Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Preuve et certification sur Internet

Davio, Etienne

Published in:
Revue de droit commercial belge

Publication date:
1997

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Davio, E 1997, 'Preuve et certification sur Internet', *Revue de droit commercial belge*, vol. 11, pp. 660-670.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 02. May. 2026

Preuve et certification sur Internet[1]

Chapitre 1: La preuve sur Internet: enjeux et difficultés

La réflexion sur la preuve par des moyens électroniques n'est pas neuve et pourtant. Les interrogations relatives à l'admissibilité de tel ou tel document informatisé comme élément de preuve, à la valeur de tel procédé de signature semblent retrouver toute leur vitalité dès le moment où ces interrogations sont posées dans le contexte Internet. Après avoir identifié, dans le présent chapitre, les enjeux et difficultés liés à la preuve sur Internet, nous étudierons au deuxième chapitre les principes et concepts de base de l'actuel régime juridique de la preuve. Dans un troisième chapitre nous envisagerons les voies possibles de solutions pour permettre la preuve informatique. Dans un quatrième chapitre nous concentrerons notre attention sur un problème particulièrement crucial dans les réseaux ouverts, à savoir l'identification du cocontractant.

Section Internet: réseau ouvert

Le réseau Internet est un réseau ouvert. La réflexion relative à la preuve informatique n'avait pas intégré cette donnée. Ainsi la "signature" reconnue, par la jurisprudence, à l'occasion de la présentation d'une carte et de la composition d'un code secret se révèle fort éloignée de la notion de signature électronique telle qu'elle se développe aujourd'hui.[2]

En quoi un réseau ouvert se différencie-t-il d'un réseau fermé?[3] Les critères de distinction varient.

Le critère premier de distinction se fonde sur le fonctionnement technique du réseau et, en particulier, sur la nature des contrôles exercés par les entités chargées d'administrer le réseau.

Ainsi, H. Perrit définit un système fermé comme un système dans lequel tout le contenu, les interfaces de communication, le stockage d'information, la réalisation de software et la sécurité est contrôlée par une entité unique: une société gérant un réseau local[4] ou un babillard électronique.[5] En présence d'un tel réseau, l'opérateur du système peut contrôler la population des utilisateurs.[6]

Par opposition, un système ouvert est un système dans lequel aucune entité administrative ou légale ne contrôle les activités de communication, le stockage d'information ou les utilisateurs.

Le réseau des réseaux, Internet, répond parfaitement à cette idée. "La structure décentralisée de l'Internet, à l'origine conçue pour résister à toute tentative de destruction exclut virtuellement toute possibilité de contrôle par une autorité unique qui prétendrait exercer la maîtrise du réseau".[7] L'absence de contrôle centralisé (et, qui plus est, son impossibilité radicale), constitue certainement une donnée majeure pour le juriste.

Un second critère retenu consiste à désigner l'environnement ouvert comme un environnement "où plusieurs intervenants étrangers et inconnus l'un à l'autre peuvent jouer".[8] Ce qui est caractéristique des réseaux ouverts, c'est que, d'emblée, des internautes, qui ne se connaissent pas, souhaitent entrer en relation contractuelle dans un contexte électronique. A l'opposé "l'Edi sur les réseaux fermés présuppose une relation commerciale préexistante qui donne lieu à la possibilité d'encadrer les transactions par une convention entre les intervenants".[9] Il faudra mesurer la portée d'une telle donnée lors de l'étude des conventions d'interchange.

Ce double degré d'ouverture, technique, d'une part, juridique, d'autre part, pour fascinant qu'il soit, ne constitue-t-il pas une fin de non-recevoir à la conclusion d'actes juridiques?

C'est ici qu'apparaît la notion de sécurité.

[1] Le présent article trouve, pour l'essentiel, son origine dans un exposé fait lors du colloque EFE "Internet, quel cadre légal et contractuel?", les 25 et 26 mars 1997, à Bruxelles.

[2] Sur cette question voy. notre article "Questions de certification, signature et cryptographie", in *Internet face au droit*, Cahier du Centre de Recherches Informatique et Droit, n° 12, Bruxelles, Story Scientia, 1997, pp. 71-73.

[3] S'agissant de définir les réseaux, on peut identifier deux composantes. D'une part, la composante physique, c'est-à-dire les raccordements entre les différents terminaux de tous ceux qui souhaitent entrer en communication. D'autre part, la composante intentionnelle: le réseau est une réunion de personnes. Dans cette ligne, le réseau apparaît comme l'ensemble des usagers interconnectés. Sur cette question voy. P. Trudel, "Introduction au droit du commerce électronique sur l'Internet", *Revue du Barreau (Canada)*, 1995, pp. 521-551 citant Allen S. Hammond, "Private Networks, Public Speech: Constitutional Speech Dimension of Access to Private Networks", [1994] 55, *University of Pittsburg Law Review*, 1085, 1095.

[4] L.A.N.: Local area network

[5] B.B.S.: Bulletin board services

[6] Perrit, H., "Security in open networks: maintaining confidentiality and getting paid", http://ming.law.vill.edu/chron/articles/pbisecu6.htm

[7] Trudel, P., *op. cit.*, pp. 521-551, qui constate que, dans le contexte des réseaux ouverts, les possibilités effectives de contrôle sont aux mains de ceux qui administrent les différents sites entre lesquels des interconnexions existent ou sont possibles.

[8] Poullet, Y., "Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve", in *Le droit des affaires en évolution. Le juriste face à l'invasion informatique*, Colloque ABJE, 24 octobre 1996, Bruxelles, Bruylant, Anvers, Kluwer, 1996, p. 48. A noter que cette caractéristique est intimement liée à la configuration technique des réseaux. Il faut cependant constater que cette caractéristique n'est pas exclusive à la communication au travers des réseaux ouverts.

[9] Masse, D.G., "Le cadre juridique en droit civil québécois des transactions sur l'inforoute", in actes du colloque *L'autoroute de l'information: convergence du droit et de la technologie*, novembre 1995, p. 7. Accessible à l'adresse : http://www.chait-amyot.ca/docs/aqd95.htm

Kluwer Éditions Juridiques Belgique

Section 2: La sécurité à la base du contrat

Tout réseau, pour être support à la transaction, a besoin d'un certain niveau de sécurité. En fait, il ne peut être question de transactions commerciales dans un réseau ouvert qui ne se serait pas donné les moyens de sécurité pour gérer les risques inhérents à son ouverture.[10]

A ces risques correspondent des réponses techniques[11], lesquelles ne peuvent trouver leur pleine mesure que si elles sont couplées à une véritable sécurité juridique.

D'un point de vue juridique, la notion de sécurité se réfère, essentiellement, à la possibilité:
1° d'authentifier l'utilisateur du système tant pour éviter les usurpations d'identité que pour assurer la non-répudiation d'une volonté exprimée;
2° d'assurer l'intégrité du message tant à l'égard de modifications accidentelles que malveillantes;
3° de garder des traces de la transaction pour valoir preuve.[12]

A la vue de cette énumération, on se rend compte que les questions de preuve et d'authentification sont centrales pour qui souhaite trouver dans Internet un lieu propice à la conclusion d'actes juridiques.

Chapitre 2: Le régime juridique de la preuve

Section 1: Fondements d'un régime de preuve réglementée

En matière civile, l'article 1341 du Code civil fixe le principe de la prééminence de l'écrit. La preuve des actes juridiques est réglementée: au delà de 15 000 francs seul un écrit signé peut être rapporté à titre de preuve et tous autres moyens de preuve, (témoignages, présomptions), ne sont pas admissibles. "Dès que l'intérêt en jeu dépasse une certaine somme, il faut préconstituer la preuve en rédigeant un écrit".[13]

Le législateur exprime une préférence marquée pour la preuve établie avant le litige. "Seule la préconstitution d'un document écrit permet, à la partie sur qui pèse le risque de la preuve, d'écarter le danger. En outre et surtout, même quand la preuve est libre, il faut emporter la conviction du juge et il est sage de s'en ménager à l'avance les moyens".[14]

Pourquoi l'écrit? Dans un système de preuve réglementée "admissibilité et fiabilité d'un moyen de preuve devraient être deux notions étroitement dépendantes".[15] Il en va ainsi pour l'écrit classique, le document papier revêtu d'une signature manuscrite. La faveur dont il fait l'objet peut s'expliquer par la haute valeur sécuritaire de l'écrit caractérisé par sa permanence, par une signature dans laquelle l'auteur se reconnaît et parce qu'il apparaît comme un support efficace à l'information des parties.[16]

Section 2: Lorsque la preuve est libre.

