 9.2, en dehors des contrats de sûretés et garanties. Toutefois, à maintes reprises, la directive, en ses articles ou considérants , évoque la protection des consommateurs. Ainsi, le considérant 65 énonce que la Commission étudiera la mesure dans laquelle les règles de protection des consommateurs existantes fournissent une protection insuffisante au regard de la société de l'information et identifiera, le cas échéant, les lacunes de cette législation et les aspects pour lesquels des mesures additionnelles pourraient s'avérer nécessaires. En droit belge, il conviendra que le législateur s'interroge sur la façon de modifier des dispositions telles que l'article 17, déjà mentionné, de la loi sur le crédit à la consommation. Il serait prudent, à cet égard, d'attendre la version définitive de la directive européenne relative à la commercialisation à distance des services financiers auprès des consommateurs. Nous rappellerons au passage qu'il n'est pas toujours aisé de déterminer si les exigences formelles du droit de la consommation relèvent d'un formalisme de validité du *negotium* ou d'un formalisme probatoire accru.

129. En matière probatoire, différentes dispositions nous paraissent certainement devoir être remises sur le métier. Au premier rang de celles-ci figure l'article 1326 du Code civil . L'exigence que l'acte constatant un engagement unilatéral soit écrit en entier *de la main* de la partie qui s'engage ou, à tout le moins, qu'un bon ou un approuvé ait été écrit de la sorte, est manifestement contraire à l'article 9 de la directive sur le commerce électronique . On peut songer à supprimer cette contrariété en substituant aux termes "de sa main" ceux de "par lui même", comme ce fut le cas en France . Ainsi, dans le cas d'un contrat unilatéral conclu sur un site web, l'internaute ne pourrait s'engager en cliquant sur une simple icône destinée à manifester son consentement mais devrait, outre l'apposition de sa signature électronique, inscrire au moyen de son clavier, dans un emplacement réservé à cet effet, les mentions traditionnelles du "bon pour" ou de l'"approuvé". L'avant-projet « commerce électronique » prévoit, quant à lui, au paragraphe 3 de son article 17, que « *l'exigence d'une mention écrite de la main de celui qui s'oblige peut être satisfaite par tout procédé garantissant que la mention émane de ce dernier* ».

130. Il convient également de s'interroger sur l'application dans le commerce électronique de l'article 1325 du Code civil suivant lequel les actes sous seing privé qui contiennent des conventions synallagmatiques ne sont valables qu'autant qu'ils auront été faits en autant d'originaux qu'il y a de parties ayant un intérêt distinct, chaque original devant, en outre, contenir la mention du nombre d'originaux réalisés.

L'on peut, avec D. GOBERT et E. MONTERO, se demander ce que pourrait être, dans l'environnement électronique, un *original*. Traditionnellement, l'original est opposé à la copie en ce que le premier, contrairement à la seconde, est revêtu d'une signature . Lorsque la signature est reproduite par un procédé quelconque et non tracée directement sur le support par son auteur, il s'agit aussi d'une copie. Dans l'environnement électronique, il faudra considérer, *mutatis mutandis*, que la copie est le message en clair séparé de sa signature, tandis que l'on est face à un original chaque fois qu'est présentée, outre le message lui-même, sa signature électronique. La cryptographie asymétrique présente ainsi la particularité de permettre la reproduction à l'infini d'un acte *en original.* Il suffit à cet effet que la "signature", autrement dit le message crypté par application de la clé privée, soit elle aussi reproduite .

131. D. GOBERT et E. MONTERO, qui aboutissent à des conclusions similaires , ajoutent, en substance, que la formalité de l'article 1325 du Code civil devient, s'agissant d'un écrit électronique signé numériquement, inutile dès lors que la *ratio legis* du texte est nécessairement accomplie : "le but de cette formalité est de permettre à chacune des parties de disposer d'une preuve du contrat. Il est aussi de faciliter une comparaison, de manière à déceler les éventuelles altérations unilatérales de l'*instrumentum*. Cette comparaison, il est vrai, devient inutile à partir du moment où le document ne peut être modifié sans le concours de l'autre partie" . Aussi les auteurs estiment-ils que la règle des originaux multiples perd désormais de son intérêt.

