La signature dans les contrats et les paiements électroniques

Gobert, Didier; Montero, Etienne

Published in:
DA/OR

Publication date:
2000

Document Version
le PDF de l'éditeur

D. GOBERT et E. MONTERO, *DA/OR*, avril 2000, n° 53, pp. 17 à 39.

La signature dans les contrats et les paiements électroniques: l'approche fonctionnelle

Didier GOBERT, Assistant,
Centre de Recherches Informatique et Droit,
Faculté de droit, FUNDP, Namur
Cofondateur de *e*-Consult

Etienne MONTERO, Professeur,
Faculté de droit, FUNDP, Namur

Publié au DA/OR, avril 2000, n° 53, pp. 17 à 39.

Introduction générale

1. La signature électronique a fait sa première apparition dans le secteur bancaire pour accompagner les paiements par carte, si tant est qu'on puisse, dans ce cas, l'assimiler à une signature au sens juridique de la notion (à cet égard, *infra*, n° 13). Aujourd'hui, son utilisation connaît un essor fulgurant dans le contexte de la communication par le biais des réseaux, qui permettent la multiplication des échanges de données en vue de conclure, modifier ou anéantir des actes juridiques, envoyer des factures ou effectuer des paiements. L'ouverture des réseaux par suite de leur interconnexion, grâce au recours à un langage de communication commun (le protocole TCP/IP, qui est à la base de l'Internet), a signifié l'émergence d'un vaste marché sans frontière et l'explosion du "commerce électronique" à l'échelle mondiale. Il est clair que ce commerce en réseaux ouverts ne pourra prospérer que dans un cadre juridique précis et rassurant. Ce qui implique de lever les incertitudes concernant, notamment, la valeur juridique accordée aux actes et signatures électroniques. A présent, il est largement admis que la réforme du droit de la preuve devient incontournable si l'on prétend promouvoir l'usage d'Internet comme support pour conclure des contrats et réaliser des paiements.

2. Il est hors de propos de reprendre ici tous les éléments du débat actuel relatif à l'adaptation du droit de la preuve[1] aux technologies modernes de l'information[2]. Les suggestions émises par la doctrine visent toutes, d'une manière ou d'une autre, à accorder aux documents signés par un moyen électronique une valeur probatoire analogue aux documents signés manuscritement. Sur le plan de la technique juridique, elles s'orientent principalement dans trois directions: les voies *conventionnelle*, *législative* et *interprétative*.

3. La *voie conventionnelle* s'est imposée naturellement dans le contexte des réseaux fermés (de banque à distance ou d'EDI[3]), à la faveur de l'incontestable caractère supplétif des dispositions légales relatives à la preuve: les contractants ne se privent pas de fixer leurs propres règles probatoires, s'accordant d'ordinaire pour assimiler la signature électronique à la signature manuscrite. Cependant, cette solution, qui exige des rapports préalables et suivis entre parties, cesse d'être une panacée dans les environnements ouverts, tel Internet, où

---

1 Pour un exposé des principes généraux du droit de la preuve, N. VERHEYDEN-JEANMART, *Droit de la preuve*, Précis de la Faculté de droit de l'U.C.L., Bruxelles, Larcier, 1991; R. MOUGENOT, *La preuve*, Rép. not., t. IV, Livre 2, 2e éd., Bruxelles, De Boeck et Larcier, 1997. Sur la signature, voy. la classique et substantielle étude de M. VAN QUICKENBORNE, "Quelques réflexions sur la signature des actes sous seing privé", note sous Cass., 28 juin 1982, *R.C.J.B.*, 1985, pp. 65-104.

2 Pour un aperçu, voir les nombreuses publications citées dans la suite de l'étude.

3 Tels que SWIFT (réseau interbancaire), ASSURNET (dans le secteur des assurances), ODETTE (secteur automobile), GALILEO ou AMADEUS (agences de voyages).

chacun peut nouer des contacts et conclure des actes juridiques avec des partenaires occasionnels.

4. Selon une autre opinion, le droit de la preuve doit nécessairement être réformé par la *voie législative*. Diverses propositions ont été formulées en ce sens. La plus radicale consiste à supprimer la prééminence de la preuve littérale en instaurant un régime généralisé de preuve libre: en ce cas, tous les modes de preuve se trouveraient placés sur le même pied quant à leur recevabilité et à leur force probante[4]. Si pareille solution a le mérite de la simplicité, force est d'admettre qu'elle ne résout rien: côté pile, elle revient à confier au juge le pouvoir largement discrétionnaire de reconnaître ou non, selon sa réceptivité aux nouvelles technologies, une valeur probante aux procédés électroniques de signature; côté face, elle met à charge de la partie qui invoque une inscription informatique de démontrer la fiabilité du procédé utilisé de manière à emporter la conviction du juge. Moins radicales sont les propositions visant à accueillir la signature électronique dans les textes, soit en introduisant une définition large de la signature, susceptible de couvrir les signatures informatiques, soit en définissant ce qu'il faut entendre par ces dernières et en précisant leur force probante. Nous aurons l'occasion de revenir sur ces hypothèses.

5. Plus confiante dans la souplesse des règles de preuve en vigueur, une partie de la doctrine suggère, enfin, que le Code civil ménage, d'ores et déjà, une large place aux preuves informatiques, pourvu que les notions – singulièrement celles, heureusement imprécises et ouvertes, d'écrit et de signature – soient correctement interprétées. Pour l'essentiel, deux points de vue ont été développés par les tenants de la *voie interprétative*.

6. Certains auteurs plaident pour une admission des moyens électroniques de preuve par le biais des *exceptions* au principe de la prééminence de l'écrit signé – "ces trous de souris par lesquels on parvient parfois à faire passer des éléphants"[5]. A leurs yeux, les contrats et paiements électroniques seraient un terrain d'élection pour l'admissibilité de la preuve par toutes voies de droit, justifiée par une impossibilité pratique, résultant des usages, de se procurer une preuve littérale (art. 1348 C. civ.). A moins de solliciter l'article 1347 et considérer le document signé électroniquement comme un commencement de preuve par écrit. Ces analyses ont suscité de justes critiques, non pas tant sur le plan de leur correction juridique que sur leur opportunité et leur aptitude à faire droit aux preuves informatiques. On a fait valoir combien le recours à l'exception de l'article 1348 était intellectuellement peu satisfaisant et risquait de vider l'article 1341 de sa substance, à mesure que se généralisent les actes juridiques dématérialisés conclus *via* les réseaux. La piste du commencement de preuve par écrit souffre les mêmes objections. Elle n'est pas de nature à apporter la sécurité juridique attendue, dans la mesure où la force probante attachée aux documents et signatures électroniques reste tributaire du pouvoir d'appréciation du juge et de son attitude face aux technologies.

7. S'inscrivant également dans la voie interprétative, l'approche dite "fonctionnelle" est nettement plus prometteuse. Elle s'oppose à une lecture que l'on pourrait qualifier de stricte ou

---

4 Ce principe a été introduit dans le Code civil des Pays-Bas en 1988 et est préconisé par la Recommandation (81) 20 du Conseil de l'Europe relative à l'harmonisation des législations en matière d'exigence d'un écrit et en matière d'admissibilité des reproductions de documents et des enregistrements informatiques.

5 Y. COOL, "Signature électronique et signature manuscrite: sœurs ennemies ou sœurs jumelles?", in *Droit des technologies de l'information. Regards prospectifs* (sous la direction de E. MONTERO), Cahiers du C.R.I.D., n° 16, Bruxelles, Bruylant, 1999, pp. 71-94.

formaliste de la signature, qui demeure attachée aux caractéristiques, jugées essentielles, de la signature *manuscrite*, telles que dégagées progressivement par la jurisprudence et la doctrine. Appliquée aux notions du Code civil, pareille approche permettrait de ranger sous les vocables d'écrit et de signature, respectivement certains documents et signatures électroniques. Dès la fin des années 80, s'autorisant de l'absence de définition légale de l'écrit et de la signature, des auteurs ont suggéré d'interpréter aussi largement que possible ces notions de manière à pouvoir y faire entrer certaines preuves issues des techniques modernes[6]. Plus précisément, constituerait un acte sous seing privé, et bénéficierait dès lors de la force probante accordée à ce type d'acte, tout document électronique (ou non) qui remplit, de manière fiable et sûre, les *fonctions* traditionnellement assignées à l'écrit papier signé manuscritement.

8. Une observation encore: les différentes orientations esquissées ne sont pas exclusives l'une de l'autre. Ainsi, certains législateurs ont consacré explicitement, moyennant une réforme de l'article 1348, le recours à cette exception prévue dans le Code civil[7]. Par ailleurs, comme on le verra ultérieurement, d'aucuns considèrent opportun, voire indispensable, que la loi consacre formellement, d'une manière ou d'une autre, l'équivalence fonctionnelle de principe entre les procédés de signature électronique et la signature manuscrite. Sans compter le besoin, plus impérieux encore, de fixer les conditions et critères de sécurité permettant de rencontrer les fonctions traditionnelles de l'écrit signé.

Comme par un effet de zoom, parmi toutes les voies déjà tracées par la pratique (on songe en particulier aux solutions contractuelles) ou envisagées par la doctrine *de lege lata* ou *ferenda*, notre attention se focalisera sur la seule *approche fonctionnelle*. Effectivement, cette dernière tend à s'imposer aussi bien en doctrine[8] que dans divers textes législatifs à l'échelon national et international (*infra*, partie II). Il est vrai qu'elle est la plus séduisante et la plus respectueuse de l'équilibre instauré par notre système normatif en matière probatoire.

Structure de l'exposé

9. Une première partie entend saisir l'approche fonctionnelle dans l'abstrait, c'est-à-dire en dehors de toute référence à des dispositifs normatifs déterminés. Etant donné la relative nouveauté des procédés électroniques de signature, il nous est apparu opportun de présenter brièvement les divers mécanismes existants de manière à fixer les idées et la terminologie en

---

6 Voir les références citées *infra*, en note 8.

7 Ainsi, la loi française du 12 juillet 1980 et la loi luxembourgeoise du 22 décembre 1986.

8 D. SYX, "Vers de nouvelles formes de signature? Le problème de la signature dans les rapports juridiques électroniques", *Dr. inform*., 1986/3, pp. 133-147; M. FONTAINE, "La preuve des actes juridiques et les techniques nouvelles", in *La preuve*, Colloque U.C.L., 1987; J. LARRIEU, "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, pp. 8-19 et I, pp. 26-34 ; M. ANTOINE, J.-F. BRAKELAND et M. ELOY, *Le droit de la preuve face aux nouvelles technologies de l'information et de la communication*, Cahiers du C.R.I.D., n° 7, Bruxelles, E. Story-Scientia, 1991, pp. 38 et s. ; Y. POULLET, "Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve", in *Le droit des affaires en évolutions, Le juriste face à l'invasion informatique*, Colloque ABJE, 24 oct. 1996, Bruxelles, Bruylant, Anvers, Kluwer, 1996, pp. 39 à 67; E. DAVIO, "Preuve et certification sur Internet", *R.D.C.*, 1997, n° 11, pp. 660 à 670 ; D. MOUGENOT, "Droit de la preuve et technologies nouvelles: synthèse et perspectives", *Droit de la preuve-Formation permanente CUP*, Volume XIX, octobre 1997, pp. 45-105 ; M. ANTOINE et D. GOBERT, "Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification", *R.G.D.C.*, juillet-octobre 1998, n° 4/5, pp. 285-310 .

la matière (point A). Ensuite, il s'agit de dégager les fonctions traditionnellement assignées à la signature manuscrite et d'évaluer leur sort sur le terrain des signatures électroniques (point B).

La seconde partie procède à une évaluation critique des différents textes légaux – déjà adoptés ou en passe de l'être, au niveau des Etats ou d'instances supra-étatiques – consacrant, à ce jour, l'approche fonctionnelle. Une mise en lumière des atouts et des insuffisances de pareille approche permet de comprendre, et d'approuver sur le principe, les diverses interventions législatives (point A). Après un tour d'horizon en droit comparé (point B), l'analyse se porte sur les projets de loi belges de réforme du droit de la preuve (point C).

I. L'approche fonctionnelle sous la loupe

A. Description sommaire des formes de signature électronique

10. Les spécialistes s'accordent généralement pour considérer que le terme de *signature électronique* désigne une notion générique englobant divers mécanismes techniques méritant d'être tenus pour des signatures dans la mesure où ils permettent, à eux seuls ou en combinaison, de réaliser certaines fonctions essentielles (identification de l'auteur de l'acte, manifestation du consentement au contenu de l'acte, *etc*.) à cette institution juridique. Ces mécanismes peuvent être regroupés en quatre catégories: la signature manuscrite numérisée, la signature biométrique, le code secret associé à l'utilisation d'une carte et la signature digitale (ou numérique). On présente tour à tour ces différents mécanismes, non sans identifier, en première approximation, certains de leurs avantages et points faibles.