§1. Cas où la preuve est libre

a) Transactions inférieures à 15 000 francs

L'exigence d'un écrit signé n'est pas requise pour les affaires de petite valeur pour lesquelles on a estimé qu'il eut été excessif d'imposer le formalisme de l'écrit.[17] Le montant actuellement retenu est de 15 000 francs. On peut dès à présent souligner que le législateur prend en compte des critères économiques et gère le risque.

b) Faits juridiques

On oppose acte juridique et fait juridique. L'acte juridique est volontaire et il est posé en vue de produire un effet de droit. A l'opposé, le fait juridique est un événement, volontaire ou non, auquel la loi attache des conséquences juridiques, sans que ces conséquences juridiques aient été recherchées par l'auteur.

La preuve des faits juridiques est libre. Cela n'évacue pas pour autant les difficultés. Tout d'abord, la qualification d'un événement en acte ou fait juridique peut être délicate. Ensuite, la preuve libre laisse entier le problème d'emporter la conviction du juge (cf. §2).

c) Lorsqu'il s'agit de prouver à l'encontre d'un commerçant

En matière commerciale, la preuve est libre. Cette solution est inscrite à l'article 25, al. 1er du Code de Commerce qui dispose que "les engagements commerciaux pourront être constatés par la preuve testimoniale, dans tous les cas où le tribunal croira devoir l'admettre, sauf les ex-

[10] Masse, D.G., *op. cit.*, p. 6 qui constate "qu'afin d'être propice au commerce, une forme de communication doit fournir un moyen, jugé acceptable par la communauté commerciale, d'assurer que la certitude soit suffisante pour justifier le risque d'y transiger".
[11] Hubin, J., *La sécurité informatique*, Cahier du Crid, n° 14, à paraître, Bruxelles, Story Scientia, 1997 qui définit la sécurité informatique comme la gestion des techniques physiques, logiques et humaines destinées à protéger, contre les accidents, les erreurs et les comportements malicieux, les êtres humains qui confient certaines valeurs à des systèmes informatiques fonctionnant dans un certain environnement.
[12] Amory, B., Schauss, M., "La formation des contrats par des moyens électroniques", *Droit de l'informatique*, 1987/4, p. 207.
[13] Verheyden-Jeanmart, N., *Droit de la preuve*, Précis de la faculté de Droit de l'Université Catholique de Louvain, Bruxelles, Larcier, 1991, p. 151.
[14] Larrieu, J. "Les nouveaux moyens de preuve: pour ou contre l'identification des documents informatiques à des écrits sous seing privé", *Cahiers Lamy Droit de l'informatique*, 1988, H/88, p. 8.
[15] Larrieu, J., *op. cit.*, p. 9
[16] Poullet, Y., *op. cit.*, p. 42.
[17] Verheyden-Jeanmart, N., *op. cit.*, p. 153.

ceptions établies pour les particuliers".[18] Si d'un point de vue théorique, c'est la nature de l'acte, commercial ou non, qui détermine le régime de preuve applicable, d'un point de vue pratique, il apparaît que la qualité de la personne à l'égard de laquelle la preuve doit être rapportée est très importante pour la détermination du régime de la preuve.[19]

De manière quelque peu schématique, cela signifie que chaque fois qu'il s'agit de prouver contre un commerçant, on appliquera le régime de la preuve libre. Par contre lorsqu'un commerçant entend prouver contre un non-commerçant, c'est le principe de la preuve réglementée qui s'appliquera.[20]

§2. Admissibilité et valeur probante[21]

Le régime de la preuve livre signifie que le législateur n'est pas intervenu pour spécifier à l'avance les moyens de preuve admissibles. En conséquence, chacune des parties peut apporter à l'appui de ce qu'elle avance tout élément de nature à prouver. Se pose, alors, la question de la valeur probante de l'élément de preuve. Sur cette question précise, le régime de la preuve libre ne nous apporte aucune réponse en ce qu'il "laisse entière la charge de convaincre le juge de la valeur de la preuve électronique".[22] Nous reviendrons dans notre prochaine section sur l'intérêt de la preuve libre en matière informatique.

Chapitre 3: La preuve informatique

Section Informatique et preuve libre

En prolongeant la réflexion entreprise précédemment sur le régime de la preuve libre, on doit s'interroger sur le bénéfice que les parties à un contrat réalisé par des moyens électroniques peuvent obtenir du régime de la preuve libre, si tant est qu'il soit d'application.

L'intérêt du régime de la preuve libre est à trouver dans l'absence de conditions d'admissibilité des preuves. Ainsi divers documents ou supports informatiques pourraient être pris en considération par le juge, de même des témoignages ou des présomptions peuvent être retenus.[23]

Dès lors que le régime de la liberté de preuve évacue la question de l'admissibilité, on doit s'interroger sur la nature des documents qui pourraient être produits et s'interroger sur leur valeur probante. Ainsi, l'impression d'une page Web contenant une offre formulée par un commerçant pourrait être prise en compte par le juge, l'engagement contractuel d'une partie pour un montant inférieur à 15 000 francs pourrait semblablement être prouvé à l'aide de la production d'un courrier électronique. La valeur de preuve de ces éléments reste sur le plan technique l'objet de bien des interrogations, interrogations qui vont influencer le juge dans l'appréciation de la valeur probante des preuves présentées.

La liberté de preuve contient certes une part de réponse aux difficultés soulevées par la preuve informatique, mais il s'agit toutefois d'une réponse fort partielle. Certains auteurs ont préconisé la généralisation du système de liberté de preuve en matière informatique.[24] Les limites tangibles d'une telle approche nous ramènent aux véritables enjeux: fondamentalement l'idée n'est pas de se débattre face un système probatoire trop contraignant ou inadapté, mais bien de pouvoir rapporter des éléments pouvant constituer des preuves de ce que l'on avance.

A défaut de pouvoir s'appuyer sur le régime de la preuve libre et plus encore dans le souci de s'assurer de la valeur probante des éléments de preuve, deux voies s'offrent aux parties qui souhaitent rapporter une preuve informatique. Il s'agit, d'une part, de la voie conventionnelle et, d'autre part, de la voie interprétative.

Section 2: La solution conventionnelle: l'accord d'interchange

La première approche est contractuelle. Elle consiste pour les contractants à s'entendre sur les éléments qu'ils prendront en compte au titre de la preuve. La matière de la preuve n'étant pas considérée comme d'ordre public, la validité de ces conventions est admise.[25] On notera cependant qu'en vertu de l'article 32, 18° de la loi du 14 juillet 1991 sur les pratiques du commerce, le législateur limite les possibilités d'aménagement conventionnel en matière de preuve dès lors que ces conventions auraient pour effet de limiter les moyens de preuve que le consommateur peut utiliser.

La voie conventionnelle semble délicate à mettre en œuvre sur Internet.

1° La multiplication des réseaux ouverts dans la mesure où ils permettent la conclusion de transactions entre des

[18] Pour une analyse détaillée de cette question, voy. Dieux, X., "La preuve en droit commercial belge", *R.D.C.*, 1986, p. 85 et s.

[19] Dieux, X., *op. cit.*, p. 89.

[20] Dieux, X., *op. cit.*, p. 89-90, . Verheyden-Jeanmart, *op. cit.*, p. 152.

