Mélanges

Michel Cabrillac

DALLOZ — Litec

L'ACTE SOUS SEING PRIVE ELECTRONIQUE : REFLEXIONS SUR UNE DEMARCHE DE RECONNAISSANCE

par

André PRÜM
Professeur à l'Université de Nancy II
Directeur du Centre de Recherche de Droit Privé et
du Laboratoire de Droit Economique au CRP-Gabriel Lippmann (Luxembourg)

En plein essor, le commerce sur l'Internet s'épanouit pour l'heure dans des conditions de sécurité juridique peu satisfaisantes. Des transactions, portant - il est vrai - sur des montants généralement assez faibles, sont conclues entre cocontractants qui s'ignorent, mais acceptent de se fier à des rencontres purement électroniques. Elles ne sont à l'abri ni d'un dysfonctionnement accidentel du réseau, ni d'agissements malveillants de tiers, ni enfin d'un comportement malhonnête du correspondant lui-même. Sauf précautions particulières, le risque n'est pas négligeable d'être trompé par une fausse identité, un message dont le contenu a été, volontairement ou non, altéré ou dont l'expéditeur refuse d'endosser la paternité. Si ces menaces n'ont pas eu raison d'une communauté d'internautes passionnés, pas plus qu'elles n'ont découragé des commerçants empressés d'affirmer leur présence sur le réseau, elles n'en constituent pas moins de sérieuses entraves au développement du commerce « en ligne » dont celui-ci ne saurait s'accommoder plus longtemps.

Pour apporter la sécurité indispensable aux échanges, il est d'ores et déjà techniquement possible d'utiliser une « *signature électronique* », par laquelle un correspondant peut s'identifier et s'approprier le contenu d'un message et qui permet au destinataire d'en vérifier l'origine et l'intégrité. La fiabilité de plusieurs de ces procédés semble aujourd'hui éprouvée et dépasserait même, selon les experts, parfois celle d'une signature manuscrite. Reste que les messages électroniques sécurisés par de telles signatures doivent également être reconnus en droit ce qui n'est pas, loin s'en faut, le cas à l'heure actuelle.

La recevabilité en preuve d'un acte sous seing privé électronique se heurte, en effet, dans la plupart des ordres juridiques à des acceptions trop étroites tant de l'écrit que de la signature, empruntées à leur support

matériel et au symbolisme attaché au geste de la main ([1]). Ces restrictions paraissent aujourd'hui manifestement dépassées et les opérateurs du commerce électronique n'ont de cesse d'en réclamer la révision. Plusieurs organisations internationales relaient leurs revendications et plaident pour une reconnaissance rapide des nouveaux procédés d'authentification électroniques ([2]). La Commission des Nations Unies pour le Développement du Commerce International (CNUCDI) en a pris l'initiative dans sa loi-type sur le commerce électronique, adoptée en 1996, en posant un principe général de non-discrimination dès lors que la signature est réalisée grâce à des méthodes suffisamment fiables eu égard à l'objet du message signé ([3]). Le groupe de travail sur le commerce électronique de la CNUDCI prépare actuellement un projet de règles uniformes sur les signatures électroniques qui tendent à préciser les conditions de mise en œuvre du principe ([4]). Plus récemment, l'Union Européenne s'est efforcée d'élaborer à son tour un cadre commun pour les signatures électroniques ([5]). Au delà de la promotion du commerce électronique, la proposition de directive vise à harmoniser les législations nationales en ce domaine afin que celle-ci ne lèvent pas de nouvelles barrières à la libre circulation des biens et des services.

Dans un débat mené sur fond de compétition internationale, les enjeux du marché virtuel ont, en effet, conduit d'ores et déjà plusieurs pays à adapter leur législation pour offrir à celui-ci le cadre le plus accueillant ([6]). L'exemple a été donné par l'Etat américain de l'Utah qui reconnaît, depuis le 1er mai 1995, une forme particulière de signature digitale reposant sur la technologie de la cryptographie asymétrique ([7]). Il a été rapidement

([1]) S. Parisien et P. Trudel, L'identification et la certification dans le commerce électronique, Ed. Yvon Blais Inc, Québec, 1996, p.21 et s.

([2]) Voir notamment l'étude de la Chambre de Commerce Internationale, « General Usage for International Digitally Ensured Commerce », CCI, 1997.

([3]) Loi-type de la CNUDCI sur le commerce électronique et Guide pour son incorporation, NATIONS UNIES, New York, 1997.

([4]) Projet de règles uniformes sur les signatures électroniques dont la dernière version a été discutée lors de la 35e session du groupe de travail sur le Commerce électronique à Vienne du 6 au 17 septembre 1999 ; A/CN.9/WG.IV/WP.82.

([5]) Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques (JO n°C 325 du 23 octobre 1998, p.5) dont la dernière mouture a été adoptée le 26 juin 1999 (7015/99).

([6]) les textes les plus significatifs sont référencés sur le site du Laboratoire de Droit Economique du CRP-Gabriel Lippmann à Luxembourg : http://www.crpgl.lu/lde.

([7]) Utah Digital Signature Act, Utah Code Annotated, titre 46, chap.3, http://www.state.ut.us :ccjj/digsig/ ; S. Parisien et P. Trudel, op.cit. p.46 et annexe 3 ; pour une description succincte de cette technologie, cf. infra.

suivi par d'autres Etats américains ([8]), ainsi qu'en Asie ([9]) et en Europe ([10]). D'autres pays s'apprêtent à reconnaître plus largement toutes formes de signatures électroniques, sur le modèle de la loi uniforme de la CNUDCI. Tel est le cas, en particulier, du Luxembourg ([11]), de la Belgique ([12]) et tout récemment de la France qui successivement ont déposé trois projets de loi en ce sens ([13]).

Avant de s'interroger sur la manière dont il convient de recevoir une signature électronique dans un ordre juridique donné, l'on doit s'entendre sur la portée exacte de cette reconnaissance.

L'objet de celle-ci demeure restreint, pour l'heure, à l'admission d'écrits signés de façon électronique comme moyen de preuve. Il n'est point question, à ce stade, d'autoriser le recours à de tels actes lorsqu'un écrit ou une signature manuscrite sont exigés « *ad validitatem* ». Comme l'a rappelé, à juste titre, le Conseil d'Etat dans son étude sur l'Internet et les réseaux numériques ([14]), un tel formalisme n'est imposé que dans des cas exceptionnels et ne saurait être levé qu'en appréciant pour chacun d'eux si les impératifs qui le sous-tendent peuvent être satisfaits de façon adéquate

([8]) Parmi les nombreux textes adoptés au niveau national Cf., en particulier, ceux de l'Etat d'Illinois (loi sur la sécurité du commerce électronique, n°3180, 1997 ; 5Ill, Comp. Stat. 175), du Minnesota (Loi sur l'authentification électronique, Minnesota Statutes § 325, 1997), du Misouri (loi sur les signatures numériques, 1998, SB 680) et de la Floride (General Bill S942 on Electronic Signature, Act of 25.5.1996) pour un tableau détaillé Cf. http://www.law.kuleuven.ac.be/icri/projects/tables.htm.