1. La signature manuscrite numérisée

11. Le mécanisme de signature électronique le plus sommaire est sans conteste celui qui consiste à numériser une signature manuscrite. A cet effet, il suffit de scanner le graphisme de manière à le convertir en un fichier informatique. L'«image» numérique ainsi obtenue peut être enregistrée dans la mémoire d'un ordinateur (ou sur un support magnétique mobile). Ainsi, il est loisible au signataire de copier l'image dans un autre fichier et ensuite d'imprimer le document "signé". Si l'imprimante et le papier sont de qualité, le résultat final ressemble, de manière confondante, à l'original. Il saute aux yeux que la force du procédé, soit la simplicité, est aussi sa faiblesse: en effet, quiconque dispose d'un spécimen (papier) de signature ou d'un accès au système ou support magnétique sur lequel celle-ci est stockée peut, lui aussi, la reproduire avec le même succès[9]. C'est dire si le procédé, à lui seul, présente un degré de sécurité technique et, partant, juridique pour le moins aléatoire. Pour ces raisons, il est clair qu'il n'a pas de beaux jours devant lui, à moins d'être combiné à l'usage de la cryptographie (*infra*, n° 15); aussi n'y ferons-nous plus allusion dans la suite de l'étude.

2. L'utilisation combinée d'une carte et d'un code secret

12. Les cartes et codes, utilisés conjointement à des fins de "signature", sont bien connus du grand public. Ce mécanisme s'est développé dans le secteur bancaire de manière à permettre l'accès du public aux guichets automatiques de banque et aux terminaux points de vente. Il rend possible des transferts de fonds et paiements accompagnés d'une "signature

9 Cf. R. MOUGENOT, *op. cit.,* p. 148, n° 121, a).

électronique". Techniquement, le procédé consiste à introduire une carte (à pistes magnétiques ou pourvue d'un microprocesseur) dans un appareil approprié (guichet ou terminal) et à composer un code secret (strictement personnel, généralement désigné par le sigle P.I.N., i.e. Personal Identification Number) à l'aide d'un clavier. A vrai dire, l'utilisation combinée d'une carte et d'un code ne peut être tenue pour une signature électronique au sens strict de la notion, telle que développée dans la présente étude: en effet, ces éléments associés constituent "bien plus un mécanisme d'autorisation d'accès à un système informatique propriétaire qu'un mécanisme de signature susceptible de permettre non seulement la réalisation des mêmes fonctions de la signature classique, mais également de réaliser ces fonctions dans la quasi totalité des situations où se manifeste la signature classique, et ce, tant dans le cadre de réseaux ouverts que fermés"[10].

13. Force est de reconnaître que les fonctions essentielles de la signature ne sont pas *idéalement* remplies[11]. D'une part, sur le terrain de l'identification, on ne peut ignorer les possibilités de fraude. Ni la carte ni le code ne sont vraiment liés à la personne: un tiers peut soustraire une carte et prendre connaissance du code (comp. *infra*, n° 18). Mais il est vrai aussi que le risque n'est pas infiniment plus élevé que celui découlant de la contrefaçon d'une signature manuscrite. D'autre part, la fonction d'appropriation du contenu de l'acte est assurée seulement si l'approbation est donnée au terme de l'opération, ce qui n'est pas toujours le cas. Parfois, en effet, l'introduction de la carte et du code intervient avant l'affichage du message (cf, par exemple, les terminaux disponibles dans les pompes à essence). Ici aussi, l'objection peut être tempérée dès l'instant où l'utilisateur est invité *ex post* à ratifier l'opération conclue[12]. Cependant, il convient de remarquer, avec D. Mougenot, que pareil système de validation a une portée réduite. En effet, l'utilisateur d'un guichet automatique de banque ou d'un terminal-point de vente n'a qu'une possibilité rudimentaire de vérifier la correcte exécution de la transaction par la banque, d'autant que le ticket est émis postérieurement à l'opération, à un moment où cette dernière est irréversible, sauf à protester auprès de la banque.

Plus fondamentalement, l'intérêt de la notion de signature électronique est de pouvoir considérer un document comme un acte sous seing privé de sorte qu'il puisse bénéficier de la force probante attachée à ce type d'acte. A cet effet, il est impérieux qu'à défaut de figurer *physiquement* sur le document, la signature lui soit au moins liée *logiquement*. Or ce n'est pas le cas, la bande journal produite par le système pour attester l'opération ne contenant aucune trace du code secret[13]. Pour cette raison, la carte et le code ne peuvent, en eux-mêmes, être assimilés à une signature[14]. Dans le secteur bancaire, cet inconvénient est surmonté grâce aux conventions conclues entre organismes financiers ainsi qu'entre ceux-ci et leurs clients[15].

3. Les signatures biométriques

---

10 S. PARISIEN et P. TRUDEL, *L'identification et la certification dans le commerce électronique*, Québec, Ed. Yvon Blais Inc., 1996, p. 99.

11 Cf. J. VAN RYN et J. HEENEN, *Principes*, t. IV, 2e éd., n° 431; B. AMORY et Y. POULLET, "Le droit de la preuve face à l'informatique et à la télématique: approche de droit comparé", *D.I.T.*, 1985, pp. 11 et s.; X. THUNIS et M. SCHAUSS, *Aspects juridiques du paiement par carte*, Cahiers du C.R.I.D., n° 1, E. Story-Scientia, 1988, n° 33 et s.; J.-P. BUYLE, "La carte de banque à piste magnétique", *R.D.C.*, 1984, p. 663 et s.

12 R. MOUGENOT, *op. cit.*, p. 150, n° 122; D. MOUGENOT, *op. cit.*, p. 78, n° 33.

13 J.-P. BUYLE, "La carte de paiement électronique", in *La banque dans la vie quotidienne*, Bruxelles, Ed. du Jeune Barreau, 1986, p. 471.

14 D. SYX, *op. cit.*, p. 138, n° 45.

15 Pour des exemples, X. THUNIS et M. SCHAUSS, *op. cit.*, pp. 46-47, n° 74 et 75, et les annexes.

14. La science biométrique s'intéresse aux caractéristiques physiques uniques des personnes, susceptibles de les identifier dans leur individualité. Parmi d'autres procédés, on peut citer l'examen des empreintes digitales (dactyloscopie) ou des vaisseaux sanguins de la rétine de l'œil (rétinoscopie), la reconnaissance vocale ou encore la reconnaissance dynamique de la signature (analyse non du graphisme comme tel, mais de la manière dont il est tracé: vitesse, mouvements, pression sur la plume…)[16]. Pourvu que la particularité biométrique soit liée à un individu et que le lien établi soit sécurisé, ces méthodes peuvent remplir une fonction d'identification, pour des applications diverses (accès à des salles protégées, à des coffres, enquête criminelle, *etc*.), et notamment, à des fins de signature.

Sauf exceptions (on songe bien sûr à l'analyse des empreintes digitales, mais aussi aux progrès notables de la reconnaissance vocale), la plupart de ces techniques en sont encore à un stade expérimental. En particulier, leur utilisation courante à des fins de signature se heurte à divers obstacles pratiques: lourdeur et coût élevé de leur implémentation, qui nécessite un lecteur *ad hoc* permettant la numérisation du paramètre physique concerné. Entre autres inconvénients, on mentionne également le fait que certains caractères physiques peuvent être sujets à des variations (la voix, l'influence du stress pour l'analyse de la dynamique de la signature…) et la réticence du public à l'usage de certains procédés[17]. Ces divers facteurs expliquent que les procédés de signature biométrique soient actuellement très peu utilisés dans les transactions sur les réseaux.

Au demeurant, si les procédés biométriques permettent d'identifier l'auteur de la signature, on estime en général qu'ils ne garantissent pas nécessairement l'expression correcte de son consentement (*infra*, n° 20). La certitude de l'*animus signandi* dépendra largement de la fiabilité du système technique et de la procédure d'ensemble dans laquelle s'intègre l'application.

4. La signature numérique ou digitale

15. La signature dite numérique ou digitale repose sur les procédés de cryptographie[18]. Pour éviter toute confusion, il convient de noter que ceux-ci peuvent servir non seulement à des fins de signature, mais aussi dans le but de garantir la confidentialité des échanges. Cette dernière fonction, appelée chiffrement[19], est généralement réalisée à l'aide de produits qui, pour la plupart, sont fondés sur le *Data Encryption Standard* (DES). Il s'agit d'un système cryptographique à clé unique (ou à clé secrète) utilisant un algorithme qui, comme le suggère son nom, chiffre et déchiffre un message à l'aide d'une seule clé. Un tel procédé est surtout efficace dans les réseaux fermés; la nécessité de faire connaître la clé à son destinataire, avec les inévitables risques d'interception, entraîne qu'à lui seul, il est, en revanche, inadapté aux réseaux ouverts ou pour une utilisation à des fins de signature.

---

16 A ce sujet, M. FONTAINE, étude précitée; D. SYX, *op. cit*., p. 138, pp. 143-144, n° 79 à 82.

17 Voir notamment M. ANTOINE, J.-F. BRAKELAND et M. ELOY, *op. cit*., p. 21.

18 Pour une explication détaillée, S. PARISIEN et P. TRUDEL, *op. cit*., pp. 93 à 113; J. HUBIN, *La sécurité informatique, entre technique et droit*, Cahiers du C.R.I.D., n° 14, E. Story-Scientia, 1998, spéc. pp. 68-112.

19 Lequel consiste en la transformation d'un message dit "en clair" en une chaîne de caractères alphanumériques qui ne sont compréhensibles que pour la personne autorisée.

Ce problème du partage des clés a été résolu par le développement de la cryptographie asymétrique, dite aussi "à clé publique". Celle-ci permet non seulement d'expédier des messages confidentiels dans de meilleures conditions de sécurité, mais aussi de réaliser des signatures numériques. Le mécanisme repose sur l'utilisation d'une paire de clés, l'une secrète et l'autre publique, unies entre elles par une formule mathématique. L'application la plus répandue de cryptographie à clé publique est le R.S.A., du nom de ses concepteurs (Rivest, Shamir et Adleman, du M.I.T.).

Sous le bénéfice de précisions ultérieures (*infra*, n° 22), utilisé à des fins de signature numérique, le procédé de cryptographie asymétrique fonctionne comme suit: le message est signé par son auteur à l'aide de sa clé privée, puis il est expédié au destinataire, qui peut le déchiffrer uniquement avec la clé publique complémentaire à la clé privée de l'émetteur. Ainsi, le destinataire est certain que le message émane bien de son auteur dûment identifié[20]. Pour assurer la confidentialité d'un échange, l'expéditeur procédera différemment: il chiffrera le message à l'aide de la clé publique du destinataire, qui pourra uniquement le déchiffrer au moyen de sa propre clé secrète. Ainsi sera-t-il le seul à pouvoir prendre connaissance du message. Il va de soi que les deux fonctions peuvent être combinées pour l'envoi d'un message à la fois confidentiel et signé.

16. Reste à préciser que l'utilisation de la cryptographie à clé publique suppose l'organisation de la publicité des clés publiques et l'instauration d'un mécanisme de contrôle visant à s'assurer que celles-ci correspondent bien aux personnes qui s'en prétendent titulaires. Cette double mission de publicité et de certification est actuellement assumée par un tiers certificateur (appelé encore "autorité de certification"). Il s'agit d'un organisme indépendant habilité, d'une part, à *vérifier l'identité* des titulaires de clé publique et à *générer des certificats*, soit des structures de données signées digitalement qui font le lien entre une personne et sa clé publique, et, d'autre part, à *assurer la publicité* la plus large des certificats ainsi émis[21]. L'autorité de certification est également tenue de maintenir à jour le répertoire contenant les certificats de clé publique, en veillant, selon le cas, à leur suspension, révocation ou renouvellement. Remarquons ici le rôle capital de ce tiers à la communication électronique pour assurer la fiabilité de la signature numérique, en vue d'échanges contraignants dans les réseaux ouverts. Au fond, le recours à ce genre de procédure, inévitable en réseaux "ouverts", revient en quelque sorte à inscrire les relations jugées sensibles dans un cadre *fermé* et sécurisé.

B. Les fonctions de la signature: du papier à l'électronique

1. Des fonctions anciennes et nouvelles

17. Il convient à présent d'examiner de plus près quelles sont les fonctions assignées à la signature classique afin de vérifier si elles sont adéquatement remplies par les signatures électroniques.

---

20 Pour autant qu'un certificat délivré par une autorité de certification confirme que la clé publique appartient réellement à l'émetteur.

21 Pour plus de détails, S. PARISIEN et P. TRUDEL, *op. cit*., pp. 117 et s.; E. DAVIO, "Certification, signature et cryptographie", in E. MONTERO (éd.), *Internet face au droit*, Cahiers du C.R.I.D., n° 12, E. Story-Scientia, 1997, pp. 80 et s., et du même auteur, "Preuve et certification sur Internet", étude précitée; M. ANTOINE et D. GOBERT, *op. cit*., spéc. pp. 293 et s.