[21] Sur les concepts de valeur probante, force probante et foi due aux actes, voy. Antoine, M., Brakeland, J.F. et Eloy, M., *Le droit de la preuve face aux nouvelles technologies de l'information et de la communication*, Cahier du Centre de Recherches Informatique et Droit, n° 7, Bruxelles, Story Scientia, 1991, p. 56.

[22] Poullet, Y., "Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve", *loc. cit.*, p. 43.

[23] Voy. Flamée, M., Thanghe, M., "Bewijsrecht: beknopte status queationis", *Le droit des affaires en évolution*, Association Belge des Juristes d'Entreprise, Bruxelles, Bruylant, Antwerpen, Kluwer, 1992, p. 218.

[24] Voy. à ce sujet Larrieu, J., *op. cit.*, p. 9 qui critique cette solution en ce qu'elle ne dissuaderait pas le contentieux judiciaire et qu'elle serait trop favorable aux entreprises, organisations dotées de nombreux moyens, par rapport aux simples particuliers, aux consommateurs.

[25] Cass. 5 janvier 1950, *Pas.*, 1950., I, p. 287. Pour d'autres références, en jurisprudence et en doctrine, voy. Antoine, M., Brakeland, J.F. et Eloy, M., *op. cit.*, pp. 50-51.

personnes en relations d'affaires occasionnelles, rend impraticable le système d'aménagement conventionnel du droit de la preuve et empêche dès lors d'y voir une solution universelle et suffisante.[26] Il faut signaler cependant que des accords sur la preuve peuvent lier des personnes qui ne se connaissent pas. Tel pourrait être le cas dans des réseaux semi-fermés. L'adhésion au réseau, ou l'abonnement à tel fournisseur d'accès, s'accompagnerait de la souscription de conditions générales applicables à toute communication avec les autres adhérents au réseau. L'utilisateur adhérent reconnaîtrait par avance la valeur de la signature des autres abonnés du réseau.

2° Cet accord d'interchange qui doit porter sur les éléments essentiels de la communication électronique ne peut pas, pour l'heure, prendre une autre forme que celle d'un écrit papier revêtu d'une signature manuscrite. On voit mal en effet comment, en l'absence d'une reconnaissance certaine de la valeur d'une communication électronique, de telles conventions pourraient être conclues *on-line*.

3° Dès lors que de tels accords d'interchange se traduisent sous la forme de contrats d'adhésion proposés par un professionnel, on peut s'interroger sur la qualité de l'adhésion du profane à ces accords. En outre, si une telle convention permet de résoudre la question de l'admissibilité de tel ou tel élément de preuve, elle laisse entière la question de la valeur probante que le juge reconnaîtra à cette preuve. La référence à des standards et partant la normalisation apparaît comme essentielle au développement de la preuve électronique.

En conclusion, on imagine fort bien le recours aux accords d'interchange dans le cadre de relations d'affaires entre professionnels. D'ailleurs le monde commercial envisage déjà de dépasser la phase des accords d'interchange pour recourir aux E-terms[27], sorte de grammaire du commerce électronique, auxquels les parties feraient référence lors de la conclusion de contrats.[28]

Section 3: La voie interprétative: le document informatique est un écrit signé

La seconde démarche est interprétative, et porte sur les concepts clé de notre droit de la preuve. Peut-on, en se fondant sur une analyse fonctionnelle des concepts d'écrit, d'original et de signature, assimiler les preuves électroniques à des écrits sous seing privé? A défaut d'y parvenir, peut-on tirer argument de certaines exceptions à l'exigence d'écrit admises par le législateur?

§1. L'exigence d'un écrit

a: Caractéristiques de l'écrit

Dès lors qu'un écrit est requis, il faut s'interroger sur la recevabilité du document écrit obtenu par voie d'enregistrement informatique. Pourra-t-il être assimilé à l'écrit exigé?

Ce débat est ancien et n'a pas attendu l'avènement d'Internet. A bien y regarder l'exigence d'écrit n'induit pas nécessairement que l'alignement des signes d'écriture soient reproduits sur un support papier.[29] En fait, "les cadres juridiques régissant la forme de l'acte sous signature privée sont plus accueillants et plus évolutifs que l'on veut bien le dire".[30]

L'écrit apparaît comme un concept ouvert. En l'absence de toute définition de l'écrit dans notre législation, on se reportera à ses caractéristiques: l'écrit "constitue un support stable et fiable sur lequel figurent des signes lisibles formant un langage".[31] Ainsi trois qualités fonctionnelles caractérisent l'écrit et justifient la valeur probante supérieure de celui-ci. Ces trois qualités qui sont l'inaltérabilité, la lisibilité et la stabilité doivent être rencontrées par le document électronique pour lui reconnaître la qualité d'écrit.[32]

On constate à ce stade que les exigences sont avant tout techniques.

1°: L'utilisation de la cryptographie va permettre d'assurer l'intégrité d'un document informatique, en vue d'éviter toutes altérations.

2°: La cryptographie permet en outre d'assurer l'intégrité dans le temps, c'est-à-dire la stabilité du contenu. Cet objectif peut être atteint par l'apposition d'une signature de la nouvelle génération sur un message revêtu d'une signature vieillissante; l'écrit informatique peut parfaitement être archivé à de telles conditions.

A cette question, il faut également rattacher la question de la stabilité du support. Il convient de maintenir la compa-

[26] Poullet, Y., "Droit de la preuve: de la liberté aux responsabilités", Texte présenté au colloque "Informatique et Droit", Montréal, 30 septembre-3 octobre 1992, p. 3.

[27] Qui réalisent, en quelque sorte, l'adaptation des Incoterms au commerce électronique.

[28] Poullet, Y., "Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve", in *Le droit des affaires en évolution. Le juriste face à l'invasion informatique*, Colloque ABJE, 24 octobre 1996, Bruxelles, Bruylant, Anvers, Kluwer, 1996, pp. 59-60.

[29] Olivier, F., Barbry, E., "Des réseaux aux autoroutes de l'information: Révolution technique? Révolution juridique. 1-De l'utilisation des réseaux", *J.C.P., éd. G*, 1996, n° 17-18, 3926, p. 174.

[30] Larrieu, J., *op.cit*, p. 10.

[31] Poullet, Y., "Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve", *Loc. cit.*, p. 53.

[32] *Ibidem*. On notera le tableau sombre dressé en 1988: "La dématérialisation des opérations, notamment dans les transactions par télématique, comme la fugacité des informations (édition sur écran), ou la fragilité des supports de données, accroissent l'impression de précarité. Enfin, la réversibilité des inscriptions magnétiques rendant possible la modification d'une donnée sans que la manipulation puisse être décelée, ajoutée à l'invisibilité et au cryptage des informations stockées en mémoire, entretiennent la suspicion notamment sur la conformité des états de sortie aux informations initialement mémorisées". Larrieu, J., *op. cit.*, p. 9.

tibilité du support, et ce même dans un environnement informatique mouvant, ou d'assurer le rajeunissement du support.

3°: La lisibilité qui s'entend de la possibilité de produire le document informatique dans une forme compréhensible à l'homme repose sur l'existence des outils logiciels adéquats. Ce qui conceptuellement ne pose guère problème.

On soulignera les difficultés qui peuvent surgir à vouloir relire un document créé avec des outils informatiques peu répandus ou anciens. Une difficulté particulière pourrait surgir si le document informatique signé a en outre fait l'objet d'un chiffrement en vue d'assurer sa confidentialité. Encore faudra-t-il parvenir à restituer le document en clair.

En conclusion, "il nous paraît inacceptable de dire que l'usage des nouvelles technologies entraîne l'absence de preuve écrite. Lorsqu'il y a échange de données, même informatisé, il y a écrit ou du moins, il y a possibilité de se constituer un écrit, non pas un écrit appréhendé au sens restrictif du terme, mais bien un écrit dans une perspective évolutive".[33] La réalité de l'écrit informatique semble acquise pour peu que l'on se place dans ce qu'il est permis d'appeler la perspective du "tout cryptographique".