Il nous semble que si le second objectif assigné à l'article 1325 du Code civil est effectivement rencontré, il n'en va pas de même du premier : la signature électronique ne garantit en rien que chacune des parties contractantes dispose d'une preuve du contrat. En outre, la seule circonstance que la *ratio legis* d'un texte soit respectée n'implique pas *ipso facto* que celui-ci sera déclaré inapplicable par les cours et tribunaux.

132. C'est pourquoi nous préférons solutionner le problème de la "règle du double" par un recours aux exceptions traditionnellement admises en la matière. Il est, en effet, unanimement reconnu que lorsqu'un contrat est conclu par échange de lettres missives, l'article 1325 du Code civil est inapplicable . Il n'y a pas de motif pour qu'il n'en aille pas de même dans l'hypothèse d'un échange de courriers électroniques signés par leurs expéditeurs .

Plus délicate est l'hypothèse du contrat conclu par l'internaute, complétant et signant une page web d'un vendeur . L'acheteur n'a en effet pas toujours, pour peu qu'il y songe, la possibilité de conserver ne fût-ce qu'une impression papier de la commande dûment complétée et, encore moins souvent, celle de télécharger ladite page web sur la

mémoire de son ordinateur. Deux ébauches de solution nous paraissent cependant envisageables.

D'abord, il serait possible que le vendeur ait recours à un tiers chargé de l'archivage des contrats et que l'acheteur soit informé de la possibilité de consulter à tout moment et sans frais le contrat par lui conclu. Dans cette hypothèse, il nous semble que l'exception traditionnelle du dépôt de l'original entre les mains d'un tiers dispenserait les parties de se plier aux exigences de l'article 1325 du Code civil. Ce service d'archivage est généralement presté par les tiers certificateurs eux-mêmes, qui diversifient ainsi leurs activités et apportent une plus-value au commerce électronique. Il est évidemment hautement souhaitable que le recours à ce type de service se propage rapidement .

En l'absence d'archivage, l'exception relative aux lettres missives pourrait peut-être également être invoquée. En effet, même lorsque le contrat est conclu sur un site web, on constate généralement que la conclusion donne lieu à un échange de documents. La page web est en effet complétée par l'acheteur - ou, plus généralement, le client - avant d'être envoyée au vendeur ou prestataire de service, qui peut ainsi la stocker, tandis que l'usage se répand, pour le vendeur, d'adresser à l'acheteur un accusé de réception. Si la page complétée et l'accusé sont l'un et l'autre signés, ce qui devrait être le cas à court ou moyen terme, l'opération pourrait, nous semble-t-il, être assimilée à un échange de lettres missives formant ensemble le contrat . Nous rejoignons ainsi R. MOUGENOT lorsqu'il affirme que dans l'optique d'une modernisation du système de preuves, l'on pourrait songer à l'abandon de l'article 1325, l'écrit multilatéral pouvant être remplacé par un système d'accusés de réception .

Observons encore qu'il est traditionnellement admis que la formalité des originaux multiples dont question à l'article 1325 du Code civil n'est pas applicable lorsqu'il s'agit de prouver contre un commerçant .

Enfin, s'agissant d'un formalisme de preuve rappelons-le, l'acte, entendons l'*instrumentum*, nul pour non respect de l'article 1325 du Code civil ou de l'article 1326 du même Code pourra, si du moins il remplit les conditions énoncées par l'article 1347 du Code civil , être utilisé à titre de commencement de preuve par écrit, ouvrant dès lors la voie aux témoignages et présomptions.

Pascale Lecocq et Bernard Vanbrabant, mars 2002.