Traditionnellement, la doctrine considère que la signature remplit une double fonction: elle permet d'identifier l'auteur d'un acte et exprime son adhésion au contenu de ce dernier. On verra que divers mécanismes de signature électronique permettent de satisfaire à ces exigences essentielles de l'institution. Certains permettent, en sus, de conférer à ces fonctions une efficacité et une importance nettement plus significatives.

A la réflexion, trois autres fonctions de la signature peuvent être identifiées, qui méritent également quelque attention. Tout d'abord, l'avènement de la signature électronique a mis en évidence une troisième fonction: elle sert aussi à vérifier si l'intégrité de l'acte a été préservée au cours de l'échange. Comme on le verra, à défaut d'être radicalement neuve, cette fonction présente, dans l'environnement numérique, un visage nouveau. Une quatrième fonction, subsidiaire sans doute, est rarement évoquée: il s'agit de la vocation de la signature à conférer à un document le statut d'original. Il faudra examiner ce qu'il advient de ce rôle corollaire, mais essentiel, de la signature dans le contexte de la communication en réseau. C'est le critère et le sort de la distinction entre copie et original qui se joue ici. Enfin, les débats actuels sur la signature ont (re)mis en lumière une fonction psychologique, voire "magique", de la signature. Qu'en reste-t-il dès l'instant où, empruntant une forme électronique, la signature se trouve privée de son attache quasi physique à la personne? Cette disparition du lien entre signature et personnalité prête-t-elle à quelque conséquence fâcheuse?

Au total, en élargissant quelque peu le champ de l'analyse classique, les fonctions de la signature sont comptées au nombre de cinq. Il s'agit ici de présenter leurs facettes actuelles, en les contrastant avec celles qui étaient les leur au temps où triomphait le papier comme support éminent des actes juridiques.

2. L'identification de l'auteur de l'acte

18. La fonction première de la signature est de permettre l'identification de l'auteur d'un document. Bien que la loi ne définisse pas la signature, une partie de la doctrine fait de l'apposition du nom une exigence nécessaire de celle-ci. Telle était aussi la position d'une frange non négligeable de la jurisprudence jusqu'à ce que la Cour de cassation adopte une position plus souple, en décidant que "la signature… est la marque manuscrite par laquelle le testateur révèle habituellement sa personnalité aux tiers"[22]. Formulé à propos des testaments olographes, il est incontestable que cet enseignement est applicable à toute signature[23]. Quant à sa portée, il paraît clair que l'emploi du nom patronymique tel qu'il résulte de l'état civil n'est pas exigé pourvu que ne subsiste aucun doute sur l'identité du signataire.

L'utilisation de la cryptographie asymétrique à des fins de signature permet de remplir, efficacement et de manière sûre, cette fonction d'identification. Pour autant que les clés secrètes soient conservées dans de bonnes conditions de sécurité, le risque de fraude est ici, sinon nul, en tout cas nettement moins élevé que celui relatif à l'utilisation des cartes et codes pour signer. Les experts considèrent que les cryptosystèmes performants, tel le DES ou le PGP, sont pratiquement inviolables et capables de résister à toutes les attaques. En outre, des mécanismes d'opposition et de révocation des clés existent, dans tous les systèmes, pour parer à toute éventualité.

---

22 Cass., 7 janv. 1955, *Pas*., 1955, I, p. 456. Dans le même sens, Cass., 2 oct. 1964, *Pas*., 1965, I, p. 106.

23 R. MOUGENOT, *op. cit*., p. 143, n° 110, et les réf.

19. Cela étant, il y a lieu de remarquer ici que la fonction d'identification se présente désormais sous un jour radicalement différent. Au point que l'on peut affirmer que, sous cet angle, la finalité de la signature change véritablement. Dans les rapports contractuels classiques, le rôle d'identification assigné à la signature manuscrite est mineur: la vérification de l'identité n'intervient qu'*a posteriori*, sur le seul *plan probatoire*, en cas de litige[24]. Ainsi en est-il car d'autres facteurs entrent en ligne de compte: la reconnaissance physique entre parties présentes, la familiarité de la voix, la présentation de documents d'identité produits par des autorités officielles, *etc*. Ce n'est qu'en cas de contestation sur l'existence ou l'étendue d'un engagement qu'est sollicitée la fonction d'identification de la signature pour *établir* la présence physique à l'acte du débiteur récalcitrant et son consentement au contenu de l'acte.

Dans les réseaux fermés, l'identification repose également sur la maîtrise préalable de l'environnement. En effet, un tel réseau est géré par une entité unique, qui exerce un contrôle sur ses composantes techniques (interfaces de communication, sécurité, contenus échangés…) et sur les utilisateurs. La participation à un réseau fermé est généralement subordonnée à une procédure d'enregistrement, les membres se connaissent en principe et ont préalablement adhéré à une convention-cadre appelée à régir leurs relations commerciales. En revanche, les réseaux ouverts se présentent comme une structure décentralisée, sans point unique de contrôle, et où des relations peuvent se nouer entre personnes qui, souvent, ne se connaissent pas. Dans ce contexte, la signature est appelée à remplir, à elle seule, la fonction d'identification. Par l'utilisation de la cryptographie asymétrique, en effet, l'identité du signataire est établie et formellement vérifiée préalablement à la conclusion de la transaction[25]. La signature numérique apparaît comme un élément déterminant dans l'identification de l'interlocuteur en ce qu'elle permet de s'assurer de l'expression correcte et sûre de son consentement. Ainsi est-il permis de conclure qu'elle a vocation à jouer un rôle déterminant, non plus seulement sur le terrain *probatoire*, mais au niveau de la *formation* même du contrat. Les développements actuels de la praxis en matière de certification des signatures et du contrôle systématique de celles-ci prouvent que les parties en usent comme d'un instrument approprié pour s'assurer de la « validité » des contrats formés par le biais des réseaux. Sans conclure pour autant au besoin d'un type nouveau de formalisme, on résiste mal à la tentation de faire l'hypothèse d'une orientation future en ce sens.

3. L'adhésion au contenu de l'acte

20. La deuxième fonction de la signature, inséparablement unie à la première, est de manifester l'adhésion du signataire au contenu de l'acte. En apposant sa signature, en principe au pied de l'acte, il fait état de sa volonté d'en approuver, dans son intégralité, la teneur. Selon une jurisprudence constante, la signature doit être manuscrite, autographe: elle doit être tracée, de la main du signataire, directement sur le document lui-même, ce qui exclut l'usage d'un papier carbone[26] ou – sauf dispositions légales en sens contraire – d'un autre élément

---

24 Voir S. PARISIEN et P. TRUDEL, *op. cit*., not. p. 101; D.G. MASSE, "L'autoroute de l'information: convergence du droit et de la technologie", sur le web: http://www.droit.umontreal.ca/; E. DAVIO, *op. cit*., *Internet face au droit*, p. 77.

25 Par contre, avec la signature biométrique, la vérification de l'identité ne s'effectue qu'en cas de litige, c'est-à-dire *ex post*. Il s'ensuit que cette dernière ne permet pas d'assurer la fonction primordiale de non-répudiation, contrairement à la signature numérique fondée sur la cryptographie asymétrique. Cette assertion doit néanmoins être nuancée dans le cas où le destinataire disposerait d'un échantillon de la signature biométrique aux fins de vérification *a priori.*

26 Cass., 28 juin 1982, précité.

intermédiaire (cachet, sceau, griffe…)[27]. Ces différentes exigences visent à lever tout doute quant à la volonté du signataire de s'approprier le contenu de l'acte. Le caractère nécessairement *manuscrit* de la signature n'est pas une exigence essentielle de la notion, il est lié au rôle historique du papier comme support privilégié des actes juridiques. Quant à la place habituelle de la signature, au bas de l'acte, elle ne résulte pas d'un principe légal. L'important, ici aussi, est de pouvoir s'assurer, avec certitude, de l'adhésion à la *totalité* de l'acte. Il n'est d'ailleurs pas contesté qu'en considération des circonstances, le juge peut être amené à admettre qu'une signature tracée à un autre endroit que la fin de l'acte couvre le tout[28].

Dès l'instant où la clé de chiffrement est appliquée de manière volontaire et personnelle, à l'exclusion de toute opération purement automatique, par l'auteur d'un document électronique, il est permis de considérer qu'il exprime son consentement à l'ensemble du contenu de celui-ci. Encore faut-il que la signature soit liée *logiquement* au document, à défaut d'un lien (quasi) physique entre les deux (dans le cas des écrits signés manuscritement). Cette exigence – qui renvoie à la question de l'intégrité (*infra*, n° 22) – conduit la doctrine à estimer que la signature électronique suppose nécessairement une *transformation de l'écrit* (*infra*, spéc. n° 55). D'où l'insuffisance des mécanismes de signature électronique qui ne reposent pas sur pareille opération (les cartes et codes, les signatures biométriques utilisées seules…) et, à l'inverse, l'intérêt des procédés de cryptographie à clé publique.

21. Sur le rôle de la signature pour marquer le consentement au contenu d'un acte juridique, on formulera, en passant, une dernière observation, d'ordre plus psychologique. Un auteur a fait valoir que la contrainte de l'écrit papier a le mérite d'attirer l'attention du signataire sur la portée juridique de son geste[29]. Celui qui s'apprête à se lier juridiquement prend conscience de son engagement au moment de signer l'acte écrit (*instrumentum*), qui solennise en quelque sorte l'acte intellectuel (*negotium*). Au contraire, dans l'environnement électronique, une partie peut se trouver engagée dans des liens contractuels, par un simple "clic", sans formalisme aucun. Cet inconvénient n'a pourtant rien d'une fatalité. Pour y remédier, il est possible de prévoir une procédure de validation, soit l'affichage préalable d'un message d'avertissement (du type: "attention, vous êtes sur le point de signer un document qui vous engage juridiquement…"). Mais surtout, ne peut-on penser que le fait de recourir à un procédé de signature électronique est, en soi, susceptible d'aider le signataire à prendre la mesure de son engagement?[30]

4. La vérification de l'intégrité

22. Une troisième fonction de la signature a été mise à jour récemment: il s'agit du maintien de l'intégrité du contenu de l'acte[31]. En réalité, la doctrine classique n'en souffle mot. En effet, sous l'empire de la signature manuscrite, cette fonction est assurée, non au moyen de la signature elle-même, mais par le biais du support papier sur lequel elle figure nécessairement.

---

27 A ce sujet, R. MOUGENOT, *op. cit*., p. 143, n° 111, p. 146, n° 113 et p. 145, n° 112, et les réf.

28 H. DE PAGE, *Traité*, t. III, 3e éd., n° 777; M. VAN QUICKENBORNE, note précitée, p. 81, n° 19; R. MOUGENOT, *op. cit*., p. 147, n° 119.

29 X. LINANT DE BELLEFONDS, "L'internet et la preuve des actes juridiques", *Expertises*, 1997, p. 226.

30 Dans la mesure où il n'utilise pas sa signature électronique pour d'autres formes de communication en réseau. On peut aussi s'interroger sur la plénitude du consentement dans l'univers de l'écrit papier dès lors que la portée de nombreuses dispositions contractuelles échappe bien souvent au non averti.

31 M. ANTOINE et D. GOBERT, *op. cit*., p. 290.

Il s'agit d'un support inaltérable (les fraudes sont difficiles à dissimuler: les ajouts ou ratures se décèlent facilement) et stable (le papier se dégrade peu). Ces qualités fonctionnelles du papier expliquent, à cet égard, qu'il ait été placé au sommet dans la hiérarchie des modes de preuve. Le contenu étant, pour ainsi dire, matériellement indissociable du support, ce dernier permet d'assurer l'intangibilité et la non-répudiation du contenu.

Dans l'environnement électronique, cette fonction se déplace doublement: du support vers le contenu, et ce, par le biais de la signature. *Primo*, à défaut d'une sécurité au niveau de la structure des réseaux (ouverts surtout), il s'agit d'assurer la sécurisation de chacun des *contenus* échangés. *Secundo*, cette sécurisation s'effectue, non plus par le biais du support des actes, mais au moyen de leur signature.

En particulier, la signature numérique, fondée sur la cryptographie asymétrique, permet de vérifier adéquatement et de façon certaine si l'intégrité à été préservée. La fonction dite de "hachage irréversible" prend ici toute son importance. Elle consiste à appliquer au message à expédier une opération mathématique de manière à produire un condensé digital du message. Ce condensé est ensuite encodé à l'aide de la clé privée: le résultat constitue la signature numérique. Le "petit" fichier crypté ainsi obtenu sera expédié simultanément à l'envoi du message lui-même (en clair ou chiffré lui aussi). Pour déchiffrer le fichier signature, le destinataire utilise la clé publique de l'expéditeur. Il lui suffit alors d'appliquer le même fonction de hachage au message reçu (préalablement déchiffré, au besoin, à l'aide de sa clé privée) et de comparer le condensé ainsi généré avec celui transmis par l'émetteur. Si une différence est notée entre les deux condensés, il faut en conclure que le message a subi une altération au cours de la transmission. Ainsi, grâce à la fonction de hachage et la comparaison des deux condensés, le destinataire est absolument certain de l'intégrité du message reçu. Il convient de remarquer que le détour par la fonction de hachage n'est pas en soi indispensable. Le message émis pourrait être encodé directement par l'émetteur à l'aide de sa clé privée. Une fois le fichier signature déchiffré, le destinataire serait pareillement à même de procéder à la comparaison des messages et de vérifier ainsi l'intégrité. Cependant, l'encodage d'un condensé et la comparaison de fichiers de petites tailles se font plus aisément et rapidement.