Si les réflexions concernant l'écrit sont anciennes et si, en parallèle, on observe une évolution des mentalités conduisant à reconnaître l'écrit informatique, il apparaît que les exigences de signature et de titre original posent problème (cf. §2 et §3).

b: Les exceptions à l'exigence d'écrit

a) Impossibilité de se procurer un écrit

L'article 1348 du Code civil dispose qu'il est fait exception à l'exigence de l'écrit sous seing privé lorsqu'il y a eu impossibilité de se procurer un écrit. "L'impossibilité de se procurer un écrit est une exception dont le maniement paraît difficile, au moment où c'est volontairement que celui qui se prévaudrait de cette exception s'est privé d'un écrit".[34]

b) Commencement de preuve par écrit

Le juge peut prendre en considération un écrit qui n'est pas signé et original lorsque cet écrit répond à deux conditions: d'une part, il émane de l'adversaire et d'autre part, il rend vraisemblable le fait ou l'acte juridique en cause.

A ces deux conditions, le magistrat peut conférer à cet écrit un statut particulier: celui de commencement de preuve par écrit. "Cette règle est importante sur Internet, car une impression d'un courrier électronique ou d'une page web que l'on veut opposer dans le cadre d'un procès à leur expéditeur ou diffuseur pourrait être qualifiée de commencement de preuve par écrit et dès lors être admise par le juge à ce titre".[35]

§2. L'originalité de l'écrit

a) La copie d'un "original présentable" (Article 1334 du Code civil)

La copie, définie comme la "transcription littérale d'un acte, faite d'après l'original"[36], est caractérisée par la circonstance qu'elle constitue une transcription non signée de l'original.[37] L'absence de signature, d'une part, et le risque de modification du contenu lors du recopiage, d'autre part, expliquent le régime strict dans lequel sont tenues les copies à l'article 1334 du Code civil. Les risques d'altération expliquent le statut de la copie, dont l'admissibilité au titre de la preuve est subordonnée à l'éventuelle demande de production de l'original. A défaut de pouvoir produire l'original, la copie pourrait être prise en compte par le juge au titre de commencement de preuve par écrit, aux conditions de l'article 1347 du Code civil.[38]

b) La copie d'un "original non présentable'

Avec l'apparition des nouveaux moyens de reproduction, on a vu se multiplier les copies d'original non-présentable. Ainsi, avec l'introduction du téléfax, on est amené à considérer que les télécopies ne peuvent constituer des copies au sens de l'article 1334 du Code civil, "l'applicabilité de cette disposition étant subordonnée à l'existence même d'un titre original (acte authentique ou acte sous seing privé)".[39] La recevabilité d'une télécopie comme preuve doit, dès lors, être envisagée par le biais de l'article 1347 du Code civil, à savoir qu'il s'agit d'un simple commencement de preuve par écrit.

c) Le message électronique, copie ou original?

L'étape suivante, franchie par la communication électronique, consiste à questionner la distinction original/copie. Soit qu'un véritable original ait été créé, soit que l'on doive se contenter d'un document n'ayant pas valeur d'original (et n'étant pas de surcroît une copie au sens de

[33] Poullet, Y., "Droit de la preuve: de la liberté aux responsabilités", Texte présenté au colloque "Informatique et Droit", Montréal, 30 septembre-3 octobre 1992.

[34] Poullet, Y., "Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve", *Loc. cit.*, p. 43.

[35] Hance, O., *Business et droit d'Internet*, Bruxelles, Best Of, 1996, p. 221.

[36] De Page, H., *Traité de droit civil*, tIII, n° 832.

[37] Verheyden-Jeanmart, N., *op. cit.*, p. 201.

[38] Verheyden-Jeanmart, N., *op. cit.*, p. 203.

[39] Antoine, M., Brakeland, J.F. et Eloy, M., *op. cit.*, p. 97. Dans l'hypothèse de la télécopie, celui qui cherche à prouver n'a jamais eu de document original entre ses mains.

l'article 1334 du Code civil), et qui serait le simple reflet d'un acte juridique pour lequel aucun original n'aurait été établi.

Nous nous sommes attachés à démontrer que le document électronique pouvait être assimilé à un écrit sous seing privé, un original, pour peu qu'aient été rencontrées les exigences de sécurité. Ce qui fait l'originalité d'un document, c'est d'une part que ce document soit signé et d'autre part que son intégrité ait été protégée. En matière informatique, la facilité de reproduction d'un document laisse penser que l'on a affaire à des copies, il n'en est rien. La technique informatique permet la reproduction, en original, du document. La formalité du double, prévue à l'article 1325 du Code civil nous rappelle que l'unicité du document n'est pas une condition de son originalité.

A ce stade, et selon la technique utilisée, il apparaît que les systèmes informatiques permettent de créer deux sortes de documents.

1° Des documents qui ont valeur d'originaux. Pour ce faire, il faut que le destinataire puisse vérifier qu'il est en présence d'un document revêtu d'une véritable signature. La signature qui se rattache au document doit être active et vérifiable. Par "signature active" nous entendons une signature qui, nonobstant le transport, est restée reliée au signataire et au contenu du message. Cette caractéristique assure l'originalité du document. Par "signature vérifiable", nous visons la possibilité pour le destinataire d'un message de contrôler l'identité du signataire et son adhésion à un contenu, dont l'intégrité a été assurée.

Ces conditions semblent bien rencontrées pour les documents signés à l'aide des procédés de cryptographie asymétrique qui apparaissent, pour leur destinataires, comme des documents revêtus d'une signature. De plus, le procédé de signature permet le contrôle de l'intégrité du contenu signé. La reproduction sous différents supports de l'écrit signé ne lui ôte pas sa qualité d'original.[40]

Nous reviendrons par la suite sur la nécessité d'adopter une conception dynamique de la signature. Celle-ci, conçue comme partie intégrante du processus d'expression d'une volonté, doit pouvoir être vérifiée originale, par toute partie, en tout point.

2° Des documents qui ont valeur de commencement de preuve par écrit[41], voire de simples présomptions. Chaque fois qu'aux yeux du destinataire, il n'apparaît pas que le message reçu est revêtu d'une signature active et vérifiable, celui-ci ne peut se voir reconnaître la qualité d'original. Qu'il s'agisse de télécopies[42] ou de message électroniques, les éléments d'identification de l'auteur, s'ils existent, apparaissent en tout ou en partie détachés de l'auteur et du contenu du message. Ces documents s'apparentent à la figure classique du document établi et signé au moyen d'un papier carbone auquel la jurisprudence dénie toute valeur d'original.[43] On notera toutefois que de semblables documents peuvent éventuellement se voir reconnaître un statut juridique spécifique au regard d'une législation particulière. Ainsi la Cour de cassation a-t-elle considéré que la copie d'un acte de cession de rémunération sur laquelle la signature du cédant a été apposée au travers d'un papier carbone peut être considérée comme un exemplaire au sens de l'article 27 de la loi du 2 avril 1965 concernant la protection de la rémunération.[44]

d) Lettres missives et formalités du double de l'article 1325 du code civil

Il apparaît qu'un message informatique signé peut être rapproché d'une lettre missive. A l'image de la lettre missive, le message électronique est un *écrit* destiné à mettre en correspondance deux personnes.[45] Il peut, dans la mesure où il contient l'acte juridique lui-même (ou lorsque plusieurs messages rapprochés les uns des autres contiennent l'acte), à l'instar des lettres missives, être considéré comme un acte sous seing privé.[46]

L'article 1325 du Code civil dispose que les actes sous seing privé qui contiennent des conventions synallagmatiques, ne sont valables qu'autant qu'ils ont été faits en autant d'originaux qu'il y a de parties ayant un intérêt

[40] Ajoutons que la technique informatique permet la création de documents originaux dont l'unicité serait assurée. Si ces procédés ne modifient pas notre analyse des questions de preuve, ils permettent une avancée remarquable sur la voie de la dématérialisation des titres négociables. L'incorporation du droit dans un titre pourrait être réalisée dans un titre informatique, par exemple un connaissement électronique. Ainsi le projet Boléro prévoit le remplacement des documents de transports maritimes par des équivalents informatiques. Les connaissements et autres titres négociables qui apparaissaient comme le dernier fief du bon vieux papier semblent pouvoir être remplacés par des équivalents informatisés, dotés de cette même négociabilité. L'incorporation d'un droit dans un support informatique semble également présente dans les solutions de monnaie virtuelle.