([9]) Singapour, loi n°9 de 1998 sur les transactions électroniques ; Malaisie, Digital Signature Bill 1997.

([10]) Cf. en particulier, la loi allemande sur les services d'information et de communication du 13 juin 1997 (Journal officiel allemand du 22 juillet 1997, BGBI, IS, 1870) et la loi italienne du 15 mars 1997 (GA 97, n°59) complétée par le décret présidentiel du 10 nov. 1997 (GA 98 n°60) et le décret du 15 avril 1999 sur les Autorités de certification (GA 99 n°87).

([11]) Projet de loi sur le commerce électronique déposé le 30 mars 1999, chambre des députés n°4554 préparé par le Laboratoire de Droit Economique du CRP-Gabriel Lippmann avec le concours du CRID de Namur, sous la direction d'André Prüm et d'Yves Poullet.

([12]) Avant-projet de loi visant à modifier certaines dispositions du Code civil relatives à la preuve des obligations et avant projet de loi relatif à l'activité d'autorités de certification agréées en vue de l'utilisation de signatures digitales.

([13]) Projet de loi portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique, enregistré à la Présidence du Sénat le 1er septembre 1999, Sénat n°488 , projet qui s'inspire très largement d'une étude réalisée par un groupe d'universitaires dans le cadre du GIP « Droit et Justice ».

([14]) Conseil d'Etat, Internet et les réseaux numériques, Etude adoptée par l'assemblée générale du Conseil d'Etat le 2 juillet 1998, La Documentation française, Paris 1998, p.79.

dans un environnement électronique.

Recherchée « *ad probationem* », la reconnaissance d'un message de données sous seing privé électronique soulève dans un régime de preuve légale ou mixte, tel que le connaissent la plupart des pays de tradition romano-germanique, la double difficulté de sa recevabilité et de sa force probante. Afin d'écarter la première, il serait certes concevable d'abandonner toutes restrictions à l'admissibilité des moyens de preuve au profit d'un système où celle-ci deviendrait entièrement libre. Bien qu'adoptée par quelques pays, la solution ne paraît guère recommandable en ce qu'elle implique un bouleversement profond du régime probatoire en vigueur. Au surplus, elle ne résout nullement la question de la valeur probante des documents électroniques, laissée au cas par cas à la libre appréciation du juge. En arrêtant par avance la valeur relative des différents instruments probatoires à l'intérieur d'une hiérarchie préétablie, le système de la preuve légale se montre sur ce point nettement plus sécurisant. Il n'existe, par conséquent, pas de raison de s'en écarter.

L'on ne saurait se satisfaire toutefois, dans ce cadre, d'une solution consistant à réduire les actes sous seing privé électronique à de simples indices pour les recevoir soit comme des commencements d'une preuve par écrit à parfaire par d'autres éléments, soit au titre des dérogations à l'obligation de se ménager la preuve écrite de certaines transactions. En l'état actuel des textes, ceci ne paraît d'ailleurs guère possible. Il faudrait déjà les modifier en créant, par exemple, comme le suggérait le Conseil National du Crédit et du Titre, une nouvelle exception à l'exigence d'un écrit pour le cas où « *le titre est établi ou conservé sous forme électronique dans des conditions assurant son intégrité et permettant l'imputabilité à son auteur* » ([15]). Mais surtout, une telle orientation conduit à refuser systématiquement aux messages signés de façon électronique la valeur probante d'un acte sous seing privé. Or, c'est précisément l'optique d'une véritable reconnaissance qui, loin de se contenter de tolérer de tels messages comme éléments de preuve, doit poser les conditions dans lesquelles un document assorti d'une signature électronique peut être assimilé, à des fins probatoires, à un écrit traditionnel revêtu d'une signature manuscrite ([16]).

Pour atteindre cet objectif, il convient, en premier lieu, de lever les obstacles conceptuels qui, aujourd'hui encore, s'opposent à ce qu'un écrit

([15]) Conseil National du Crédit et du Titre, Problèmes liés à la dématérialisation des moyens de paement et des titres, Mai 1997, p.55 à 80.
([16]) Dans le même sens, cf. l'étude précitée du Conseil d'Etat.

puisse être consigné sur un support volatil et qu'une signature résulte de l'utilisation d'un procédé technique plutôt que d'un geste de la main ([17]) (I). La voie à la réception étant ouverte, il importe de poser les modalités exactes de la reconnaissance. Il ne saurait être question de reconnaître la valeur probante d'un acte sous seing privé à tout et à n'importe quel message de données assorti d'un sceau électronique sans s'assurer que celle-ci présente un degré de sécurité et de fiabilité comparable à celui d'une signature manuscrite (II).

I – SUPPRESSION DES OBSTACLES A LA RECONNAISSANCE DE L'ACTE SOUS SEING PRIVE ELECTRONIQUE

Le Code civil français, comme ses homologues belge et luxembourgeois, fidèles, sur ce point, aux textes originels du Code Napoléon, ne donnent aucune définition de l'écrit, de la preuve littérale ou de la signature. En théorie, il n'existe donc pas d'obstacle dans ces législations à une interprétation évolutive de ces concepts permettant l'accueil de documents informatiques signés par un procédé purement électronique. D'ailleurs, certains auteurs considèrent déjà de tels messages comme des écrits assimilables à des actes sous seing privé ([18]). L'opinion reste cependant isolée dans un courant doctrinal largement attaché à la conception traditionnelle de ces actes comme, plus généralement, de l'écrit et de la signature. Il en va de même de la jurisprudence qui, à l'exception de quelques rares décisions, refuse de reconnaître une pleine valeur probante aux actes numériques, voire simplement de les admettre comme commencements de preuve par écrit ([19]).

Le temps est venu de s'écarter d'une vision trop classique (1°) afin de s'orienter vers une acception nouvelle et ouverte de l'acte sous seing privé (2°).

([17]) Peu importe à cet égard, à notre avis, que l'on s'oriente vers une assimilation complète des messages de données, protégés par une signature électronique suffisamment sûre, à des actes sous seing privé ou vers un simple régime d'équivalence entre les deux. Si la première suppose, de toute évidence, une conception rénovée de l'écrit signé ; le second ne saurait non plus s'accommoder de la survie d'exigences formelles impossibles à transposer dans un environnement électronique. Cf. position différente exprimée dans l'étude précitée du Conseil d'Etat, p.90.

([18]) Sous la réserve, le cas échéant, de lever certains obstacles formels, comme l'exigence du double exemplaire.

([19]) Cf. l'arrêt de la Chambre commerciale du 15 décembre 1992 (Bull. IV, n°419) par lequel celle-ci dénie toute portée juridique à une photocopie avant que la chambre civile n'admette finalement qu'elle pouvait servir de commencement de preuve par écrit (Civ. I, 14 février 1995, JCP, 1995, II, 22409, note Y. Chartier).