Force est de constater qu'à ce niveau, la signature, en tant que telle, est appelée à remplir une fonction jusqu'ici inédite. On relève aussi le rôle déterminant de cette fonction dans l'environnement, peu sûr, des réseaux ouverts. La signature numérique fondée sur la cryptographie à clé publique – dont l'authenticité a pu être vérifiée par l'examen du certificat émis à l'intervention d'une autorité indépendante – permet, en quelque sorte, de "fermer le système", grâce à une sécurisation des flux de données et messages réellement importants.

23. Le même procédé de cryptographie permet aussi d'assurer l'intégrité (du contenu) *dans la durée*, peu importe à cet égard que le document, assorti d'une signature numérique, soit inscrit sur un disque dur (exploité en ligne) ou ait été soustrait à l'informatique en temps réel, pour *archivage* (inscription sur un CD-ROM, une bande plombée…)[32]. En toute hypothèse, encore faut-il avoir prévu le moyen d'obvier à l'éventuelle obsolescence des supports (moyennant leur rajeunissement), des clés et des certificats de clé publique[33]. Ces deux derniers aspects sont normalement du ressort des autorités de certification, qui veilleront à recréer une nouvelle

---

32 Comp. X. LINANT DE BELLEFONDS, *op. cit*., p. 226.

33 On sera également attentif au problème de la lisibilité, le temps passant, des documents pourvus d'une signature numérique. En effet, il peut devenir malaisé de relire des documents créés avec des outils informatiques introuvables ou dépassés et de restituer en clair un document chiffré. Sur ce point, E. DAVIO, "Preuve et certification sur Internet", *op. cit*., chap. 3, section 3.

paire de clés et un nouveau certificat (si la paire de clés utilisées pour signer ne présente plus un degré de sécurité suffisant) et, plus largement, à contrôler que les certificats émis sont toujours exacts et conformes à la réalité (voir aussi *infra*, n° 25).

Si la technique de la signature numérique permet sans conteste de réaliser simultanément les fonctions d'identification et d'intégrité, tel n'est pas le cas de tous les procédés de signature électronique. Ainsi, la signature manuscrite numérisée et les signatures biométriques ne permettent pas de garantir l'intégrité du document transmis, sauf à être combinées avec un mécanisme de cryptographie.

5. L'attribution à un document du statut d'« original »

24. La signature remplit une quatrième fonction, rarement évoquée comme telle: elle permet de conférer à un document le statut de document original. Il s'agit là d'une exigence essentielle de l'acte sous seing privé qui, par définition, doit être un écrit original (c'est-à-dire signé). Avec l'apparition des supports informatiques et la facilité de reproduction des données numériques y figurant, la distinction original/copie se trouve quelque peu bousculée. On aurait tort de croire que toute reproduction d'un document informatique s'analyse en une copie. En effet, l'unicité d'un document n'est pas la condition de son originalité, comme l'atteste la formalité des originaux multiples imposée par l'article 1325 du Code civil. Contrairement à ce qui est parfois affirmé, l'existence d'une garantie fiable quant à l'intégrité d'un document ne suffit pas davantage au maintien de sa forme originale (*infra*, n° 39 et n° 52). En fait, c'est la *signature* qui élève un document au rang d'original. La copie s'en distingue précisément par la circonstance qu'elle en est une transcription non signée[34]. La technique informatique présente la particularité de rendre aisée la reproduction, en original ou en copie, d'un document. Dès lors que la signature de l'émetteur reste attachée au document nonobstant la transmission et que son authenticité peut être vérifiée, le nouveau document a valeur d'*original*, à l'instar du document *originaire*. Dans le cas contraire, il s'analyse en une copie et a valeur de commencement de preuve par écrit ou de simple présomption. Ici encore, on doit constater que ce n'est plus le support qui assure l'indispensable maintien de l'intégrité du document, mais la signature, dont le mécanisme permet de *figer logiquement le contenu* du document (*supra*, n° 22)[35].

25. Il s'ensuit que le document muni d'une signature numérique se dégrade en copie dès l'instant où le certificat de clé publique se trouve révoqué ou frappé de caducité car, dans ce cas, la signature ne peut plus être vérifiée. D'où la haute importance de la mission de gestion des certificats confiée aux autorités de certification. Il leur appartient de veiller à suspendre, voire révoquer, les certificats ou de procéder à leur renouvellement. En cas d'obsolescence des clés et, partant, des signatures, par suite d'une évolution technique (qui fait qu'un code indéchiffrable hier ne l'est plus aujourd'hui), il leur faudra aussi émettre un nouveau certificat.

Pour nuancer ce propos, notons néanmoins qu'un document signé numériquement pourrait garder la valeur d'original, alors même que le certificat serait révoqué ou aurait expiré, voire que la technique serait devenue obsolète, si le document est conservé par un tiers indépendant dans le cadre d'un régime sécurisé d'archivage électronique, combiné à un système d'horodatage des documents. Ceci permettrait de répondre aux nombreuses exigences légales

---

34 H. DE PAGE, *Traité*, t. III, 3e éd., n° 832; R. MOUGENOT, *op. cit.*, p. 185, n° 187; N. VERHEYDEN-JEANMART, *op. cit.*, p. 201, n° 417.

35 A ce sujet, E. DAVIO, *op. cit.*, *R.D.C.*, 1997, n° 11, pp. 664 et s.

qui imposent la conservation des originaux pendant un nombre d'années (5, 10, 20 ou 30 ans) largement supérieur à la durée du certificat. Pour ce faire, encore faut-il déterminer les conditions techniques et juridiques auxquelles l'archivage pourra être effectué. Ce problème, qu'il n'est naturellement pas possible d'examiner ici en détail, ne semble pas insurmontable et doit nécessairement être pris en compte par le législateur.

Quoi qu'il en soit, on retiendra de tout ceci que la distinction original/copie garde toute sa vigueur et sa pertinence dans l'environnement informatique.

26. Enfin, qu'advient-il du prescrit de l'article 1325 du Code civil en ce qui concerne l'échange de données électroniques en vue de conclure un acte sous seing privé? Cette hypothèse peut être rapprochée du cas des lettres missives échangées pour la conclusion de contrats. Or, celles-ci sont soumises aux règles de forme des actes sous seing privé, à l'exclusion de celles jugées incompatibles avec leur nature. Ainsi, une doctrine et une jurisprudence unanimes considèrent que la formalité des originaux multiples, imposée en matière d'actes sous seing privé constatant des conventions synallagmatiques, ne leur est pas applicable[36]. L'analogie de situations porte à considérer que la règle de l'article 1325 peut aussi être écartée dans la communication électronique[37]. Cela étant, rien ne s'oppose, *de facto*, à l'accomplissement des formalités prévues par cette disposition. Il suffit d'établir un original pour chaque partie ayant un intérêt distinct et de mentionner, sur chaque exemplaire, le nombre d'originaux. Il est admis, du reste, qu'une partie ne signe pas l'exemplaire qui lui est destiné pourvu qu'il ait été signé par les autres parties auxquelles on l'oppose[38].

6. La dimension "magique"

27. Enfin, un auteur a soutenu que la signature remplissait également une fonction "magique"[39]. Le tracé d'un graphisme original en guise de signature est présenté comme une manière d'exprimer vis-à-vis des tiers un trait de sa personnalité. Sans nier la portée psychologique de la signature, il convient, à notre avis, de la relativiser et de remarquer qu'elle n'est pas essentielle à la notion. Nombre de signataires y accordent peu d'importance, préférant sacrifier l'élégance ou la singularité du graphisme à la lisibilité de leur nom patronymique. A l'inverse, si un graphisme est complètement illisible au point que son auteur ne peut être identifié, il ne constitue pas une signature valable[40]. Car, en définitive, que la signature porte réellement la marque de la personnalité importe moins que son aptitude à identifier son auteur. Et, à n'en pas douter, la fonction d'identification de la signature peut fort bien se passer des fioritures.

---

36 Cf. R. MOUGENOT, *op. cit*., p. 155, n° 133; N. VERHEYDEN-JEANMART, *op. cit*., p. 295, n° 639 et les réf.; P. VAN OMMESLAGHE, "Examen de jurisprudence (1974 à 1982). Les obligations", *R.C.J.B*., 1988, p. 169, n° 248.

37 E. MONTERO, "Internet et le droit des obligations conventionnelles", in *Internet sous le regard du droit*, *Editions du Jeune Barreau de Bruxelles*, 1997, p. 54, n° 13; D. MOUGENOT, "Droit de la preuve et technologies nouvelles: synthèse et perspectives", *op. cit*., p. 81, n° 36.

38 R. MOUGENOT, *op. cit*., p. 156, n° 137; N. VERHEYDEN-JEANMART, *op. cit*., n° 532.

39 W. WILMS, "Van handteking naar elektronische notaris. De validering van elektronische communicatie", *R.W*., 1995-1996, p. 840.

40 R. MOUGENOT, *op. cit*., p. 144, et les références jurisprudentielles citées.

II. L'approche fonctionnelle à travers les textes

A. Le législateur mis à contribution

1. Les vertus de l'approche fonctionnelle

28. Pendant de nombreuses années, on a pu se dispenser d'une réforme législative du droit de la preuve en vue de l'adapter aux nouvelles technologies de l'information. Comme on l'a vu, en effet, le caractère fermé des réseaux a généralement permis aux parties de combler par voie conventionnelle les vides de la loi. De fait, les intéressés n'ont pas manqué de faire usage de cette faculté d'aménager les règles supplétives de la preuve, notamment en conférant une valeur juridique à certains mécanismes de signature électronique.

Le développement relativement récent d'Internet a changé la donne. Caractérisé par son ouverture, le réseau des réseaux permet au tout venant d'y accéder librement et à tout moment, y compris pour nouer des relations juridiques occasionnelles avec des partenaires inconnus au préalable. La solution contractuelle n'étant plus de mise en pareille hypothèse, il devient difficile de se satisfaire du régime probatoire attaché à l'acte sous seing privé, et plus exactement de la conception formaliste de la signature qui a été retenue par la Cour de Cassation[41], bien avant l'avènement d'Internet il est vrai.

S'il est aisé d'affirmer qu'on ne peut plus se satisfaire uniquement du concept de signature manuscrite, il est par contre plus difficile de déterminer les évolutions qui devraient être prônées afin de pouvoir faire preuve au moyen d'un document signé électroniquement. Toutefois, l'idée d'adopter une approche fonctionnelle du concept de signature a fait du chemin à la fois en doctrine (*supra*, n° 7 et 8, et les réf.) et dans divers textes législatifs nationaux[42] et internationaux[43].

Ainsi, en consacrant une définition fonctionnelle de la signature, on considère que constitue une signature, et bénéficie dès lors des effets juridiques liés à celle-ci, non seulement la signature manuscrite, mais également tout mécanisme qui permet de remplir avec une fiabilité raisonnable les *fonctions* traditionnelles de la signature.

2. La nécessité d'une modification légale

29. Il est permis de s'interroger sur la nécessité de légiférer pour consacrer la piste, largement approuvée, des équivalents fonctionnels. Certains auteurs estiment qu'une modification de la

---

41 Cass., 24 févr. et 3 nov. 1910, *Pas.*, 1910, I, pp. 241 et 475 ; Cass., 1er mars 1917, *Pas.*, 1917, I, p.118 ; Cass., 7 janv. 1955, *Pas.*, 1955, I, p. 456 ; Cass., 2 oct. 1964, *Pas.*, 1965, I, p.106 ; Cass., 28 juin 1982, *R.C.J.B.*, 1985, p. 69, note M. VAN QUICKENBORNE.

42 Projet de loi belge visant à "modifier certaines dispositions du Code civil relatives à la preuve des obligations", *Doc. parl.*, Ch. Repr., sess. ord. 14 avril 1999, n° 2141/1 (ce texte a été déposé lors de la précédente législature et n'a pas été relevé de caducité par La Chambre nouvellement constituée) ; Avant-projet de loi luxembourgeois sur le commerce électronique : http://www.droit.fundp.ac.be/crid/eclip/default.htm.

43 Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation, 1996, Nations Unies, New York, 1997, disponible à l'adresse suivante : http://www.un.or.at/uncitral/fr-index.htm ; Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *J.O.C.E.*, L 13/12 à 20 du 19 janvier 2000.

loi n'est pas souhaitable[44]. Ils font confiance aux juges pour développer les potentialités des textes existants. On doit leur donner raison et tort à la fois.