[41] L'article 1347 du Code civil prévoit la réunion de trois conditions: un écrit, qui émane de celui contre qui la demande est formée et qui rende vraisemblable le fait allégué.

[42] Sur cette question voy. M. Fontaine qui semble partisan de la reconnaissance de la valeur d'original au document reçu, du moins si certains moyens de sécurisation sont adoptés. M. Fontaine, "La preuve des actes juridiques et les techniques nouvelles", in *La Preuve*, colloque UCL, 1987, p. 25. Cette approche ne contredit pas notre analyse dans la mesure où elle s'applique à l'envoi de télécopies en réseau fermé. Sur l'utilisation de la télécopie voy. également, Antoine, M., Brakeland, J.f. et Eloy, M., *op. cit.*, p. 97 et Amory, B. et Thunis, X., "Aspects juridiques de l'utilisation du télécopieur", *D.I.T.*, 1988/4, p. 35.

[43] Voy. Cass., 28 juin 1982, *R.C.J.B.*, 1985, p. 57 et note Van Quickenborne, M.

[44] Cass., 10 février 1997, Belgische Kredietverzekeringmaatschappij/Demuyt Albert, (616), cité in *R.D.C.*, 1997, pp. 395-396. La cour, ayant écarté l'application de l'article 1325 du Code civil au motif qu'il ne s'agissait pas en l'espèce d'un contrat synallagmatique, retient que l'exigence de l'article 27 alinéa 2 et 3, selon lequel l'acte de cession de la rémunération doit être établi, à peine de nullité, en autant d'exemplaires qu'il y a de parties ayant un intérêt distinct, ne concerne pas un régime de preuve mais vise la protection du cédant; que le cédant doit recevoir un exemplaire de l'acte afin de pouvoir vérifier, en tant que partie liée, la portée de son engagement.

[45] Sur la question des lettres missives, voy. Verheyden-Jeanmart, N., *op. cit.*, p. 288.

[46] Verheyden-Jeanmart, *op. cit.*, p. 288.

distinct. Cette exigence n'est cependant pas retenue en matière de lettres missives car son "respect se heurte à une impossibilité d'ordre pratique".[47] Par extension, la formalité du double semble pouvoir être évitée dans une communication électronique.

Pour le reste, si les parties à un échange télématique souhaitent apposer leur signature sur un document unique, en vue de la conclusion d'un contrat synallagmatique, il n'y a pas d'obstacle majeur à l'accomplissement des formalités prescrites à l'article 1325 du Code civil: mention du nombre d'originaux (un pour chaque partie ayant un intérêt distinct) et établissement d'un original pour chaque partie ayant un intérêt distinct. Sur ce dernier point, il importe peu que les différents originaux soient rigoureusement identiques[48], l'essence de l'article 1325 du Code civil étant que chaque partie soit en possession d'un original du contrat, afin que "chacun puisse apporter également la preuve de sa créance contre son cocontractant".[49]

On ajoutera que la jurisprudence et la doctrine admettent que le dépôt de l'acte entre les mains d'un tiers, qui le produira à la demande de l'une ou de l'autre des parties, permette de satisfaire sinon la lettre, du moins l'esprit de l'article 1325 du Code civil, à savoir assurer l'égalité des parties.[50] Dans le contexte de la communication sur Internet, on peut envisager l'intervention des autorités de certification pour assurer cette fonction quasi notariale.

§3. L'écrit doit être signé

La signature est un signe par lequel une personne, d'une part, s'identifie comme l'auteur de l'acte et, d'autre part, indique sa volonté d'adhérer au contenu de l'acte auquel la signature se réfère et sur lequel elle a été apposée.

Classiquement ces fonctions sont réalisées par la signature manuscrite. Il apparaît cependant que la technique informatique permet de rencontrer ces fonctions par le moyen des signatures électroniques.[51] L'apparition du réseau Internet et des réseaux ouverts remet en cause l'achèvement de ces fonctions par des procédés simples basés sur la présentation d'une carte et la composition d'un code secret.

Il ne suffit pas d'affirmer que le législateur n'a jamais eu qu'une conception fonctionnaliste de la signature (identifier et exprimer la volonté) et que l'exigence de signature manuscrite n'est pas inscrite dans notre code civil, il faut envisager la façon de réaliser dans un réseau ouvert les fonctions de la signature. Tel sera l'objet de notre chapitre 4.

[47] Verheyden-Jeanmart, *op. cit.*, p. 295.

[48] Pour une interprétation en sens contraire, voy. Hance, O., *Business et droit d'Internet*, Bruxelles, Best Of, 1996, pp. 223-24.

[49] Verheyden-Jeanmart, *op. cit.*, p. 245.

[50] Verheyden-Jeanmart, *op. cit.*, p. 249.

[51] Syx, D., "Vers de nouvelles formes de signature. Le problème de la signature dans les rapports électroniques", *Droit de l'informatique*, 1986, p. 133 et s.

Chapitre 4: L'identification du cocontractant dans un réseau ouvert

Section 1: Importance du débat sur la signature dans les réseaux ouverts

A ce stade, nous devons insister sur ce qui apparaît comme la caractéristique la plus marquante du réseau ouvert. Dans un tel système, la sécurité est contenue à même le message par le moyen des procédés de signature électronique.[52] Désormais, la sécurité d'un réseau réside avant tout dans la sécurisation du flux d'information et non plus uniquement dans sa structure. Chaque information, chaque message va être sécurisé par sa signature électronique.

C'est ici qu'apparaît le rôle central que doivent jouer les mécanismes de signature électronique. Il leur revient d'assurer la sécurité de l'échange des consentements.[53]

Section 2: Le chiffrement aux fins de signature

§1. Position du problème

Nous abordons ici la problématique délicate de l'identification des acteurs dans un environnement qui n'est soumis à aucun contrôle qui en limite l'accès.[54] A priori, le réseau ouvert n'offre aucune certitude sur l'identité d'un interlocuteur. Comment s'assurer que celui-ci est bien celui qu'il prétend être?

A cette question, se rattache la question de savoir si le cocontractant a bel et bien manifesté sa volonté de s'approprier le contenu de l'acte.

Dans la recherche de procédés qui permettraient de s'assurer de l'expression du consentement d'une personne déterminée, les mécanismes de cryptographie, en particulier les procédés de cryptographie asymétrique, vont apporter une aide déterminante.

§2. La cryptographie à clé publique

La fonction première de la cryptographie vise à rendre secret le contenu d'une communication.

[52] "Les principales garanties de sécurité quant à l'identification de l'émetteur, à l'intégrité des messages et quant à leur confidentialité résident non pas dans la structure du réseau lui-même, mais bien dans la sécurisation des messages qui y sont véhiculés", Parisien, S., Trudel, P., *L'identification et la certification dans le commerce électronique*, éd. Yvon Blais (Canada), p. 18.

[53] En approfondissant cette idée, on peut se demander si la signature n'est pas en passe de devenir, dans les réseaux ouverts, une véritable condition de validité du contrat. Sur cette question voy. Davio, E., "Questions de certification, signature et cryptographie", in *Internet face au droit*, Cahier du CRID, n° 12, Bruxelles, Story-Scientia, pp. 76-77.

[54] Masse, D.G., *op. cit.*, p. 5, qui pour sa part considère qu'Internet est un réseau ouvert, en ce sens "qu'il n'est soumis à aucun contrôle qui en limite l'accès".