A – L'ABANDON DE L'ACCEPTION TRADITIONNELLE DE L'ACTE SOUS SEING PRIVE...

La conception classique de l'acte sous seing privé repose sur le double postulat qu'un écrit ne se conçoit pas en dehors d'un support matériel, en général un support papier et que sa signature doit nécessairement être autographe et manuscrite.

Le premier se prolonge dans la distinction opérée entre l'original et les copies qui tient directement à la conservation ou non de l'acte sur son support initial. Le second résulte d'un usage ancien attribuant au geste manuel de la signature une importante valeur symbolique ([20]). En effet, le caractère manuscrit de celle-ci n'est imposé par aucun texte de portée générale ; le législateur s'étant contenté d'en poser l'obligation dans des cas tout à fait exceptionnels, comme le testament olographe ([21]), les actes authentiques ([22]) ainsi que divers actes de procédure. En raison de la confiance particulière qu'elle inspire, la signature manuscrite continue cependant d'être considérée comme la seule forme acceptable de ratification, apte à exprimer, de façon non équivoque, la volonté de son auteur et à permettre l'identification de ce dernier. Tous les autres signes, tels les paraphes, griffes, empreintes digitales ou autres codes secrets se voient généralement déniés ces qualités et ne sont pas de ce fait admis comme d'authentiques signatures ([23]). Il n'en va autrement que dans les rares situations où une loi, une convention ou un usage les admet expressément. Or, les textes en ce sens demeurent exceptionnels ([24]). La voie contractuelle suppose que les parties soient en position de trouver un accord préalablement à leurs échanges, ce qui est exclu pour la plupart des transactions négociées directement sur un réseau électronique ouvert comme l'Internet. Quant à la jurisprudence, elle se montre très réservée pour admettre l'existence d'usages en sens contraire, même entre commerçants ([25]).

Cette circonspection n'est assouplie ni par la liberté laissée à tout un

---

([20]) I. Dauriac, La signature, thèse dactyl. présentée à l'Université Panthéaon-Assas (Paris II), le 10 janvier 1997, n°133.
([21]) Art. 970 c. civ.
([22]) Décret du 2 nov. 1971, art. 15.
([23]) F. Terré, Introduction générale au Droit, Précis Dalloz, 1994, n°522.
([24]) Le recours aux signatures non manuscrites n'est guère autorisé que pour certains instruments de paiement ou de crédit, en particulier pour la lettre de change (loi n°66-380 du 16 juin 1966) et le « Bordereau Dailly » (loi n°93-1444 du 31 décembre 1993).
([25]) Com. 27 juin 1961 (2 arrêts), Bull., IV, n°289 et 299, RTDCom, 1962, 89, obs. J. Becqué et H. Cabrillac, I. Dauriac, op.cit, n°137.

chacun de choisir le graphisme de sa signature, ni par la tolérance de tous supports matériels suffisamment stables. Seul un arrêt récent, rendu par la chambre commerciale à propos de l'acceptation d'un bordereau de cession de créances professionnelles, semble amorcer une évolution. La haute juridiction y retient, en effet, qu'un écrit, exigé ad validitatem, « *peut être établi et conservé sur tout support, y compris par télécopies, dès lors que son intégrité et l'imputabilité de son contenu à l'auteur désigné ont été vérifiées ou ne sont pas contestées* » ([26]). Le sens et la portée exacte de cette solution demeurent difficiles à cerner, comme l'ont abondamment souligné les commentateurs. Il semble bien cependant que la Cour s'oriente vers une nouvelle acception de l'instrumentum qui l'amène à considérer comme un original un document télécopié ne portant qu'une image de la signature. De là à admettre qu'un acte sous seing privé puisse ne pas être signé manuellement, ne paraît plus constituer un pas infranchissable.

Un message de données authentifié par une procédure électronique ne remplit aucun des deux critères traditionnels de l'acte sous seing privé. Stocké dans la mémoire d'un ordinateur, il n'est pas lié à ce support, et peut être transféré tel quel sur un nouveau support. Il ne porte pas directement la trace d'une marque personnelle apposée par son signataire; son authentification prendra simplement la forme d'une transformation du message réalisée par le biais d'un procédé informatique dont le signataire a le contrôle.

En l'état actuel du droit, un tel message ne peut, par conséquent, être reçu comme un écrit signé. Tout au plus pourrait-il être admis comme un commencement de preuve par écrit. Sa pleine reconnaissance suppose de modifier notre conception de l'acte sous seing privé.

B – ... AU PROFIT D'UNE *CONCEPTION RENOVEE*

Le concept d'acte sous seing privé fait appel tant à la notion d'écrit ou de preuve littérale qu'à celle de signature. Son ouverture à de nouveaux instruments probatoires requiert ainsi l'élargissement de l'une et de l'autre de ces deux notions. Est-il utile cependant de cerner chacune par une définition légale, la question ne fait pas l'unanimité à en croire les récents projets de loi déposés en France, en Belgique et au Luxembourg. Si tous s'efforcent de définir la signature, seul le projet français retient une description formelle de la preuve littérale tout en posant les conditions de

([26]) Com. 2 déc. 1997 ; D. 1998, 192, note D.R. Martin ; JCP G 1998, p.905, observ. P. Catala et P.Y. Gauthier ; JCP G II, 10097, note Grynbaum ; JCP E, 1998, p.178 , note T. Bonneau.

recevabilité de l'écrit électronique. Les textes en discussion en Belgique et au Luxembourg se bornent à préciser les critères du caractère original d'un acte sans définir l'écrit ou la preuve littérale.

Les mérites respectifs des deux approches ne peuvent être mesurés qu'à l'aune de la nouvelle conception de la signature.

1°) Définition de la signature

Deux approches sont a priori concevables pour définir la signature, selon que l'on s'efforce de cerner plutôt la nature du geste ou sa finalité.

Précurseur en la matière, le code civil du Québec s'est attaché essentiellement à la première en retenant que « *la signature consiste dans l'apposition qu'une personne fait sur un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante, pour manifester son consentement* » ([27]). Le choix présente l'inconvénient de lier le concept à certaines expressions matérielles dont il peut s'avérer, par la suite, délicat de délimiter avec précision l'étendue. Le débat actuel sur la possibilité de considérer les procédés de signature digitale comme des « *marques personnelles* » en fournit l'illustration, quoique la doctrine québécoise, dans son ensemble, n'y voit guère d'obstacles ([28]).