On doit leur donner en partie raison car, comme le constate D. Mougenot, la « jurisprudence a déjà fait preuve d'une grande capacité à élaborer des systèmes juridiques complexes à partir de textes très généraux »[45] . D'autre part, certaines décisions ont interprété les concepts d'écrit et de signature d'une manière évolutive[46].

Mais on doit également leur donner tort pour plusieurs raisons. D'une part, ces décisions sont isolées et manifestement insuffisantes pour opérer un renversement de la jurisprudence actuelle. Comme le fait remarquer D. Mougenot, pour que la jurisprudence puisse exercer sa capacité d'innovation, « encore faut-il que les juges aient à se prononcer sur des cas d'espèce. Or, nous avons relevé le petit nombre de litiges soumis à la justice (…) La mise sur pied d'un droit de la preuve de nature jurisprudentielle risque fort de prendre du temps et de rester lacunaire »[47]. Du reste, on ne peut plus se permettre d'attendre car le nombre de transactions conclues *via* Internet augmente de manière exponentielle en sorte que l'insécurité juridique se fait de plus en plus ressentir. D'autre part, même si certains juges ont eu l'occasion de se prononcer en faveur d'une approche fonctionnelle, ceux-ci ne règlent le problème que partiellement. Pour illustrer notre propos, limitons-nous à commenter brièvement un arrêt de la Cour de cassation française relativement récent et assez novateur.

30. L'arrêt de la chambre commerciale de la Cour de cassation française du 2 décembre 1997[48] porte sur une affaire de cession de créance. La question était de savoir si l'acceptation de la cession peut être valablement donnée par le débiteur, sous la forme d'une télécopie. En l'espèce, la Cour répond favorablement en jouant, non pas sur le concept de copie fidèle et durable, ni sur celui de commencement de preuve par écrit, mais tout simplement sur le concept d'écrit (acte sous seing privé). Pour la Cour, le concept d'écrit peut être interprété largement pour autant qu'il réponde à certaines fonctions. L'écrit « peut être établi et conservé sur tout support, y compris par télécopie, dès lors que son intégrité et l'imputabilité de son contenu à l'auteur désigné, ont été vérifiées ou ne sont pas contestées ». Ce qui compte, en définitive, ce n'est ni le formalisme, ni le support physique, ni le mode de communication des volontés, mais la certitude que l'écrit émane bien de celui auquel il pourrait être opposé, en d'autres termes, que ni son origine, ni son contenu n'ont été falsifiés (la Cour parle d'imputabilité et d'intégrité).

Même si la Cour ne semble traiter que du concept d'écrit, elle adopte résolument une interprétation fonctionnelle de ce concept. Mais elle ajoute que celle-ci ne vaut que si les fonctions « ont été vérifiées ou ne sont pas contestées ».

31. Deux enseignements peuvent être tirés de cet arrêt.

---

44 D. AMMAR, "Preuve et vraisemblance – contribution à l'étude de la preuve technologique", *R.T.D.civ*., 1993, p. 532 ; A. MYNARD, "Télématique et preuve en droit civil québecois et français : une antinomie?", *D.I.T.*, 1992, p. 21.

45 D. MOUGENOT, « Droit de la preuve et technologies nouvelles : synthèse et perspectives », *Droit de la preuve-Formation permanente CUP*, Volume XIX, octobre 1997, p. 98.

46 Voy. notamment les décisions citées par D. GOBERT, "La sécurisation des échanges par la reconnaissance de la signature électronique : condition d'existence des réseaux d'avocats", in *Multimédia: Le cyberavocat*, Formation permanente CUP, Volume XXIX, Liège-Namur, février 1999, p 173.

47 D. MOUGENOT, *op.cit.*, p. 99.

48 Cass. fr. (com.), 2 déc. 1997, *Dalloz*, 1998, p. 192.

Premièrement, la Cour se libère des exigences formelles et règle ainsi le problème de la *recevabilité* des documents non signés manuscritement (et *a fortiori* des documents électroniques). Elle affirme qu'un document écrit ne doit plus être déclaré irrecevable par le seul fait qu'il ne s'agit pas d'un écrit papier signé manuscritement, et cela même si l'acte juridique dépasse le montant fixé par la loi. De plus, elle déclare que la télécopie ne doit pas être traitée comme une copie fidèle et durable ou un commencement de preuve par écrit, mais tout simplement comme un écrit[49].

Deuxièmement, si la Cour se prononce en faveur de la *recevabilité* d'autres écrits que l'écrit traditionnel, elle est plus réservée quant à leur *valeur probante*. En effet, elle ne semble pas accorder d'office à cet écrit (la télécopie) la force probante qui est attribuée à l'acte sous seing privé. Elle ne le sera que si les fonctions (imputabilité et intégrité) ont été vérifiées ou ne sont pas contestées. Si l'acte n'est pas contesté (ce qui est le cas en l'espèce), il est aisé d'affirmer que les fonctions sont satisfaites. Par contre, si l'acte est contesté, le juge ne lui accordera la force probante d'un acte sous seing privé que si l'intégrité et l'imputabilité de celui-ci ont été vérifiées. Toutefois, comme le problème ne se posait pas, la Cour ne souffle mot du contenu concret de ces vérifications et de la manière dont elles doivent s'opérer. Elle se borne à considérer qu'il revient au juge du fond d'analyser les circonstances dans lesquelles a été émis l'écrit pour établir s'il peut être retenu comme établissant la preuve d'un acte. On ne se trouve guère dans une position plus enviable que celle que l'on a connu jusqu'à présent, puisqu'une nouvelle fois les parties devront tenter de convaincre le juge que l'imputabilité et l'intégrité de l'acte sont garanties avec une certaine fiabilité, en rencontrant les mêmes difficultés que celles rencontrées lorsqu'elles devaient persuader le juge que les conditions pour pouvoir bénéficier des exceptions à l'exigence d'un écrit étaient remplies. Ainsi, « ces écrits seront nécessairement toujours *imparfaits*, parce que soumis à une appréciation souveraine du juge, cas par cas, de leur fiabilité et imputabilité, à la différence de ce qu'il en est pour les *écrits parfaits* du Code civil, même sous seings privés, qui s'imposent aux juges (sauf le cas de la *dénégation de signature*) »[50]. On ne fait donc que déplacer le problème, du moins en ce qui concerne la force probante attachée à ce type d'écrit.

Enfin, signalons que cet arrêt est contesté en ce qu'il se situe sur le terrain de la preuve commerciale, caractérisé par sa souplesse, et traite de la cession de créance, matière régie par une loi particulière et non par le Code civil[51]. Pour ces raisons, il semble hasardeux de généraliser l'interprétation défendue par cet arrêt. Pierre Leclercq en conclut que, malgré celui-ci, « là où la loi (c'est usuel en droit de la consommation) impose, pour des raisons de protection ou de fond, et pas seulement de preuve, que les engagements soient *sous seings privés*, les actes ne pourront être dématérialisés et les signatures devront avant longtemps encore être *classiques* »[52].

3. Une définition fonctionnelle de la signature: une condition nécessaire mais non suffisante

---

49 Cela permet d'éviter de devoir exploiter le régime des exceptions (copie fidèle et durable, commencement de preuve par écrit), dont l'application à des documents électroniques est incertaine.

50 P. LECLERCQ, note sous Cass. fr. (com.), 2 déc. 1997, *D.I.T.*, 1998/1, pp. 56-60.

51 T. BONNEAU, note sous Cass. fr. (com.), 2 déc. 1997, *J.C.P.*, E, 1998, n°5, pp. 178-181.

52 P. LECLERCQ, note précitée.

32. Une intervention législative privilégiant l'approche fonctionnelle semble donc un passage obligé. Elle est soutenue par de nombreux auteurs[53] et est encouragée[54], voire entamée, dans certains Etats[55].

Cette intervention législative ne doit toutefois pas se limiter à introduire une définition fonctionnelle de la signature. Si tel était le cas, elle manquerait son principal objectif, à savoir mettre fin à l'insécurité juridique qui résulte de l'application et de l'interprétation des règles existantes.

L'adoption d'une approche fonctionnelle est donc une condition nécessaire, mais pas suffisante. D'un côté, elle est nécessaire car elle permet d'étendre les concepts d'écrit et de signature et ainsi d'assurer leur *recevabilité* à titre de preuve, même lorsque la loi exige un écrit au-delà d'un certain montant. En d'autres mots, le législateur indiquerait au juge qu'il ne peut plus contester un document signé au seul motif qu'il n'est pas assorti d'une signature manuscrite. D'un autre côté, elle est insuffisante car, ce faisant, le législateur ne se prononce pas sur la *force probante* des écrits dont la signature n'est pas manuscrite. Il se limite à préciser qu'il leur sera reconnu une force probante comparable à l'acte sous seing privé à la condition que les fonctions de la signature soient satisfaites avec une certitude raisonnable et donc que le document signé se situe dans un contexte dont la fiabilité est prouvée.

Or, on sait qu'une telle preuve est difficile et de toute façon soumise à l'appréciation souveraine du juge qui tranchera en fonction du cas d'espèce, mais aussi de l'appréhension qu'il a ou non vis-à-vis des nouvelles technologies.

Partant de ce constat, il apparaît souhaitable qu'outre l'adoption d'une définition fonctionnelle, le législateur mette en place un régime de présomption réfragable. Ainsi, il considérerait que, pour certains mécanismes de signature électronique, les fonctions de la signature sont présumées être remplies de manière fiable. Un écrit signé dans ces conditions s'imposerait au juge de la même manière qu'un écrit traditionnel. Pour le reste, le signataire resterait libre de contester sa signature (comme il peut le faire pour la signature manuscrite) puisque la présomption est réfragable.

Nous pouvons donc dire que, sur le plan de la recevabilité, l'approche fonctionnelle du législateur doit être *neutre* afin que le juge puisse recevoir et apprécier tout mécanisme de signature. Par contre, s'il se prononce sur le plan de la force probante, l'approche législative doit nécessairement être *technologique* car, par là même, on affirme la fiabilité d'une technologie particulière afin de dispenser le juge de cette appréciation.

---

53 M. ANTOINE et D. GOBERT, *op. cit.*, pp. 308-310; G. MAINCON-VITRAC, "EDI et régime de la preuve", *Expertises*, 1996, pp. 146 et s.; E. MONTERO, *op. cit*., pp. 62-64 ; D. MOUGENOT, *op. cit.*, pp. 98-99.

54 Voy. le rapport du Conseil d'Etat français de juillet 1998 : http://www.internet.gouv.fr/francais/textesref/rapce98/accueil.htm, pp. 74-92.

55 Par exemple, en Allemagne (Loi allemande sur le multimédia du 13 juin 1997, article 3 (sur la signature digitale), Journal officiel allemand du 22 juillet 1997 (BGBl, IS, 1870), entrée en vigueur le 1er août 1997, http://www.iid.de/iukdg/iukdge.html), en Italie (Décret présidentiel italien du 10 novembre 1997, n° 513 on "Regulations establishing criteria and means for implementing Section 15 (2) of Law N° 59 of 15 March 1997 concerning the creation, storage and transmission of documents by means of computer-based or telematic systems", publiée in *Gazzetta Ufficiale*, 13 mars 1998, n° 60, http://www.aipa.it/english/law[2/pdecree51397.asp), en Belgique (Projet de loi belge visant à "modifier certaines dispositions du Code civil relatives à la preuve des obligations", *Doc. parl.*, Ch. Repr., sess. ord. 14 avril 1999, n° 2141/1) ou au Luxembourg (http://www.droit.fundp.ac.be/crid/eclip/default.htm.).

B. Tour d'horizon en droit comparé

33. Après avoir présenté les atouts de l'approche fonctionnelle du concept de signature, il semble utile d'analyser concrètement la manière dont ce dernier a été saisi par certaines législations nationales ou internationales. Les approches sont diverses. Certaines adoptent une vision résolument large de la notion de signature, sans faire référence à la forme manuscrite ou électronique de celle-ci. D'autres privilégient une technologie particulière de signature électronique (signature numérique, signature biométrique, *etc*.). Enfin, une définition large et neutre de la signature électronique est parfois proposée, tout en conservant la dichotomie entre la signature manuscrite et la signature électronique.

1. Vers une définition ouverte de la signature?

a) Le Code civil du Québec

34. Dans le domaine de la preuve électronique, le Québec fait figure de proue. En effet, le Code civil du Québec (ci-après C.c.Q.) contient non seulement des dispositions générales sur la preuve électronique[56], mais surtout une définition de la signature qui élargit cette notion au-delà de la simple transcription du nom. Celle-ci se traduit désormais par la transcription d'une marque personnelle utilisée de façon courante par une personne pour manifester son consentement :

> ***Article 2827 C.c.Q.*** *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.*

On constate que les fonctions classiques de la signature, à savoir l'identification et la manifestation de la volonté du signataire, sont consacrées par cette définition.