Ce résultat peut être atteint par les mécanismes de cryptographie classique, également appelée cryptographie symétrique, en raison de l'utilisation d'une clé identique pour chiffrer puis pour déchiffrer. L'expéditeur utilise une clé secrète pour rendre illisible un message, le destinataire utilisera la même clé secrète pour lire le message. La principale faiblesse d'un tel système est la nécessité d'un partage de la clé secrète, laquelle doit exister en deux exemplaires. En outre, le partage de la clé secrète entraîne l'impossibilité d'identifier avec certitude lequel des deux titulaires est l'émetteur du message unique. En conséquence, la cryptographie symétrique ne permet pas de générer de véritables signatures.

La cryptographie moderne ou cryptographie asymétrique a résolu tant la question du partage des clés que celle de la signature.

La cryptographie asymétrique également appelée cryptographie à clé publique[55] consiste à déterminer, pour chaque utilisateur, deux clés de chiffrement reliées entre elles. Un message chiffré avec l'une des clés ne peut être déchiffré qu'avec l'autre et vice versa. La cryptographie est dite asymétrique parce que la clé qui sert à chiffrer n'est pas la même que celle qui sert à déchiffrer. Le lien mathématique entre les deux clés est tel qu'il est impossible de découvrir une des clés en partant de l'autre.

Les deux clés liées vont connaître des sorts opposés. L'une est gardée secrète, connue de son seul titulaire, l'autre est rendue publique, c'est la clé publique.

La première fonction de la cryptographie asymétrique est de rendre un message illisible à tous sauf à son destinataire. Il s'agit d'assurer la confidentialité d'une communication. Pour ce faire, Bob, expéditeur du message, va le chiffrer avec la clé publique du destinataire, Alice. Dès ce moment, le message chiffré ne pourra plus être déchiffré qu'à l'aide de la clé secrète d'Alice. C'est à ce stade que surgit le débat contemporain sur les éventuelles restrictions législatives à l'usage de la cryptographie.[56]

La seconde fonction d'un tel système est une fonction de signature. Comment Bob peut-il convaincre Alice qu'il est bien l'auteur d'un message? Si Bob, auteur d'un message, chiffre celui-ci avec sa clé secrète (qu'il est, par définition, seul à connaître) et l'expédie à Alice, cette dernière va procéder au déchiffrement du message à l'aide de la clé publique de Bob. Si Alice parvient de la sorte à déchiffrer le message, elle acquiert la certitude que ce message provient bel et bien de Bob et que celui-ci y a adhéré. Ce qui revient à dire que le message est signé.

En résumé, si Bob veut rendre confidentiel le message qu'il destine à Alice, il le chiffre avec la clé publique d'Alice. S'il veut signer ce message, il le chiffre avec sa clé secrète. Et bien évidemment, il peut combiner les deux fonctions.

A ce stade, on peut identifier deux zones de risques, l'une a trait à la clé secrète, l'autre à la clé publique.

§3. Les risques afférents à la conservation de la clé secrète

On constate que les procédés de cryptographie asymétrique permettent une gestion efficace du risque informatique. Cela ne saurait nous faire oublier les risques physiques liés à la conservation de la clé secrète par son titulaire. En effet, si ce dernier perd la maîtrise de sa clé secrète, une tierce personne pourrait s'en servir et signer en lieu et place du titulaire de la clé.

De manière générale, le titulaire d'une clé secrète doit en assurer une conservation des plus attentives. En outre des mécanismes d'opposition et de révocation de clés existent dans tous les systèmes. Les responsabilités du titulaire quant à la conservation de sa clé secrète sont des plus lourdes. A cet égard, deux remarques doivent être formulées. *Primo*, la protection de cette relation singulière doit être assurée tant par une information de l'utilisateur que par la mise en place de mécanismes qui confortent le lien entre la clé secrète ou son support et son titulaire. En ce sens nous recommandons qu'une clé secrète soit systématiquement rapprochée de son titulaire par le recours à un code secret à mémoriser.

Secundo, l'apparente infaillibilité logique des systèmes conduit à reporter l'intégralité du risque sur le titulaire de la clé secrète. Cette situation est dénoncée par Benjamin Wright qui condamne la tendance à mettre tous les œufs dans le même panier, à savoir la clé secrète.[57] Car, en

[55] Dont l'apparition remonte à 1975.

[56] Antoine, M., "Cryptography in Belgian Law", *EDI Law Review*, 1996, vol. 3, n° 3, pp. 221-228.

[57] Benjamin Wright critique la solution adoptée dans de nombreux états américains et pour la première fois par l'état de l'Utah, dans une loi intitulée *Digital Signature Act* ou *Utah Act*, qui trouve sa place dans le *Utah Code Ann.* § 46-3-101. Pour Benjamin Wright, la stratégie adoptée dans le *Utah Act* suppose un renversement de la charge de la preuve ainsi qu'une concentration du risque sur la clé secrète. (Cette vision est transposable à la plupart des solutions législatives ou conventionnelles qui mettent en place des infrastructures à clés publiques). "Not only does the Utah strategy shift risk to the private key, it concentrates the risk there. The *Utah Act* gives recipients like Bob strong reason to expect that if a document is signed with Alex's private key then Alex is legally responsible for the document. *Utah Act* section 46-3-401 provides that a document signed with a digital signature is normally presumed to be signed by the person owning the relevant private key (so long as his public key is certified by a licensed CA)... This presumption in turn gives Alex powerful incentive to protect the key... Under the Utah strategy, control of Alex's private key becomes all important. In other words, virtually all the eggs are placed in one basket – the private key", Benjamin Wright, "Eggs in baskets: Distributing the Risks of Electronic Signature", communication présentée à Montréal, le 31 août 1995 dans le cadre de la conférence *Faire des affaires en toute sécurité sur les autoroutes de l'information*, p. 4, cité par Parisien, S., "Aspects juridiques et technologiques des mécanismes de signature électronique: une analyse comparative", http://www.droit.umontreal.ca/AQDIJ/Colloque_10_11_95/Parisien/parisien_udm.html. Le texte de B. Wright est accessible, contre rémunération à l'adresse http://www.infohaus.comm/access/byseller/Benjamin_Wright/Benjamin_Wright.Eggs_in_Baskets.paid.txt. Le texte de B. Wright est également publié dans le *John Marshall Journal of Computer and Information Law*, 1997, pp. 189-201.

effet, si par impossible un cryptosystème était cassé par un ingénieux fraudeur, le préjudice de l'utilisation de cette clé secrète forgée incomberait au titulaire de la clé secrète originale lequel est présumé avoir assuré incorrectement la conservation de sa clé secrète.

Section 3: les Autorités de Certification

§1. Le certificat de clé publique

Si on se tourne vers la clé publique, une question se pose:

Comment être certain que telle clé publique, présentée comme étant celle de Bob, est effectivement la sienne?

L'utilisation de la cryptographie à clé publique aux fins de signature électronique suppose le recours à des mécanismes de contrôle visant à s'assurer que la clé rendue publique est bien celle de la personne qui s'en prétend titulaire. Un tel contrôle va être rendu possible grâce aux certificats de clés publiques qui émanent d'entités qui peuvent attester de l'existence d'un lien entre une clé publique et tel utilisateur déterminé.

Deux figures de contrôle peuvent être envisagées soit une structure de type pyramidal, soit une structure de type horizontal. Nous ne nous attarderons pas sur cette seconde forme de certification, quoique cette dernière est largement répandue, c'est en effet sur base du web-of-trust que sont certifiées les clés publiques générées dans le cadre du PGP.[58] En pareil cas, il n'y a pas de hiérarchisation, on ne parle pas d'autorité. La certification est le fait de pairs.[59]

§2. Les missions de l'autorité de certification: délivrance et gestion des certificats

Les autorités de certification sont des tiers de confiance qui ont pour mission de renforcer la fiabilité et la sécurité des mécanismes de cryptographie à clé publique.[60] La notion d'autorité de certification est définie dans la norme X 509 de l'UIT comme étant "une autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer leur clé publique et leur certificat".[61]

1° Leur mission première est la certification des clés publiques et donc l'émission de certificats de clé publique.[62] Lorsqu'elle certifie une clé publique, l'autorité de certification vise à s'assurer de l'identité de la personne à qui appartient la clé publique et ce afin de garantir à toute personne qui aurait à utiliser telle clé publique déterminée qu'à cette clé publique correspond bien tel individu.