En outre, cette option conduit à envisager la signature principalement comme un signe appréhendé à travers sa forme. Or, les travaux de recherche récents rappellent qu'une telle approche ne rend pas pleinement compte des effets de la signature et de la force probante qu'elle confère à l'acte signé en tant qu'instrument de preuve préconstitué. La constatation s'impose pour les actes notariés dont la signature par le notaire ne peut être considérée comme l'accomplissement d'une simple formalité ([29]). Celle-ci participe bien plus de l'essence de la réception de l'acte par le notaire dont il tient son authenticité. Elle vaut tout autant pour les actes sous seing privé dont la signature est un élément consubstantiel. Au delà du signe, qui n'en est que l'extériorisation concrète, la signature mérite d'être considérée en soi comme un acte juridique ([30]). C'est à travers cet acte, que le signataire s'approprie le titre matériel auquel il confère force et valeur probantes. La validation résulte de l'adhésion consciente au contenu de celui-ci et doit prendre une forme reconnaissable par autrui.

([27]) Art. 2827 Code civil du Québec.
([28]) Droit du Cyberespace, sous la dir. de P. Trudel, Les éditions Thémis, Montréal, 1997, p.19.9.
([29]) J. Flour, Sur une notion nouvelle d'authenticité, Rép. Déf., 1972, art.30159, p.977.
([30]) I. Dauriac, op. cit. n°287 et s. n°451.

Peu importe, dans cette optique, la nature du signe employé à condition que l'intention soit claire et puisse être comprise comme une signature. Pour cela, il suffit que le signe satisfasse aux qualités essentielles reconnues à toute signature, à savoir qu'il permette d'identifier le signataire et de manifester sa volonté d'approuver l'acte. A une approche matérielle de la signature, assise sur une conception formaliste et nécessairement trop étroite du signe, il faut ainsi préférer une définition fonctionnelle.

C'est cette direction que les principaux travaux sur la reconnaissance des signatures électroniques exhortent à suivre. La loi-type sur le commerce électronique, élaborée par la CNUDCI, recommande une approche fondée sur « *l'équivalent fonctionnel* » des documents sur support papier et visant à déterminer de quelle manière les objectifs et les fonctions de tels documents seraient susceptibles d'être assurés dans un environnement dématérialisé. Concernant plus précisément l'exigence d'une signature, un consensus s'est dégagé au sein de cette organisation internationale pour admettre que celle-ci est remplie lorsqu'une méthode suffisamment fiable est utilisée pour identifier le signataire et indiquer qu'il approuve l'information contenue dans le message de données. La solution n'est pas d'ailleurs sans rappeler le « *Statute of frauds* » des Etats-Unis d'Amériques selon lequel la signature inclut tout symbole exécuté ou adopté par une partie avec l'intention d'authentifier un acte ([31]). Elle est partagée aujourd'hui par l'Union Européenne dont la proposition de directive sur un cadre commun aux signatures électroniques retient comme critère essentiel la fonction d'authentification des signatures.

Si l'approche fonctionnelle ne semble plus faire de doute, il faut encore donner un sens exact aux deux finalités caractéristiques de la signature : l'identification du signataire et la validation de l'acte.

En premier lieu, il convient de dissiper un malentendu sur la fonction d'identification dont le but n'est pas, contrairement à une opinion répandue, d'établir l'origine de l'acte signé. Lorsque celui-ci n'est pas reconnu par son auteur, l'analyse de la signature peut certes contribuer à identifier le signataire, mais il n'est pas indispensable que le signe révèle directement cette identité. La preuve en incombe, conformément au droit commun, à celui qui se prévaut de l'acte ([32]). Comme le met en évidence une étude récente consacrée à la signature, le pouvoir d'identification du

([31]) Uniform Commercial Code, art. 1-201 (39).
([32]) D . Veaux, Actes sous seing privé, Règles générales, J.Cl. Civ., art. 1322 à 1324, 8, 1997, n°56 ; F. Terré, op. cit. n°531.

signe doit être compris avant tout comme l'instrument symbolique de l'appropriation de l'acte par le signataire ([33]). Cette fonction se satisfait d'un lien arbitraire entre la personne de celui-ci et le signe qu'elle utilise. Elle suppose seulement que la procédure de signature fournisse des garanties suffisantes relatives à l'intervention personnelle du titulaire du signe pour assurer la validation de l'acte. L'exigence est susceptible d'être remplie par un autographe manuscrit ainsi que par l'emploi de codes secrets ou autres sceaux électroniques que leurs titulaires peuvent garder sous leur contrôle exclusif.

Pour autant, tous les signes capables d'authentifier de la sorte l'acte signé ne seront pas reçus comme des signatures valables. Seuls seront admis ceux qui, de surcroît, sont aptes à exprimer la volonté du signataire d'approuver l'acte. Or, ce pouvoir de validation n'est reconnu qu'aux signes dont le mode de production atteste a priori que l'auteur a agi de façon consciente et délibéré pour s'approprier le contenu de l'acte signé.

La signature manuscrite est censée traduire une telle volonté et ce non seulement en raison des qualités intrinsèques du signe autographe ou des garanties offertes par son support nécessairement matériel. Ne reconnaît-on pas, en effet, largement la validité des signatures manuscrites réalisées par des illettrés ou des aveugles, voire celles accomplies par une main guidée par un tiers ? Le pouvoir de validation repose sur une présomption ([34]) dont il n'est pas interdit d'étendre le champ d'application à d'autres procédés présentant des garanties équivalentes quant à la connaissance de l'acte par le signataire et son intention d'en faire sien le contenu. Tel est l'objet des conventions de preuve reconnaissant la signature par l'emploi de codes secrets, dont les tribunaux n'ont pas hésité à confirmer la validité ([35]). Hormis cette hypothèse, ceux-ci font preuve cependant d'une attitude réservée, comme en atteste notamment la jurisprudence rejetant les empreintes digitales en tant que mode de signature. Pour les signatures autres que manuscrites dont on souhaiterait consacrer l'efficacité, il est dès lors recommandé de poser les conditions sous lesquelles elles se voient dotés d'un pouvoir de validation.

Sous ces précisions, il est permis de retenir, à l'instar des projets de lois français, belge et luxembourgeois qui prévoient, à quelques nuances

([33]) I. Dauriac, op. cit., 206 ; cf. aussi F. Terré, op.cit. n°522.
([34]) P. Foriers, Introduction au droit de la preuve, in La preuve en droit, études publiées sous la direction de Ch. Perelman et P. Foriers, Travaux du Centre National de Recherches Logiques, Bruylant, Bruxelles, 1981, p.7 et s.
([35]) Civ. I, 8 nov. 1989, Bull. civ., I, n°342, RTDCom., 1990, 78, observ. M. Cabrillac et B. Teyssié.

près, des définitions identiques de l'acte de signature, que la signature, nécessaire à la perfection d'un acte sous seing privé, doit identifier celui auquel cet acte est opposé et manifester son adhésion au contenu de celui-ci. Ces qualités paraissent suffisantes pour caractériser l'acte de signature de façon générale sans qu'il soit indispensable de décrire plus amplement la manière dont il doit s'accomplir ou s'extérioriser concrètement. Au contraire, de telles précisions risqueraient de restreindre l'ouverture recherchée du concept.