La fonction de manifestation du consentement est clairement exprimée et ne nécessite aucun commentaire.

La fonction d'identification résulte des notions de « marque personnelle utilisée de façon courante ». En effet, selon certains auteurs, « la recherche de l'intention manifeste du législateur nous porte à croire que l'expression *'une marque personnelle qu'elle utilise de façon courante'* suppose, en clair, que cette marque soit susceptible de permettre l'identification d'une personne. Ainsi, on doit sans doute considérer comme répondant aux

---

[56] **Art. 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.

Art. 2838. L'inscription des données d'un acte juridique sur support informatique est présumée présenter des garanties suffisamment sérieuses pour qu'on puisse s'y fier lorsqu'elle est effectuée de façon systématique et sans lacunes, et que les données inscrites sont protégées contre les altérations. Une telle présomption existe en faveur des tiers du seul fait que l'inscription a été effectuée par une entreprise.

Art. 2839. Le document reproduisant les données d'un acte juridique inscrites sur support informatique peut être contredit par tous moyens.

critères de l'article 2827, une marque qui permet d'identifier une personne avec une raisonnable certitude »[57].

35. La fonction qui consiste à attribuer à un document le statut d'original n'est pas reprise dans la définition mais coule de source. Serge Parisien et Pierre Trudel affirment que « l'article 2827 fait de la signature des parties la seule exigence formelle relative à l'ensemble des actes sous seing privé. Celui-ci y est d'ailleurs défini comme étant celui qui porte la signature des parties »[58]. Un document aura donc le statut d'acte sous seing privé, d'original, et bénéficiera ainsi du régime probatoire favorable qui y est lié, parce qu'il est signé.

36. Par contre, la fonction d'intégrité ne semble pas avoir été entrevue. Cela étonne dans la mesure où, par cette formulation large, le C.c.Q. permet l'utilisation de signatures dites électroniques[59]. Or, dans l'environnement électronique, la fonction d'intégrité repose généralement sur le mécanisme technique utilisé. On pourrait argumenter que celle-ci est sous-entendue. En effet, on n'imagine pas qu'on puisse adhérer à un acte qui pourrait aisément être modifié par la suite sans que l'on s'en aperçoive[60].

37. Le Code civil du Québec a le mérite d'avoir lancé le mouvement de l'approche fonctionnelle et sert incontestablement d'exemple. Un document signé électroniquement sera désormais *recevable* en justice dans l'hypothèse où un écrit signé manuscritement est exigé. Mais pour bénéficier de la *valeur probante* accordée à l'acte sous seing privé, il faudra, au cas par cas, faire la preuve que le mécanisme utilisé constitue une marque personnelle qui permet d'identifier le signataire avec une certitude raisonnable et manifester son consentement, la preuve incombant à celui qui invoque l'acte signé. Même si, pour ce faire, l'on aura recours à un expert en informatique capable de témoigner de la fiabilité du mécanisme de signature et de l'authenticité de la signature litigieuse, il n'empêche néanmoins que subsiste une certaine insécurité juridique. En effet, cette définition fonctionnelle ne permet pas à l'utilisateur de déterminer, préalablement au litige, voire à la conclusion de la transaction, quel mécanisme, parmi les différentes techniques de signature électronique, satisfera aux conditions de l'article 2827 et passera avec succès l'épreuve de l'appréciation du juge.

b) La loi modèle de la CNUDCI

38. La CNUDCI a adopté en 1996 une loi type sur le commerce électronique et un guide pour son incorporation[61].

Elle part du constat que le recours à des moyens modernes de communication, tels que le courrier électronique et l'échange de données informatisées, pour la conduite des opérations commerciales internationales se répand rapidement et devrait continuer de se développer à

---

57 P. TRUDEL, G. LEFEBVRE et S. PARISIEN, *La preuve et la signature dans l'échange de documents informatisés au Québec*, Québec, Publications du Québec, 1993, p. 65, note 213.

58 S. PARISIEN et P. TRUDEL, *op. cit.*, p. 26. Voir aussi D. MOUGENOT, "Le code judiciaire à l'épreuve du cyberespace : la nécessaire réforme", in *Multimédia. Le cyberavocat*, Formation permanente CUP, Volume XXIX, Liège-Namur, février 1999, p. 402 et références citées à la note 10.

59 S. PARISIEN et P. TRUDEL, *op. cit.*, p. 33. On ne voit d'ailleurs pas pourquoi le législateur québecois se serait doté d'une définition de la notion de signature si ce n'est pour élargir celle-ci au-delà de sa forme traditionnelle.

60 D. GOBERT, *op. cit.*, p. 177.

61 Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation, 1996, Nations Unies, New York, 1997 disponible à l'adresse suivante : http://www.un.or.at/uncitral/fr-index.htm

mesure que s'élargit l'accès aux supports techniques tels les autoroutes de l'information et l'Internet. Toutefois, la communication d'informations ayant une valeur juridique, sous forme de messages sans support papier, peut être entravée par des obstacles juridiques à l'utilisation de tels messages ou par l'incertitude quant à leur effet ou leur validité juridique. La loi type a pour objectif d'offrir aux législateurs nationaux un ensemble de règles internationalement acceptables sur la manière de surmonter un certain nombre de ces obstacles et de créer un environnement juridique plus sûr pour ce que l'on appelle aujourd'hui le "commerce électronique". Les principes énoncés dans la loi type se veulent également utiles pour les particuliers qui pratiquent le commerce électronique pour la formulation de certaines des solutions contractuelles pouvant être nécessaires pour surmonter les obstacles juridiques au développement de ce type de commerce.

Dans ce document, la CNUDCI adopte une approche ouverte et fonctionnelle des concepts de signature et d'original.

La loi type ne donne pas comme telle une définition de la signature mais elle lui consacre un article dans le chapitre II. intitulé « Application des exigences légales aux messages de données ». L'article 7 sur la signature stipule que :

> *1. Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données :*
>
> *a) Si une méthode est utilisée pour identifier la personne en question et pour indiquer qu'elle approuve l'information contenue dans le message de données; et*
>
> *b) Si la fiabilité de cette méthode est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris de tout accord en la matière.*
>
> *2. Le paragraphe 1 s'applique que l'exigence qui y est visée ait la forme d'une obligation ou que la loi prévoie simplement certaines conséquences s'il n'y a pas de signature.*
>
> *3. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes : [...].*

Cet article 7 doit être lu conjointement avec l'article 9 qui traite de l'admissibilité et de la force probante des messages de données :

> *1. Aucune règle d'administration de la preuve ne peut être invoquée dans une procédure légale contre l'admissibilité d'un message de données produit comme preuve :*
>
> *a) Au motif qu'il s'agit d'un message de données; ou*
>
> *b) S'il s'agit de la meilleure preuve que celui qui la présente peut raisonnablement escompter obtenir, au motif que le message n'est pas sous sa forme originale.*
>
> *2. L'information prenant la forme d'un message de données se voit dûment accorder force probante. Cette force probante s'apprécie eu égard à la fiabilité du mode de création, de conservation ou de communication du message, la fiabilité du mode de préservation de l'intégrité de l'information, à la manière dont l'expéditeur a été identifié et à toute autre considération pertinente.*

L'article 7 se fonde sur la reconnaissance des fonctions remplies par la signature dans les échanges sur papier. Afin de garantir qu'un message ne puisse se voir refuser valeur juridique du simple fait qu'il n'a pas été authentifié de la manière voulue pour les documents sur papier, une formule générale a été retenue par cet article. Celui-ci s'attache aux deux fonctions traditionnelles de la signature, à savoir l'identification de l'auteur d'un document et la confirmation que ce dernier approuve la teneur dudit document. Le paragraphe 1, a) énonce que l'exigence d'une signature requise par la loi est satisfaite dès lors qu'une « méthode » permet de remplir ces deux fonctions. Le paragraphe 1, b) précise que cette méthode doit présenter un degré de fiabilité suffisant. Cette condition est toutefois très relative, et sera soumise à l'appréciation souveraine du juge, car elle dépendra « de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris tout accord entre l'expéditeur et le destinataire du message de données ». Nonobstant ce dernier élément, l'article 7 n'établit pas de distinction entre les situations dans lesquelles les parties à des transactions de commerce électronique sont liées par un accord antérieur et celles dans lesquelles les parties n'avaient aucune relation contractuelle préalable. En l'absence de convention, il présente donc un intérêt non négligeable.

L'article 9 a pour objet d'établir l'admissibilité des messages de données en tant que moyen de preuve dans les procédures juridiques ainsi que leur valeur probante, et cela indépendamment de la présence ou non d'une signature. S'agissant de l'admissibilité, le paragraphe 1, a)[62] prévoit que les messages de données ne devraient pas être rejetés en tant que moyens de preuve au seul motif qu'ils empruntent la forme électronique. Tout document électronique doit donc être déclaré recevable par le juge. S'agissant de l'évaluation de la force probante d'un message de données, le paragraphe 2 contient des indications utiles sur la façon d'apprécier celle-ci. Mais une nouvelle fois, la force probante dépendra de la fiabilité du système utilisé, souverainement appréciée par le juge.

39. La loi type contient aussi un article 8 relatif à la notion d'original :

> *1. Lorsque la loi exige qu'une information soit présentée ou conservée sous sa forme originale, un message de données satisfait à cette exigence :*
>
> *a) S'il existe une garantie fiable quant à l'intégrité de l'information à compter du moment où elle a été créée pour la première fois sous sa forme définitive en tant que message de données ou autre; et*
>
> *b) Si, lorsqu'il est exigé qu'une information soit présentée, cette information peut être montrée à la personne à laquelle elle doit être présentée.*
>
> *2. Le paragraphe 1 s'applique que l'exigence qui y est visée ait la forme d'une obligation ou que la loi prévoie simplement certaines conséquences si l'information n'est pas présentée ou conservée sous sa forme originale.*
>
> *3. Aux fins de l'alinéa a du paragraphe 1 :*
>
> *a) L'intégrité de l'information s'apprécie en déterminant si celle-ci est restée complète et n'a pas été altérée, exception faite de l'ajout de tout endossement et de toute modification intervenant dans le cours normal de la communication, de la conservation et de l'exposition; et*

---

[62] Nous ne traiterons pas du paragraphe 1, b) qui vise la notion de la "meilleure preuve", propre aux systèmes juridiques de la *Common Law*.

> *b) Le niveau de fiabilité requis s'apprécie au regard de l'objet pour lequel l'information a été créée et à la lumière de toutes les circonstances y relatives.*
>
> *4. Les dispositions du présent article ne s'appliquent pas dans les situations suivantes : [...].*

Contrairement à ce qu'enseigne la doctrine belge traditionnelle (*supra*, n° 24, et les réf.), la loi type semble faire dépendre le caractère original d'un acte, non pas de sa signature, mais de l'existence de garanties fiables quant au maintien de l'intégrité du contenu de cet acte. L'objectif poursuivi par la loi type est louable puisqu'il s'agit d'affirmer qu'un document ne doit pas perdre automatiquement le statut d'original parce qu'il ne se trouve plus sur son premier support. On peut toutefois se demander si le caractère original d'un acte résulte réellement du maintien de l'intégrité ou de sa signature. Un acte signé manuscritement perd-il automatiquement le statut d'original parce qu'une partie ou un tiers modifie *ex post* le contenu de ce document ? Un document est-il original par le seul fait que son intégrité est préservée ? Il nous semble que non. Si on admet que l'une des fonctions de la signature électronique consiste à garantir l'intégrité du contenu du document, il en résulte que le document signé ne sera pas altéré et que l'on pourra lui reconnaître un caractère original. Mais l'inverse n'est pas vrai. Un document dont l'intégrité est garantie n'est pas nécessairement signé. En effet, d'un point de vue technique, les différentes fonctions de la signature ne sont pas toujours réalisées par un mécanisme informatique unique mais peuvent résulter de la combinaison de plusieurs techniques (par exemple, *supra*, n° 22). Dès lors, on peut imaginer un document dont l'intégrité est préservée[63], mais dont il est impossible de déterminer l'auteur[64]. Peut-on encore parler dans ce cas de document original ? A l'évidence, non. Nous pouvons donc affirmer que le caractère original de l'acte résulte de la signature de celui-ci par son auteur, et non exclusivement du maintien de son intégrité, étant entendu par là que l'intégrité de cet acte sera nécessairement garantie, puisque l'approche fonctionnelle nous apprend que l'une des fonctions de la signature est le maintien de l'intégrité[65].

40. Même si la légistique du texte laisse à désirer et que de nombreuses zones d'ombre subsistent, retenons globalement que la loi type a le mérite de plaider pour l'adoption d'une approche fonctionnelle, condition indispensable (mais toutefois insuffisante) au développement des transactions électroniques, et d'inciter les Etats à réfléchir à la question. Ces différents textes adoptés par la CNUDCI ne sont pas contraignants. Il ne s'agit pas de conventions internationales destinées à être ratifiées par les Etats. Il s'agit simplement d'une bonne source d'inspiration mise à la disposition des législateurs nationaux. Ces textes méritent néanmoins une attention particulière dans la mesure où ils constituent un ensemble de règles internationalement acceptables, qui permettent une certaine harmonisation et qui exercent une influence évidente sur les autorités européennes.