Suite à cette certification, l'autorité de certification émet un certificat de clé publique. Ce certificat est une constation signée électroniquement par l'autorité de certification, relative à l'identité du sujet mentionné dans le certificat de clé publique et à la clé publique correspondante.

En plus de ces informations factuelles, le certificat peut également contenir ou faire référence aux conditions juridiques en rapport avec ce certificat. De telles conditions sont relatives aux conditions dans lesquelles le certificat a été émis et au statut juridique de l'autorité de certification.

Pour le destinataire d'un certificat, il faut qu'apparaisse clairement la signification du certificat et l'étendue de la confiance qu'il peut y placer. Par exemple, il convient de préciser les conditions de l'émission du certificat et le degré d'exactitude des affirmations contenues dans le certificat. Pour l'autorité de certification, ces conditions juridiques sont de première importance en vue de limiter ou d'exclure, dans une certaine mesure, sa responsabilité, dans le respect des tiers, tel le destinataire du certificat. De l'autre coté, le destinataire peut rechercher à engager la responsabilité de l'autorité de certification pour le respect des termes spécifiés.

2° L'autorité de certification doit veiller à la constitution et à l'actualisation du répertoire contenant les certificats de clé publique qu'elle a émis. Elle aura en charge la suspension et la révocation des certificats. L'autorité devra également intervenir pour assurer l'expiration, la réinscription et le renouvellement des certificats.

3° En outre, les autorités de certifications peuvent remplir d'autres missions. Il peut s'agir d'assurer l'horodatage d'un document[63], de certifier le contenu d'un document, la fonction d'un intervenant (médecin, avocat) ou encore d' assurer la conservation de documents à des fins probatoires.

[58] Le logiciel PGP, pour *Pretty Good Privacy*, est un logiciel de chiffrement largement répandu parmi les utilisateurs d'Internet. On peut l'obtenir gratuitement sur de nombreux sites. Voy. Zimmermann, Philip, PGP User's Guide volume 1: Essential Topics (Oct. 11, 1994), accessible à l'adresse URL ftp://netdist.mit.edu/pub/PGP.

[59] Sur cette question voy. Froomkin, M., "The essential role of trusted third parties in electronic commerce", 75 Gregon L. Rev. 49 (1996), disponible à l'adresse http://www.law.miami.edu/~froomkin/articles/trusted.htm.

[60] UIT-T, Recommandation X. 509, Annuaire- cadre d'authentification, note 323, art. 3.3 c). D'autres tâches de certification peuvent encore être accomplies par l'autorité de certification. Ainsi elle peut certifier des caractéristiques de la personne autre que l'identité: âge, appartenance à un ordre professionnel, lieu de résidence. Elle peut également attester de l'existence d'un document à un moment déterminé.

[61] UIT-T, Recommandation X. 509, Annuaire- cadre d'authentification, note 323, art. 3.3 c).

[62] Dans une architecture à clé publique, "l'utilisation de la clé publique permet de vérifier une signature numérique réalisée à l'aide de la clé secrète correspondante. Néanmoins, il importe de s'assurer que ces clés correspondent bel et bien à l'identité avérée du signataire. Il est en effet possible d'imaginer qu'une personne utilise une paire de clés asymétriques en présentant frauduleusement celles-ci comme correspondant à l'identité d'un tiers ou d'une personne fictive; l'utilisation de certificats, émis par une autorité de certification, permet de pallier à cette difficulté". Parisien, S., Trudel, P., *op. cit.*, pp. 117-118.

[63] Sur cette question Verheyden-Jeanmart, N., *op. cit.*, p. 159, qui constate que les questions relatives aux modalités de preuve de la date de l'acte restent controversées.

Section 4: Le niveau de sécurité et la régénération des clés

§1. Choix d'un niveau de sécurité adéquat

La sécurité totale n'existe pas. En cryptographie, la sécurité d'une clé s'évalue en considération du temps et de l'argent nécessaire à un fraudeur pour casser cette clé. La clé sera réputée sûre si le bénéfice que le fraudeur pourrait tirer du décryptage est minime en fonction des efforts à fournir.

Apparaît ainsi l'idée qu'il peut y avoir des exigences variables quant à la qualité des signatures, en particulier selon l'importance du message".[64]

Ainsi, lorsqu'un contractant souhaite sécuriser ses transactions, il doit déterminer l'enjeu financier des opérations, afin de choisir le niveau de sécurité adéquat. Dans le système Belsign, le client a le choix entre trois niveaux de sécurité distincts.[65] Une sécurité relativement limitée pouvant parfaitement convenir pour des opérations de moindre importance. En fonction des différents niveaux de certificats, les contrôles, les garanties et responsabilités de l'autorité de certification varieront.

§2. L'obsolescence des clés et signatures

Une clé réputée indéchiffrable à ce jour pourrait ne plus l'être dans 5 ou 10 ans. Quelle valeur pourra-t-on reconnaître alors aux éléments de preuve constitués aujourd'hui? Les solutions retenues en Allemagne[66] intègrent cette donnée nouvelle. Dans un premier temps, le projet d'ordonnance prévoyait que la durée de sécurité d'une signature électronique était limitée à 5 ans et pour conserver sa valeur probante le document devait être signé à nouveau avant l'expiration de cette période de 5 ans.[67] La dernière version du projet d'ordonnance réaffirme la durée de vie limitée des signatures, cette durée étant désormais fixée en considération de chaque algorithme particulier et publiée au journal officiel.[68]

Les questions d'ordre pratique, soulevées par la problématique du vieillissement des signature, sont nombreuses. Ainsi, pour assurer l'application d'une telle disposition n'est-il pas indispensable de recourir à un horodatage systématique des messages?[69] De quelle manière procédera-t-on au rajeunissement d'une signature? Faudra-t-il se tourner vers le signataire initial?

Section 5: Les responsabilités de l'autorité de certification

On l'aura compris, les missions des autorités de certification sont capitales. Entre leurs mains réside la sécurisation des réseaux et par là même le développement d'Internet à des fins commerciales.

Le premier champ de responsabilité de l'autorité de certification réside dans l'émission du certificat. "En émettant un certificat, l'autorité de certification confirme que les informations qui y figurent sont exactes et complètes".[70] L'utilisateur est en droit de s'attendre à un haut niveau de fiabilité. A défaut de pouvoir offrir une garantie absolue d'exactitude, l'autorité de certification doit indiquer le niveau de garantie qui se rattache au certificat.

L'autorité de certification pourra être tenue pour responsable d'un manquement à l'obligation de sécurité, particulièrement lorsque la confidentialité de sa propre clé secrète est compromise.[71]

"La responsabilité d'une autorité de certification peut également être engagée si celle-ci ne procède pas, de façon diligente, à la suspension ou à la révocation de certificats, ainsi qu'à la publication des certificats ainsi invalidés".[72]

Conclusion

L'approche globale de la problématique de la preuve laisse apparaître les nombreuses dissensions entre le droit de la preuve tel qu'il figure dans nos codes et le commerce électronique tel qu'on l'envisage sur Internet. Notre exposé, en travaillant tant sur les concepts juridiques que sur les aspects techniques, vise à montrer qu'une réconciliation de ces deux pôles est possible, voire toute proche.