Cette nouvelle acception de la signature suffit-elle pour lever tous les obstacles à la réception en preuve d'un acte sous seing privé électronique ou bien faut-il préciser également les concepts d'écrits ou d'original ?

2°) Définition de l'écrit ou de l'original ?

Le projet de loi français propose d'introduire les nouvelles règles consacrées aux écrits électroniques par une définition générale de la preuve littérale ou par écrit aux termes de laquelle celle-ci « *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* » ([36]). En ce qui concerne les formes que peut revêtir l'écrit, la description pourrait difficilement être plus large. Seule l'exigence du caractère lisible du document paraît délimiter le concept ; encore que la condition paraisse quelque peu triviale pour un instrument de preuve ([37]).

Les mérites de la définition n'apparaissent pas davantage dans sa conjugaison avec les conditions particulières posées pour les écrits électroniques. D'après le projet, un tel écrit ne serait « *admis en preuve au même titre que l'écrit sur support papier,* (que) *sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* » ([38]). La première exigence nous semble ressortir plutôt d'une définition de la signature dont elle constitue l'une des fonctions caractéristiques. Pour les actes non signés, l'identification de celui dont ils émanent reste d'un intérêt réduit ([39]) et ne devrait pas, de toute manière, être une condition pour les recevoir en

([36]) Projet d'article 1316 du code civil.
([37]) Sauf éventuellement à comprendre qu'elle signifie que l'information doit « *rester accessible pour être consultée ultérieurement* » conformément à l'article 6 de la loi type de la CNUDCI.
([38]) Projet d'article 1316-1 du code civil.
([39]) Cf. article 1311du code civil.

preuve. Quant à la garantie de l'intégrité, le texte français aborde, en vérité, deux problèmes liés mais distincts : celui de la sécurité originelle de l'acte et celui de la préservation ultérieure de cette qualité ([40]). Le premier problème rejoint les autres conditions spécifiques auxquelles il faut soumettre la reconnaissance des actes sous seing privé électronique, permise par l'élargissement des notions d'écrit et de signature ([41]). La portée du second, en revanche, est plus large puisqu'elle se réfère à la distinction générale entre l'acte original et une copie.

Dans une vision classique, cette distinction s'appuie, en effet, sur une différenciation relative à la nature du support : l'acte original est conçu comme celui qui a été conservé sur son support initial, alors que la copie résulte d'un transfert sur un nouveau support. Le droit attache des effets importants à cette différenciation. Les copies non signés d'un acte sous seing privé ne sont susceptibles d'être produites en justice qu'à condition que celui qui s'en prévaut soit capable de montrer également l'original ([42]). L'exigence n'est levée, depuis la loi du 12 juillet 1980, qu'à la condition que l'original ait été reproduit de façon fidèle et durable sur un support indélébile ayant fait l'objet d'une modification irréversible ([43]). Destiné à permettre la conservation de certains écrits sur des microfiches, ce tempérament ne suffit pas pour recevoir des documents électroniques ([44]).

L'avènement de l'informatique remettant en question la notion même de support, du moins de support matériel, l'originalité d'un document ne peut plus se ramener, comme par le passé, à une absence de changement du support. Le risque serait, en effet, de voir tout acte électronique, même signé, systématiquement disqualifié en une simple copie. Pour l'écarter, il convient de s'attacher à une acception nouvelle de l'originalité. Conformément aux recommandations de la CNUDCI, celle-ci peut être recherchée dans l'assurance que le contenu de l'acte signé n'a subi aucune altération depuis son origine. C'est ainsi que les projets luxembourgeois et belge définissent le document original comme celui qui présente des garanties fiables quant au maintien de son intégrité à compter du moment où il a été créé pour la première fois sous sa forme définitive ([45]).

([40]) La définition reprend à quelques nuances près les termes de l'arrêt de la chambre commerciale du 2 déc. 1997, précité.
([41]) Cf. infra.
([42]) Article 1334 c.civ.
([43]) Article 1348 al.2 c.civ.
([44]) Terré, op.cit., n°548.
([45]) projet d'article 1322-2 du Code civil luxembourgeois et projet d'article 1322 al. 2 du Code civil belge.

Fort de cette nouvelle conception de l'originalité, l'acte sous seing privé électronique peut être reconnu pleinement sans qu'il soit indispensable de définir la preuve littérale ou par écrit. Cet exercice délicat paraît même peu recommandable en ce qu'il risque de susciter plus de difficultés qu'il n'en résout. Mieux vaut se contenter d'une évolution implicite de ce concept, telle qu'elle est dictée, de toute manière, par l'approche fonctionnelle de la signature ([46]).

La suppression des obstacles à la réception en preuve de l'acte sous seing privé électronique ne signifie pas que tout message de données authentifié par un procédé électronique se voit reconnaître ipso facto la force probante d'un écrit signé. Celle-ci ne sera donnée qu'à certaines conditions et sous certaines modalités qu'il convient, à présent, de préciser.

II – DEFINITION DES CONDITIONS DE SECURITE DES ACTES SOUS SEING PRIVE ELECTRONIQUES

La valeur probante d'un acte sous seing privé manuscrit tient, en réalité, autant aux garanties présentées par le geste manuel de la signature qu'à la sécurité offerte par son support matériel. La première n'existant ici qu'à travers la seconde, la fiabilité et l'intégrité de l'acte font rarement l'objet d'une appréciation distincte. Ce n'est que dans des situations exceptionnelles où le support de l'acte s'avère insuffisamment stable que celui-ci pourrait être rejeté comme instrument de preuve malgré le fait qu'il soit signé. En revanche, les tribunaux n'hésitent pas à reconnaître des signatures réalisées elles-mêmes par des moyens peu sûrs, comme par exemple une signature au crayon. Tout au plus permettent-ils de contester la portée d'une signature figurant sur une partie non signifiante du document plutôt qu'à la fin de celui-ci comme il est d'usage.

Les signatures électroniques ne se concrétisent plus par une marque personnelle apposée sur un document en papier. Elles consistent dans l'utilisation d'un procédé d'authentification destiné à protéger un message ou une communication détachés eux-mêmes de tout support durable. A supposer qu'un tel dispositif réponde aux critères fonctionnels de la signature, la valeur probante de l'acte signé dépendra toujours de son degré de sécurité. Le niveau d'exigence requis mérite d'être précisé (A).

En même temps, il conviendra de veiller à ce que les conditions

([46]) Dans le même sens, M. Antoine et D. Gobert, Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification, Rev. Gén. de Droit civ. belge, 1998, n°4/5, p.285, spéc. p.291.

posées à ce titre ne créent pas de facto un obstacle insurmontable à la réception en preuve des documents signés de façon électronique. Autrement dit, celui qui entend se prévaloir d'un tel document doit concrètement pouvoir faire face à la preuve de sa fiabilité (B).