---

63 Un document archivé sur un CD ROM (*Read Only Memory*) par exemple ne peut être modifié, étant donné que le code binaire est gravé sur le support. Toute tentative de modification risquerait d'endommager le document de manière irréversible et de le rendre illisible. Par ailleurs, le logiciel de traitement de texte *Word* par exemple permet de protéger, à l'aide d'un mot de passe, un document contre toute modification.

64 C'est le cas si aucune technique d'identification n'a été utilisée.

65 Les autres fonctions (identification et consentement) seront également remplies puisque l'acte original est signé. Peu importe donc que les différentes fonctions soient réalisées par un seul mécanisme informatique ou par la combinaison de plusieurs mécanismes (dont seulement certains sont qualifiés de signature au sens technique, et non juridique, du terme, ce qui entretient d'ailleurs une confusion malsaine). Ce qui compte réellement, c'est qu'elles soient toutes remplies pour qu'on puisse considérer qu'il s'agisse d'un document signé et qu'on le traite comme tel (notamment sur le plan du droit de la preuve).

2. Vers une solution technologique?

a) La loi de l'Utah

41. L'adoption et l'entrée en vigueur du *Utah Digital Signature Act*[66] (ci-après loi de l'Utah), respectivement les 27 février et 1er mai 1995, font de l'Utah le premier Etat américain à s'être doté d'une loi consacrée à la signature électronique. Ce texte reconnaît de manière expresse la recevabilité de cette dernière. En effet, la loi de l'Utah prévoit qu'un document signé de façon électronique est tout aussi valide qu'un document réalisé à l'aide d'un support papier[67].

Il importe de noter le caractère limitatif de l'expression « signé électroniquement ». La loi de l'Utah a manifestement fait un choix technologique puisqu'aux termes de celle-ci, la signature numérique, basée sur la cryptographie asymétrique, représente le seul mécanisme de signature qui permette de signer électroniquement un document. La notion de signature électronique y est d'ailleurs définie par une référence précise au fonctionnement technique de ce mécanisme :

> *Article 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 accuretly 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.*

Cette définition ne laisse évidemment aucune place à l'interprétation. Elle privilégie la cryptographie asymétrique comme mécanisme unique de signature électronique, à l'exclusion de tout autre mécanisme basé notamment sur la biométrie ou sur l'utilisation de codes secrets. Il est évident que la cryptographie, à elle seule, n'est pas suffisante pour assurer les fonctions de la signature, et notamment celle d'identification. Celle-ci doit être combinée à l'intervention d'une autorité de certification dont le rôle premier consiste à émettre des certificats. A cet effet, la loi de l'Utah prévoit un volet relatif à l'intervention de semblable organisme[68].

Selon cette loi, d'importantes présomptions découlent de l'utilisation de certificats. Ainsi toute signature numérique, vérifiée avec succès par l'utilisation d'une clé publique inscrite dans un certificat, est présumée avoir été apposée par le signataire et est reconnue comme telle[69]. Par ailleurs, une signature numérique réalisée à l'aide d'une clé privée est présumée avoir été apposée par le signataire avec l'intention d'authentifier le message et exprime sa volonté d'adhérer au contenu du message[70].

42. On le voit, trois fonctions de la signature se retrouvent clairement dans le texte de la loi de l'Utah. La fonction d'intégrité est directement consacrée dans la définition de la signature digitale. Les fonctions d'identification et de manifestation de la volonté sont envisagées par le biais des présomptions. On ne peut toutefois pas parler véritablement d'une approche

---

66 Ce texte a été publié intégralement dans l'*EDI Law Review*, 1995, 2, pp. 157-196.

67 Loi de l'Utah, article 403.

68 Loi de l'Utah, article 401 et s.

69 Loi de l'Utah, article 405.

70 Loi de l'Utah, article 406, b).

fonctionnelle puisque le seul mécanisme visé par cette loi est celui de la signature numérique. Il en résulte que d'autres mécanismes de signature électronique ne pourront bénéficier, même s'ils remplissent ces trois fonctions, des présomptions de cette loi et de l'équivalence juridique à la signature manuscrite. Toutefois, et même si la loi de l'Utah ne se prononce pas expressément (ce qui est regrettable) sur la recevabilité de l'ensemble des signatures électroniques, on devrait pouvoir considérer que tel est quand même le cas. Pour le reste, le juge resterait libre d'en apprécier la valeur probante, à défaut de bénéficier des présomptions de la loi. Cette dernière remarque devrait donc, nous semble-t-il, tempérer les critiques qui ont été faites quant à son caractère technologique[71]. Il apparaît raisonnable qu'on ne reconnaisse pas automatiquement force probante à tous les mécanismes de signature électronique s'il existe un doute sur leur fiabilité ou si leur utilisation n'est pas faite dans un contexte sécurisé, tel que celui retenu par cette loi.

b) Les lois allemande et italienne

43. L'Allemagne et l'Italie sont les deux premiers pays de l'Union européenne à s'être dotés d'une législation relative à la signature électronique. Après analyse de ces textes, on constate que l'approche de ces deux pays est technologique puisque ceux-ci ne traitent que du mécanisme de signature numérique (fondé sur la cryptographie asymétrique), et plus exactement du régime juridique des autorités de certification qui interviennent dans l'utilisation de ce mécanisme de signature.

La loi allemande[72] du 13 juin 1997 est particulièrement technique. Elle définit la signature dans son article 3, §2, (1) comme suit : *« digital signature shall mean a seal affixed to digital data which is generated by a private signature key and establishes the owner of the signature key and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority or the authority according to §3 of this Act »*. Il ne fait nul doute que cette définition ne vise que le mécanisme de signature digitale, fondée sur la cryptographie asymétrique, dite à clé publique. Les dispositions de cette loi visent essentiellement à déterminer le régime juridique des autorités de certification. D'autre part, une ordonnance[73] complète cette loi en fixant la procédure d'accréditation ainsi que les composantes techniques afin que la signature digitale soit utilisée et que les autorités de certification opèrent dans un contexte de fiabilité et de sécurité acceptable.

La loi allemande a donc fait un choix technologique, ce qui en soi n'est pas totalement critiquable car il faut bien reconnaître que ce mécanisme offre un niveau de sécurité élevé tout en ayant un coût limité. Il est par contre plus étonnant que la loi ne traite pas de la valeur juridique, notamment en droit de la preuve, à accorder à un document signé digitalement dans les conditions de cette loi[74]. On peut probablement en conclure que les règles classiques du droit de la preuve du Code civil allemand continuent à s'appliquer. Tout au plus, le juge allemand est-il assuré désormais que certains mécanismes de signature électronique peuvent

---

71 E. DAVIO, "Questions de certification, signature et cryptographie", *op. cit.*, p. 84.

72 Loi allemande sur le multimédia du 13 juin 1997, article 3 (sur la signature digitale), Journal officiel allemand du 22 juillet 1997 (BGBl, IS, 1870), entrée en vigueur le 1er août 1997, http://www.iid.de/iukdg/iukdge.html

73 Disponible à l'URL suivant : http://www.iid.de/iukdg/sigve.html

74 Notons toutefois que les fonctions d'identification et d'intégrité ressortent de la définition de la signature digitale.

identifier de manière fiable l'émetteur d'un document électronique et garantir son intégrité, ce qui devrait l'inciter à accorder plus facilement une valeur probante à ce type de document.

44. En Italie, une loi du 15 mars 1997[75] stipule en termes généraux dans son article 15 que *« la création d'actes ou de documents informatiques ainsi que leur transmission et leur conservation par voie télématique sont légalement valides »*. Cette loi a été précisée par un décret présidentiel du 10 novembre 1997[76]. A l'instar de la loi allemande, ce décret est technique et fait un choix technologique. Il suffit pour s'en convaincre de citer la définition de la signature qui est donnée dans la section 1 : *« Digital signature means the result of a computer-based process (validation) implementing an asymmetric cryptographic system consisting of a public and a private key, whereby the signer asserts, by means of the private key, and the recipient verifies, by means of the public key, the origin and integrity of a single electronic document or a set of such documents »*. Par contre et contrairement à la loi allemande, la loi italienne s'est prononcée sur la valeur probante à accorder à un document signé digitalement. En effet, la section 5 de cette loi stipule qu'un document électronique signé avec une signature digitale conformément aux prescriptions du décret bénéficie de la même force probante que l'acte sous seing privé visé à l'article 2702 du Code civil italien. La section 4 prévoit le même type d'assimilation pour le concept d'écrit puisqu'il stipule que les documents informatiques qui respectent les prescriptions du décret doivent être considérés comme rencontrant les exigences légales en matière d'écrit. Dans ce contexte, on comprend que le législateur italien ait jugé superflu de donner une définition fonctionnelle abstraite de la signature. Cela signifie également que le régime privilégié accordé à la signature digitale ne bénéficie pas aux autres mécanismes de signature électronique actuels ou futurs.

3. Vers une définition de la signature électronique?

a) La directive européenne sur la signature électronique

45. Le 16 juin 1998, la Commission européenne a présenté une proposition de directive sur un cadre commun pour les signatures électroniques[77]. Suite aux quelques discussions animées, une nouvelle version a été présentée au Conseil des ministres européen du 22 avril 1999 et a fait l'objet d'une position commune[78]. Le texte étant soumis à la procédure de co-décision, il a été présenté au Parlement européen pour d'éventuels amendements, pour enfin être adopté le 13 décembre 1999[79].

---

75 Law N° 59 of 15 March 1997 "concerning the creation, storage and transmission of documents by means of computer-based or telematic systems", http://www.aipa.it/english/law[2/law5997.asp

76 Décret présidentiel italien du 10 novembre 1997, n° 513 on "Regulations establishing criteria and means for implementing Section 15 (2) of Law N° 59 of 15 March 1997 concerning the creation, storage and transmission of documents by means of computer-based or telematic systems", publié in *Gazzetta Ufficiale*, 13 mars 1998, n° 60, http://www.aipa.it/english/law[2/pdecree51397.asp

77 Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques, COM (98)297 final, 13 juin 1998, *J.O.C.E.*, C 325/5-11 du 23 octobre 1998 ou http://www.ispo.cec.be/eif/policy/com98297fr.doc. Pour un commentaire approfondi de la première version de cette proposition de directive, voy. R. JULIA-BARCELO et T.C. VINJE, "Electronic signatures - another step towards a European framework for electronic signatures : the Commission's Directive proposal", *Computer Law & Security Report*, octobre 1998, n° 14/5, pp. 303-313.

78 Voy. l'URL suivant : http://europa.eu.int/comm/dg15/fr/media/sign/index.htm

79 Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *J.O.C.E.*, L 13/12 à 20 du 19 janvier 2000.

Cette directive résulte du constat que les initiatives législatives se multiplient dans plusieurs Etats membres et qu'il devient urgent de disposer d'un cadre juridique harmonisé au niveau européen afin d'éviter que le fonctionnement du marché intérieur ne soit gravement entravé. A cette fin, elle établit les conditions cadres pour l'utilisation des signatures électroniques ainsi que leur reconnaissance juridique.

46. La directive nous donne une double définition de la signature électronique. D'une part, elle définit de manière très générale le terme *signature électronique* comme *« une donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification »* (article 2, 1.). D'autre part, elle propose une définition d'une catégorie particulière de signature électronique qu'elle qualifie de *signature électronique avancée* (article 2, 1*bis*) :

> *On entend par signature électronique avancée, une signature électronique qui satisfait aux exigences suivantes :*
> *a) être liée uniquement au signataire ;*
> *b) permettre d'identifier le signataire ;*
> *c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ; et*
> *d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.*

L'objet de cette distinction n'est pas claire. Elle a manifestement été inspirée par les travaux de la CNUDCI[80]. La directive a probablement voulu attirer l'attention sur le fait qu'il existe une multitude de techniques baptisées « signature électronique », dès lors qu'elles permettent, à elles seules ou en combinaison, de réaliser les fonctions dévolues à la signature. Cependant, toutes ne présentent pas nécessairement un niveau de sécurité acceptable sur le plan juridique. Le point 1 des définitions vise certainement à englober ces différents mécanismes, sans toutefois leur reconnaître une valeur juridique comparable à celle de l'écrit papier signé manuscritement (voir ci-après). On suppose que c'est à dessein que la définition parle de « donnée servant de méthode d'authentification », l'authentification pouvant porter tant sur l'origine des données que sur leur intégrité, voire sur d'autres éléments. Par cette définition, la directive a voulu affirmer sa neutralité technologique en ne privilégiant aucun mécanisme particulier de signature électronique.