Sous l'angle technique, ainsi qu'en attestent le développement rapide des infrastructures à clés publiques et les réflexions entreprises dans de nombreux états, il semble que la reproduction des fonctions traditionnelles de l'écrit papier et de la signature manuscrite passe par le recours à la cryptographie. Cette dernière apparaît clairement comme le moteur de la sécurisation sur Internet. Sommes-nous engagés irréversiblement sur la voie du

[64] Poullet, Y., *op. cit.*, p. 13; Froomkin, M. *op. cit.*, p. 5. Ce dernier envisage les différents niveaux de signature en fonction de la nature de la nature de l'opération, en référence à ce qu'offre l'autorité de certification VeriSign.

[65] http://www.belsign.be

[66] German Digital Signature Law, disponible en anglais à l'adresse http://ourworld.compuserve.com/homepages/ckuner/digsig4.htm
German Draft Digital Signature Ordinance (version du 7 juillet 1997), disponible en anglais à l'adresse http://ourworld.compuserve.com/homepages/ckuner/verord04.htm

[67] §18 du German Draft Digital Signature Ordinance (version du 20 décembre 1996), accessible à l'adresse http://ourworld.compuserve.com/homepages/ckuner/verord03.htm#Digital Signature Ordinance 20,12,96

[68] German Draft Digital Signature Ordinance (version du 7 juillet 1997), §17 et 18, disponible en anglais àl'adresse http://ourworld.compuserve. com/homepages/ckuner/verord04.htm

[69] Cette exigence d'horodatage est affirmée au § 18 du projet d'ordonnace allemand disponible en anglais à l'adresse http://ourworld.compuserve.com/homepages/ckuner/verord04.htm

[70] Parisien, S., Trudel, P., *op. cit.*, p. 134.

[71] Parisien, S., Trudel, P., *op. cit.*, p. 133.

[72] Parisien, S., Trudel, P., *op. cit.*, p. 133-134.

"tout cryptographique"? Dans un réseau ouvert, en l'absence de sécurité issue de l'architecture du réseau, nous avons vu que la sécurisation devait s'opérer sur l'information elle-même. Dès lors, il ne faut pas s'étonner que la cryptographie, dont la fonction n'est autre que d'assurer la sécurité d'une information qui circule, soit vouée à un bel avenir.

Sous l'angle juridique, on peut partir du constat que le débat sur la preuve se ramène à un débat sur la sécurité et la gestion du risque. Le législateur est intervenu pour fixer, au travers d'exigences probatoires, un certain degré de sécurité. Cette sécurité offerte, les parties peuvent s'en départir. Les importantes dérogations au régime de la preuve réglementée – relations entre commerçants, opérations de faible valeur, possibilité de dérogation conventionnelle - laissent aux contractants la liberté de déterminer la sécurité qui leur convient. D'aucuns iront sans doute jusqu'à renoncer à se préconstituer une preuve.

Le législateur belge ne s'est pas enfermé dans une définition de l'écrit ou de la signature, mais s'est attaché à leur haute valeur sécuritaire. A ce titre, on peut affirmer que le législateur ne s'est jamais départi d'une vision fonctionnelle, vision dictée par les impératifs de sécurité probatoire. Cette approche fonctionnelle a très tôt été mise en avant par certains auteurs qui refusaient de légitimer la preuve électronique par le biais d'exceptions et suggéraient d'introduire, dans notre législation, une définition fonctionnelle de l'écrit et de la signature.[73]

Une réforme du droit de la preuve, longtemps ajournée, semble aujourd'hui inéluctable. L'avènement même des autoroutes de l'information dicte que les législateurs appuient le mouvement qui, en matière de preuve, va de la liberté à la responsabilité.[74] Le législateur doit œuvrer dans le sens d'une responsabilisation de différents intermédiaires ou intervenants dans la communication sur le réseau.[75] Cette responsabilisation s'inscrirait dans la droite ligne du mouvement de normalisation auquel aspirent les réseaux. Par normalisation, il faut entendre tant l'adoption de standards que la clarification des normes applicables[76] et la définition des obligations afférentes à chacune des parties dans le processus de sécurisation.[77]

La difficulté majeure pour les législateurs d'aujourd'hui n'est pas tant d'affirmer que l'informatique peut servir la constitution d'éléments de preuve, que de déterminer, au sein d'une technique mouvante, les procédés qui rencontrent les fonctions assignées à l'écrit et à la signature. L'ouverture offerte par une définition fonctionnelle, techniquement neutre, des concepts d'écrit et de signature semble battue en brèche par la nécessité de pointer, parmi les techniques existantes, celles qui sont propres à réaliser ces fonctions.[78]

Cela étant fait, nos systèmes juridiques doivent encore réussir l'intégration harmonieuse des solutions nouvelles, imaginées pour les communications électroniques, aux côtés des solutions existantes. Si idéalement une vision intégrée du droit de la preuve peut être défendue, l'analyse fonctionnelle des concepts d'écrit et de signature va en ce sens, il faut se garder d'une assimilation trop brutale. Une évolution sensible dont il faut tenir compte est le passage du système de preuve essentiellement statique vers un système nettement plus dynamique.[79] La preuve, dans un environnement électronique, n'apparaît pas tant comme un objet[80], que comme un processus de sécurisation qui va permettre l'expression du consentement.[81]

Etienne Davio
Assistant à la Faculté de Droit de Namur
Centre de Recherches Informatique et Droit

[73] Voy. ainsi Poullet, Y., *op. cit.*, p. 44; Antoine, M., Brakeland, J.F. et Eloy, M., *op. cit.*, p. 212. L'approche de l'équivalent fonctionnel a été retenue dans les travaux de la CNUDCI lors de l'élaboration de son "Guide pour l'incorporation de la loi type sur certains aspects juridiques de l'échange de données informatisées (EDI) et des moyens connexes de communication, A/CN.9/426-CNUDCI,29è session, New York, 28 mai-14 juin, 1996, n° 30 et s.

[74] Poullet, Y., "Droit de la preuve: de la liberté aux responsabilités", Texte présenté au colloque "Informatique et Droit", Montréal, 30 septembre-3 octobre 1992.

[75] L'intervention législative ne tient pas tant au corpus des règles traditionnelles en matière de preuve et que l'affinement des techniques informatiques semble conforter. On pense par exemple à la notion d'écrit, voire de document, notions qui initialement semblaient ne pas avoir de place dans un environnement électronique.

[76] Citons dans cette mouvance le nouveau Code civil du Québec qui dans une section intitulée "des inscriptions informatiques", traite de la preuve des actes juridiques et dispose notamment en son article 2837: "Lorsque les données d'un acte juridique sont inscrites sur support informatique, le document reproduisant ces données fait preuve du contenu de l'acte, s'il est intelligible et s'il présente des garanties suffisamment sérieuses pour qu'on puisse s'y fier". Pour apprécier la qualité du document, le tribunal doit tenir compte des circonstances dans lesquelles les données ont été inscrites et le document reproduit. Il s'ensuit plusieurs dispositions fixant les moyens d'appréciation du niveau du sérieux des garanties présentées.

[77] A ce stade, il faut souligner la nécessité d'une normalisation à grande échelle. "Une harmonisation mondiale de ces pratiques de preuve nous éviterait la question indiscrète de la loi applicable et donc du régime induit" Olivier, F., Barbry, E., *op. cit.*, p. 175.

[78] Ainsi, comme l'on fait de nombreux législateurs, si l'on décide que la signature digitale pour être valable doit reposer sur le recours à la cryptographie asymétrique et aux services d'autorités de certification agréées, on disqualifie toute autre forme de signatures (par exemple la "signature" basée sur la cryptographie symétrique ou la "signature" basée sur la cryptographie asymétrique mais sans recours à une autorité de certification agréée).

[79] Cette évolution remet en question, par exemple, la distinction classique copie-original.

[80] A l'image d'une information manuscrite ou dactylographiée apposée sur une feuille de papier, revêtue d'une signature manuscrite.

[81] S'agissant de la signature électronique, on observe la généralisation d'une vérification a priori des signatures. S'agissant des signatures manuscrites, leur vérification apparaît rare et elle a lieu essentiellement a posteriori.