A – L'EXIGENCE DE FIABILITE DE L'ACTE SOUS SEING PRIVE ELECTRONIQUE

La signature manuscrite d'un acte constitue un gage non seulement de son approbation consciente, mais aussi de son imputabilité à une personne déterminée. En effet, même si la signature n'établit pas directement l'origine de l'acte, elle consiste, par nature, en un signe unique, propre au signataire et employé par celui-ci pour signifier son consentement à l'acte sur lequel il l'appose. Une falsification de ce signe par un tiers, sans être exclue, pourra normalement être détectée par une expertise graphologique, si elle n'est pas immédiatement visible. A ces assurances, le document portant la signature ajoute la qualité, d'une part, d'être immédiatement accessible à la lecture et celle, d'autre part, d'être consigné sur un support qui lui assure a priori une grande stabilité. L'une et l'autre ne sont plus automatiquement garanties dans un environnement électronique. Les données ne sont pas accessibles de façon immédiate mais uniquement par le truchement d'un affichage sur un écran ou une impression et ce grâce à l'utilisation d'un logiciel capable de les interpréter. Les supports de stockage sont rarement indélébiles et, en tout état de cause, vieillissent beaucoup plus rapidement que le papier, ce qui nécessite de retranscrire régulièrement les informations sauvegardées sur de nouveaux supports.

Enfin et surtout, le document signé à la main créé un lien indissociable entre le contenu de l'acte validé et sa signature. Après s'en être dessaisi, son signataire ne pourra plus le dénier. Ni lui, ni un tiers, ne pourront modifier le corps du document sans que celui-ci n'en porte la trace. L'intégrité de l'acte signé est protégée.

Des garanties similaires doivent être recherchées lorsqu'un acte destiné à servir comme instrument de preuve est établi et authentifié par un procédé purement électronique. D'un point de vue technique, des solutions satisfaisantes existent d'ores et déjà. Il s'agit de savoir sous quelles conditions le droit de la preuve est prêt à les recevoir. À cet égard et au vu des premières expériences étrangères en matière de reconnaissance de signature électronique, se pose d'abord la question de la neutralité de la législation par rapport aux technologies disponibles ou à venir. Ce n'est qu'ensuite qu'il sera possible de préciser les critères de fiabilité requis des

actes sous seing privé électronique.

1°) La neutralité des moyens

Du simple code secret à l'utilisation d'algorithmes de chiffrement ou de la biométrie, les procédés permettant de signer un message de données électroniques et d'en garantir la fiabilité sont, dès à présent, très variés ; sans imaginer ceux que les progrès de la technologie nous feront découvrir ([47]). Certains sont destinés plus précisément à sécuriser des échanges au sein d'un réseau fermé ou entre personnes partageant un même système ou une même clé de signature. D'autres ont vocation à être utilisés même dans un environnement totalement ouvert, comme l'Internet, où le signataire d'un message n'aura pas pu s'entendre préalablement avec son destinataire sur l'utilisation de moyens communs. Parmi ces dernières techniques, il y en a une qui paraît aujourd'hui s'imposer de facto comme un standard : la signature numérique ou digitale fondée sur la cryptographie asymétrique.

Le procédé suppose l'utilisation de deux clés de chiffrement complémentaires, l'une privée, dont le caractère secret doit effectivement être préservé, l'autre publique, librement distribuée. La première sert à signer un message en le transformant, de façon irréversible, en une chaîne de données que seule la clé publique, transmise au destinataire, permettra de décoder. L'une et l'autre sont conçues de telle manière qu'à une clé privée corresponde une seule et unique clé publique. Le destinataire du message aura ainsi la garantie que celui-ci n'a pu être rédigé que par le titulaire de la clé privée et qu'il n'a fait l'objet d'aucune altération depuis sa signature ([48]). Pour le protéger contre toute usurpation d'identité, un tiers pourra, le cas échéant, lui certifier que la clé publique jointe au message appartient effectivement à la personne qui s'en prévaut. Dépendant de la longueur des clés de chiffrement, cette technologie offre actuellement, d'après les spécialistes, la plus grande sécurité. Forte de ses atouts, la signature numérique à clé publique tend à devenir la référence incontournable pour les applications les plus diverses aussi bien que la technologie la plus largement diffusée sur le réseau Internet au point que d'aucuns la confondent avec toutes les autres formes de signatures électroniques.

Devant cette situation, la tentation est grande de consacrer le procédé également sur le plan juridique en s'appuyant sur le mécanisme de la cryptographie asymétrique pour préciser les conditions de fiabilité requises

([47]) S. Parisien et P. Trudel, op.cit. p.93 et s.
([48]) Pour de plus amples détails, cf. S. Parisien et P. Trudel, op.cit., p.93 et s.

d'une signature électronique. Plusieurs législations y ont succombé, d'abord outre-Atlantique ([49]), puis également en Europe. Pour nous arrêter aux exemples les plus proches, telle est la solution retenue par la loi allemande sur les services d'information et de communication du 13 juin 1997 ([50]) et par la législation italienne ([51]) qui, l'une et l'autre, définissent la signature électronique directement par rapport à l'emploi de la cryptographie asymétrique.

La référence à une technologie précise et connue, facilite la définition des signatures admissibles dans un environnement électronique, des conditions de leur efficacité en même temps que des responsabilités associées à une mauvaise utilisation de cette technologie. Elle présente néanmoins l'inconvénient de restreindre la reconnaissance des signatures électroniques à une seule de ces formes et d'exclure ainsi toutes les autres techniques, présentes ou futures, dont la fiabilité est avérée ; sans évoquer les hésitations que l'on peut nourrir de façon générale sur l'opportunité d'une législation reposant sur des choix purement technologiques, plutôt qu'orientée autour des finalités des règles posées, indépendamment des procédés techniques susceptibles de les satisfaire.

Cette neutralité est prônée par la loi uniforme de la CNUDCI qui

---

([49]) Cf. en particulier, le Digital Signature Act de l'Etat de l'Utah qui s'efforce de cerner avec précision la définition de la signature digitale et d'encadrer, de manière non moins précise, l'intervention des autorités de certification en arrêtant la valeur des certificats qu'elles peuvent émettre. art. 103 (10) : « Digital signature means a transformation of a message using an asymetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine : (a) whether the transformation was created using the private key that corresponds to the signer's public key ; and (b) whether the message has been altered since the transformation was made ».

([50]) Journal officiel allemand du 22 juillet 1997, BGBI, IS, 1870, art. 3 sur la signature digitale, § 2 (1) : « Eine Digitale Signatur im Sinne dieses Gesetzes ist ein im mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifierungstelle oder der Berhörde nach § 3 versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschheit der Daten erkennen lässt ».

([51]) Décret présidentiel italien n°513, du 10 novembre 1997, relatif à la création, à la conservation et à la transmission de documents sur la base de systèmes informatiques ou télématiques, pris en application de la loi n°59 du 15 mars 1997, Gazetta Ufficiale, 13 mars 1998, n°60, « Digital Signature, means the result of a computer-based process implementing an asymetric cryptographic system consisting of a public and a private key, whereby the signer asserts, by means of a private key, and the recipient verifies, by means of the public key, the origin and the integrity of a single electronic document or set of such documents ». Le régime vient d'être précisé par un décret du 15 avril 1999 (GA 1999, n°87).

insiste sur le fait qu'une méthode de signature, quelle qu'elle soit, doit être reconnue si sa fiabilité « *est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué* » ([52]). Un projet de Règles Uniformes précise l'exigence en posant les conditions dans lesquelles le niveau de sécurité atteint doit être considéré d'office comme acceptable ([53]). Transposables directement à la technologie de la signature numérique à clé publique, ces règles ne se trouvent, sous aucun aspect, liés exclusivement à ce procédé particulier.

Hésitante dans un premier temps, la Commission européenne s'est ralliée finalement à cette optique. La dernière mouture de sa proposition de directive ne se réfère plus à la cryptographie asymétrique mais permet d'accueillir également d'autres dispositifs de signature reposant sur des technologies similaires ([54]). La même neutralité caractérise les projets en discussion en France et au Luxembourg. C'est donc dans cette perspective qu'il convient de préciser les critères de fiabilité d'une signature électronique.

2°) Les critères de fiabilité

Pour répondre aux standards de sécurité admis pour l'acte signé de façon manuscrite, un acte sous seing privé électronique devra présenter des garanties relatives tant à son imputabilité à un signataire déterminé, qu'à son intégrité.

a) L'imputabilité de l'acte

Le recours à un procédé de signature, plutôt qu'à un graphisme personnel, éventuellement imitable mais jamais susceptible d'être partagé par plusieurs personnes, soulève immédiatement l'interrogation de savoir comment un tel procédé peut individualiser une personne déterminée afin de lui permettre de s'approprier le contenu du document signé. Ces fonctions ne paraissent pouvoir être satisfaites qu'à la double condition que le dispositif utilisé pour créer une signature électronique soit unique et particulier à une seule personne et susceptible d'être conservé sous son contrôle direct et exclusif.

([52]) Loi-type, art. 7.

([53]) Projet de règles uniformes sur les signatures électroniques dont la dernière version a été discutée lors de la 35ème session du groupe de travail sur le Commerce électronique à Vienne du 6 au 17 septembre 1999 ; A/CN.9/WG.IV/WP.82.

([54]) Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques (JO n°C 325 du 23 octobre 1998, p.5) dont la dernière mouture a été adoptée le 26 juin 1999 (7015/99).

En d'autres mots, la même signature électronique ne pourra être attribuée à plusieurs personnes. En revanche, l'on pourrait très bien imaginer qu'une seule et même personne dispose de plusieurs signatures électroniques qu'elle utilise à des fins différentes. De même, que l'on peut admettre une signature sous pseudonyme ou encore une signature reconnue directement à une personne morale dont celle-ci déléguerait l'utilisation à certains de ses représentants ou, pourquoi pas, comme cela est déjà le cas dans certains pays ([55]), à un agent électronique. Dans toutes ces hypothèses, il importe simplement qu'une personne déterminée se porte fort des actes signés. Cette responsabilité incombe naturellement à celui qui s'est fait connaître comme le détenteur de la clé de la signature et dont il est censé assurer la garde en empêchant toute personne non autorisée de se l'approprier.

b) L'intégrité de l'acte

L'intégrité d'un acte mérite d'être apprécié au moment où il est établi pour être ensuite évalué dans le temps. Le premier examen permet de décider si l'acte peut être considéré comme un acte sous seing privé, le second de vérifier, le cas échéant, le caractère original de l'écrit signé lorsqu'il est produit en preuve. L'un et l'autre sont susceptibles naturellement de soulever de délicates questions techniques lorsqu'il s'agit d'apprécier la fiabilité d'un procédé informatique utilisé pour établir un tel écrit ou pour le conserver. Notre propos n'est pas de les évoquer ici.

Cependant, une difficulté qui a trait plus particulièrement au caractère immatériel de la signature électronique nous semble devoir être prise en compte dans les conditions de reconnaissance de l'acte sous seing privé électronique. Contrairement à une signature manuscrite, nécessairement apposée sur un document déterminé, les dispositifs d'authentification électroniques ne se trouvent plus physiquement attachés aux données auxquelles ils s'appliquent. Il n'est pas exclu ainsi que la signature électronique jointe à un message de données puisse être enlevée de celui-ci sans que l'opération laisse la moindre trace. De même, le message signé de façon électronique pourrait être modifié après sa signature, toujours sans que cette altération soit perceptible. De tels risques ne sont évidemment pas tolérables pour des documents auxquels l'on souhaite reconnaître la force probante d'un acte sous seing privé.

([55]) Loi sur la sécurité du commerce électronique de l'Illinois (n°3180, 1997 ; 5Ill, Comp. Stat. 175) art. 5-105.

Aussi, une signature électronique n'est-elle susceptible de conférer cette valeur à un message de données qu'à condition qu'elle en garantisse aussi l'intégrité. Cela signifie qu'elle doit y être attaché de façon indissociable et de telle manière que toute modification du message protégé, y compris l'effacement de la signature elle-même, soit immédiatement détectable. Il s'agit là d'une condition de sécurité qu'il convient de prévoir de façon expresse pour les actes sous seing privé électronique afin de pallier les risques inhérents à leur caractère immatériel.

B – LA PREUVE DE LA FIABILITE DE L'ACTE SOUS SEING PRIVE ELECTRONIQUE

La complexité des procédés d'authentification électroniques peut rendre la preuve de leur fiabilité extrêmement difficile. Elle le sera d'autant plus lorsqu'elle incombe à une personne autre que le signataire lui-même, qui entend se prévaloir de l'acte sans avoir participé à sa création. Le fait de ne pas pouvoir démontrer que celui-ci satisfait aux exigences normales de sécurité risque alors de le priver de toute valeur probante. Pour éviter cet écueil, il convient de réfléchir dans quelles situations la fiabilité d'un dispositif de signature électronique ne pourrait pas être présumé (1°). Une telle présomption aura pour conséquence de transférer le risque de preuve à celui qui souhaite contester la signature. Elle appelle dès lors des précisions sur les conditions dans lesquelles cette contestation pourra prospérer (2°).

1°) Les présomptions de fiabilité

Par souci de ne pas préjuger de solutions techniques particulières, le cadre de reconnaissance des actes sous seing privé électronique se doit d'accueillir tous les procédés d'authentification qui remplissent les fonctions caractéristiques d'une signature et présentent un niveau de fiabilité adéquat. Malgré l'émergence de certains standards, des procédés très variés sont susceptibles a priori d'y répondre. Tous n'offrent cependant pas les mêmes garanties de sécurité. Certains d'entre eux, comme la signature digitale à clé publique, impliquent l'intervention d'un tiers appelé à certifier l'identité du signataire et le dispositif de signature utilisé. D'autres se réalisent en dehors de toute procédure de ce genre et leur sécurité devra être appréciée au cas par cas.

Afin de faciliter la reconnaissance des signatures électroniques, il paraît justifié de tenir compte de ces différences en admettant, dans certains cas, que leur fiabilité puisse être présumée. La présomption pourrait se fonder, en particulier, sur l'attestation délivrée par une autorité indépendante et digne de confiance.

Le système n'est cependant opérationnel qu'à condition que tout un chacun puisse savoir exactement dans quelles circonstances il est autorisé à se fier à une signature électronique assortie d'un tel certificat.. Celles-ci doivent dès lors être arrêtées par voie législative. Plusieurs pays s'y sont déjà employés en définissant un régime de certification auquel peuvent adhérer les autorités qui souhaitent voir leurs certificats bénéficier d'une présomption de sécurité ([56]). Ces initiatives méritent aujourd'hui d'être coordonnées afin que la reconnaissance des signatures électroniques ne se cantonne pas à des cadres strictement nationaux mais s'inscrive dans une perspective internationale. Les discussions engagées au sein de la CNUDCI et de l'Union européenne tendent à arrêter les conditions de l'harmonisation nécessaire. Leurs projets prévoient l'un et l'autre de préciser les vérifications minimales auxquelles doivent procéder les autorités de certification et sur lesquelles doivent porter leur attestation. Parmi celles-ci figurent essentiellement le contrôle de l'identité du titulaire de la signature et de la sécurité du dispositif permettant de la vérifier. L'agrément des autorités de certification se trouve soumis, au surplus, au respect de certaines obligations destinées à rassurer ceux qui se fient à leurs certificats quant aux conditions dans lesquelles celles-ci exercent leur activité. Le crédit que l'on prévoit d'accorder à leurs certificats s'appuie sur ce double niveau d'exigences posées pour l'attestation et pour celui qui la délivre.

Ayant pour but de créer une simple dispense de preuve, la présomption de fiabilité du dispositif de signature électronique est sujette à la démonstration que celui-ci ne présente, malgré lés apparences, pas les garanties de sécurité requises. L'écrit numérique ne sera dans ce cas plus reconnu comme acte sous seing privé, mais servira, tout au plus, comme simple commencement de preuve par écrit. À l'inverse, le message de données authentifié par une signature électronique qui ne satisfait pas aux critères de fiabilité pour être admis a priori ne sera pas nécessairement disqualifié comme acte sous seing privé. Faute de bénéficier de la présomption, celui qui s'en prévaut devra seulement prouver que l'acte est intègre et imputable à son signataire.

Si la différence peut-être importante en pratique, elle se cantonne néanmoins à une pure question de preuve. Fondamentalement, la reconnaissance de la signature électronique reposera toujours sur les mêmes critères, à savoir qu'elle remplit les fonctions caractéristiques de toute signature dans des conditions de sécurité satisfaisantes. Mieux vaut,

([56]) M. Antoine et D. Gobert, art. cit.

dans ces conditions, se garder d'évoquer l'idée de deux catégories de signatures distinctes, celle qualifiées d' « *avancées* » ou de « *renforcées* » dont la fiabilité serait présumée, et toutes les autres ([57]). La distinction laisse sous-entendre une forme d'infériorité des secondes par rapport aux premières, alors qu'une fois reçues, les unes comme les autres doivent se voire reconnaître exactement la même valeur probante. L'examen des conditions dans lesquelles l'acte sous seing privé électronique pourra être contesté permettra de mieux l'apprécier.

2°) Contestation d'un acte sous seing privé électronique

La force probante d'un instrument de preuve se mesure au moyens permettant de le contester. L'écrit sous signature privée jouit à cet égard d'une situation privilégiée dans notre système probatoire puisqu'il ne peut être attaqué que par un autre écrit. Il n'en va autrement que dans les cas où la preuve est de toute manière libre, que ce soit en raison de la faible valeur de la transaction ou parce qu'elle est administrée contre un commerçant.

Ce principe, fondé sur le parallélisme des formes doit il être maintenue pour les actes sous seing privé électronique ? La question est débattue. Les travaux préparatoires du projet de loi français préconisaient à cet égard que l'on devait pouvoir prouver contre ou outre un écrit électronique « *sur le fondement de présomptions graves, précises et concordantes* » ([58]). Sans exposer l'acte sous seing privé électronique au risque d'une contestation par tous moyens, la solution n'abandonnait pas moins l'exigence d'une preuve littérale. L'écrit électronique serait ainsi doté d'une force probante légèrement inférieure à celle d'un écrit traditionnel revêtu d'une signature manuscrite. Mais, l'idée n'a, à ce stade, pas été reprise par le projet de loi déposée le 1er septembre 1999. Pas plus que ne l'a été une autre suggestion consistant à créer directement une hiérarchie entre les deux formes d'écrits sous signatures privées. Dans l'avant-projet de loi, il était prévu, en effet, d'interdire de contester un écrit signé à la main par un écrit électronique ([59]). Le projet de loi ne porte plus la trace de cette restriction.

L'une et l'autre proposition traduisaient, en réalité, une certaine défiance vis-à-vis des écrits électroniques et de leur procédés

([57]) La distinction est prévue par la proposition de directive et le projet de règles uniformes de la CNUDCI.
([58]) Projet d'article 1316-1 al. 3 de l'avant projet de loi élaboré sous l'égide du GIP « Droit et Justice ».
([59]) Projet d'article 1316-1 al. 1er de l'avant projet de loi élaboré sous l'égide du GIP « Droit et Justice ».

d'authentification ([60]). Or, ceux-ci ne sont précisément reconnus qu'à la condition qu'ils présentent des garanties de sécurité, relatives tant à leur imputabilité qu'à leur intégrité, équivalentes à celle d'un écrit traditionnel. Il n'existe dès lors aucune raison d'opérer une discrimination qui s'inscrit en faux contre l'assimilation recherchée des documents numériques à de véritables actes sous seing privé.

Rien n'empêchera, par ailleurs, le juge saisi d'une contestation d'apprécier lequel des documents, signés de façon manuscrite ou électronique, doit être préféré. Un tel examen au cas par cas paraît une solution à la fois plus souple et plus sûre que celle consistant à rejeter d'office toute preuve par un écrit électronique contre un écrit classique ([61]). La foi que nous nous apprêtons de faire aux actes sous seing privé électronique trouve ainsi son prolongement dans la confiance que notre système probatoire doit prêter également au juge.

([60]) Cf. X. Linant de Bellefonds, L'internet et la preuve des actes juridiques, Expertises, juin-juillet 1997, p.225 et s.

([61]) P. Leclercq, Propositions diverses d'évolutions législatives sur les signatures électroniques, Droit de l'informatique et des télécommunications, 1998/3, p.19 et s.