Cette neutralité technologique est toutefois tempérée par le point 1*bis* dans lequel on considère que certaines signatures électroniques peuvent être avancées, et donc sécurisées, pour autant qu'elles satisfassent aux exigences de cet article. Ces exigences présentées de manière technique consacrent en réalité les fonctions d'identification (point b[81]) et d'intégrité

---

80 Voir, par exemple, Commission des Nations Unies pour le Droit Commercial International, Rapport du groupe de travail sur le commerce électronique sur les travaux de sa trente troisième session (New York, 29 juin-10 juillet 1998), A/CN.9/454, 21août 1998. Voir aussi http://www.un.or.at/uncitral/fr-index.htm. Il faut savoir qu'au-delà de la loi type adoptée en 1996, le groupe de travail sur le commerce électronique de la CNUDCI travaille actuellement à l'élaboration d'un projet de règles uniformes sur les signatures électroniques et les autorités de certification. Dans celui-ci, elle définit les notions de signature électronique, signature numérique, certificat et autorité de certification. Elle détermine les effets juridiques de ces signatures. Elle fixe le contenu minimal du certificat et le régime de responsabilité des autorités de certification ainsi que des utilisateurs de certificats. Elle propose des règles en matière de reconnaissance mutuelle des certificats.

81 Les points a) et c) ne font que stipuler les conditions préalables à l'exigence d'identification du signataire : en effet, une donnée ne permettrait pas d'identifier le signataire, et d'éviter les risques de

(point d). La neutralité technologique de cette définition n'est qu'apparente dans la mesure où il ne fait pas de doute qu'actuellement, seule la technique de signature digitale, fondée sur la cryptographie asymétrique, répond à la définition de la signature électronique avancée. Le contenu des annexes ne laisse planer aucune incertitude à ce sujet.

L'intérêt de cette distinction se fait ressentir dans l'article 5 qui traite des effets juridiques de la signature électronique. Afin de reconnaître une valeur juridique à la signature électronique, cet article contient deux clauses : l'une d'assimilation et l'autre de non discrimination.

1. *Les Etats membres veillent à ce que les signatures électroniques avancées basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature*
   a) *répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier, et*
   b) *soient recevables comme preuve en justice.*

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

47. La clause d'assimilation consiste à assimiler la signature électronique à la signature manuscrite lorsque certaines conditions sont remplies[82], c'est-à-dire à considérer qu'elle doit être admissible comme preuve en justice et qu'elle doit bénéficier de la force probante accordée à la signature manuscrite.

D'un point de vue légistique, il est étonnant que l'article 5.1. commence par traiter de la force probante (point a) des signatures électroniques avancées pour ensuite envisager leur recevabilité (point b) puisque celle-ci est un préalable et une condition indispensable de leur reconnaissance juridique. De plus, notons que cette clause d'assimilation ne profite pas à l'ensemble des mécanismes de signature électronique, mais uniquement aux signatures électroniques avancées (pour autant que les autres conditions soient remplies).

48. La clause de non discrimination (article 5.2.) s'applique lorsque les conditions prévues à l'article 5.1. ne sont pas remplies pour bénéficier de la clause d'assimilation. Dans ce cas, les Etats membres doivent veiller à ce que l'effet ou la validité juridique d'une signature électronique ne soit pas contesté au seul motif que la signature se présente sous forme électronique, ou qu'elle ne repose pas sur un certificat qualifié, ou encore qu'elle ne repose pas sur un certificat délivré par un prestataire de service de certification accrédité au sens de la directive. Le principe énoncé dans cet article doit être entendu comme celui de la recevabilité des signatures électroniques *lato sensu*. Toutefois, à défaut de répondre aux spécifications de l'article 5.1., il appartient à celui qui s'en prévaut de convaincre le juge de sa valeur probante.

---

répudiation, si cette même donnée était liée à plusieurs signataires ou si elle était créée et gérée par plusieurs personnes.

82 La signature électronique doit être avancée au sens de l'article 2, 1*bis*, elle doit reposer sur un certificat qualifié tel que défini à l'article 2, 5, et enfin elle doit être créée par un dispositif sécurisé de création de signature tel que décrit à l'annexe 3 de la directive.

49. La formulation de l'article 5 appelle deux commentaires[83].

Puisque l'article 5.1. traite de la force probante des signatures électroniques avancées, il n'était pas nécessaire de traiter dans un second temps de leur recevabilité puisque celle-ci est une condition *sine qua non* de leur reconnaissance juridique. Il eut donc été plus clair de poser, dans un premier temps, le principe de la recevabilité de toute signature électronique et de traiter, dans un second temps, de la force probante des signatures électroniques avancées. De plus, cela aurait évité de devoir traiter du problème de la recevabilité dans la clause d'assimilation (art. 5, 1, b), comme évoqué plus haut.

Ensuite, on peut observer qu'en pratique, l'article 5.1. de la directive ne présente un intérêt que si les Etats membres, tout en respectant le principe de la liberté d'exercice de l'activité de certification, mettent sur pied un régime d'accréditation des prestataires de service de certification subordonnant l'octroi d'une accréditation au respect des conditions prévues à l'annexe 2, ce qui suppose la mise en place d'une procédure d'octroi de l'accréditation et un contrôle préalable (sous la forme d'un audit) du respect de ces conditions.

En dehors de toute initiative nationale en vue de l'accréditation des prestataires de service de certification, la personne qui se prévaut d'un document signé électroniquement serait tenue d'apporter la preuve que les conditions fixées par les trois annexes de la directive ont effectivement été remplies afin de bénéficier de la clause d'assimilation. Cette situation est difficilement acceptable, surtout si la charge de la preuve incombe au consommateur, étant donné la difficulté de rapporter une telle preuve.

On peut dès lors craindre que l'objectif visé par la directive, à savoir renforcer la sécurité juridique, soit manqué puisque, quand bien même le texte résoudrait la question de la recevabilité des documents signés électroniquement, le pouvoir discrétionnaire du juge quant à l'appréciation de leur valeur probante serait de nature à rendre l'issue du litige incertaine.

c) Le projet de loi luxembourgeois

50. En mars 1999, le Conseil des ministres luxembourgeois a adopté un projet de loi relatif au commerce électronique[84]. Ce projet contient notamment un titre II sur la preuve et la signature électronique. Dans ce dernier, l'article 5 introduit une définition de la signature dans le Code civil libellée comme suit :

> *La signature nécessaire à la perfection d'un acte sous seing privé identifie celui auquel il est opposé et manifeste son adhésion au contenu de l'acte.*
>
> *Elle peut être manuscrite ou électronique.*
>
> *La signature électronique consiste en un ensemble de données, liées de façon indissociable à l'acte, qui en garantit l'intégrité et satisfait aux conditions posées à l'alinéa premier du présent article.*

---

83 Cf. M. ANTOINE, D. GOBERT et A. SALAÜN, "Le développement du commerce électronique : les nouveaux métiers de la confiance", in *Droit des technologies de l'information. Regards prospectifs* (sous la direction de E. MONTERO), Cahiers du C.R.I.D., n° 16, Bruxelles, Bruylant, 1999, pp. 3-32.

84 Ce texte est disponible à l'adresse suivante : http://www.etat.lu/ECO/. Il est actuellement retravaillé pour être déposé à nouveau.

Le projet part du constat que l'admission de nouvelles formes de signature à côté de la signature manuscrite passe nécessairement par une définition de la signature. Toutefois, il ne convient de lier cette définition ni au mode d'expression de la signature, ni à son support. Celle-ci doit être caractérisée à travers ses deux fonctions essentielles : l'identification du signataire et son adhésion au contenu de l'acte.

L'absence de toute référence aux possibles formes que la signature peut revêtir permet d'ouvrir le concept aux procédés d'authentification les plus divers offerts par les nouvelles technologies (signatures digitales, biométriques…). Elle évite aussi l'imprécision, et partant l'insécurité, inhérente à toute définition matérielle de la signature.

Le deuxième alinéa de l'article lève toute hésitation sur la recevabilité de la signature électronique. En ce qui concerne cette dernière, le texte entend cependant répondre à un risque lié spécifiquement à sa dématérialisation, celui de voir l'acte auquel elle se rapporte modifié en dehors de tout consentement du signataire. Ainsi, la signature électronique n'est reconnue que si elle remplit la condition supplémentaire d'être liée de façon indissociable à l'acte et d'en garantir l'intégrité. Contrairement au Code civil du Québec, le texte maintient donc la dichotomie entre la signature manuscrite et la signature électronique, et fait de la fonction d'intégrité une fonction propre à la signature électronique.

51. Cet article 5 doit être lu en combinaison avec l'article 17 qui traite des effets juridiques de la signature électronique :

> ***§1.*** *Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique créée par un dispositif de création de signature que le signataire puisse garder sous son contrôle exclusif et qui repose sur un certificat qualifié, constitue une signature au sens de l'article 1322-1 du Code civil.*
>
> ***§2.*** *Une signature électronique ne peut être rejetée par le juge au seul motif qu'elle se présente sous forme électronique, qu'elle ne repose pas sur un certificat qualifié.*

Cet article s'inspire essentiellement de l'article 5 de la directive sur les signatures électroniques. Nous renvoyons donc le lecteur aux commentaires et critiques déjà formulés (*supra*, n° 47 à 49).

Le premier paragraphe constitue la clause d'assimilation au sens de la directive. Eu égard aux niveaux de sécurité et de fiabilité résultant du respect des conditions stipulées dans ce paragraphe, une telle signature doit être considérée comme équivalente à une signature manuscrite sans qu'un juge ne puisse remettre en cause sa valeur probante intrinsèque, ce qui, bien entendu, n'interdit pas à celui auquel elle est opposée de la contester de la même manière qu'une signature manuscrite. Ce raisonnement ne sera toutefois tenable que si l'on considère qu'un certificat qualifié est un certificat émis par une autorité de certification qui a été préalablement agréée dans le cadre d'une procédure d'accréditation, ce qui n'apparaît pas clairement dans le texte.

Le deuxième paragraphe consacre la clause de non discrimination. Si une signature électronique ne satisfait pas aux conditions prévues dans le §1, elle ne bénéficie pas de l'équivalence automatique à la signature manuscrite, mais elle ne peut être rejetée par le juge pour cette seule raison. Il appartiendra à la personne qui s'en prévaut d'apporter la preuve de la fiabilité de la technique utilisée afin d'établir que la signature répond aux critères posés par l'article 1322-1 du Code civil. A défaut, l'acte auquel elle est attachée pourrait toujours servir de commencement de preuve par écrit ou d'indice à l'appui d'une preuve par présomption. On

peut se demander si ce §2 de l'article 17 n'est pas redondant avec l'article 5 qui affirme déjà le principe de la recevabilité des signatures électroniques.

52. Pour mémoire, mentionnons que l'article 6 propose, à l'instar de la loi modèle de la CNUDCI, une nouvelle notion de l'original :

> *L'acte sous seing privé électronique vaut comme original lorsqu'il 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.*

Etant donné la similitude avec l'article 8 de la loi modèle de la CNUDCI, nous renvoyons aux commentaires que nous avons faits précédemment (*supra*, n° 39).

C. Evaluation critique des textes belges en projet

53. En Belgique, des initiatives ont été prises afin d'assurer une reconnaissance juridique de la signature électronique. En effet, le 12 juin 1998, le Conseil des ministres a adopté, en première lecture, deux avant-projets de loi allant dans ce sens. Le premier vise à modifier certaines dispositions du Code civil relatives à la preuve des obligations (ci-après « projet preuve »). Le second vise à mettre en place un régime juridique applicable aux activités des autorités de certification agréées (ci-après « projet autorités de certification »), et cela dans le cadre de l'utilisation de signatures digitales[85].

En sus de la demande d'avis de la section de législation du Conseil d'Etat, ces deux textes ont été discuté au sein d'Agora 98, forum de discussion officiel à propos de la société de l'information en Belgique, créé à l'initiative du ministre des Affaires économiques d'alors[86]. Ces discussions ont débouché sur un rapport de grande qualité et sur des recommandations remises au ministre.

Le projet autorités de certification a été adopté en seconde lecture par le Conseil des ministres du 26 mars 1999. Il n'a toutefois pas été déposé devant la Chambre avant sa dissolution. Par contre et de manière surprenante, le projet preuve n'a pas été soumis au Conseil des ministres pour seconde lecture, mais a été déposé au Parlement *in extremis*[87].

---

85 Il convient de noter que, suite au changement de gouvernement, le nouveau Ministre des affaires économiques a déposé en Conseil des Ministres du 14 octobre 1999 un texte remanié sur la signature électronique et les prestataires de service de certification, afin de l'adapter à la directive européenne. Celui-ci n'est toutefois pas encore publié. Pour ce qui est du projet preuve, le Ministre de la justice n'a manifestement pas encore proposé un nouveau texte à la date de la rédaction de cet article. Pour ces raisons, nous nous limiterons à commenter les anciens textes.

86 Plus exactement, ces textes ont été discutés dans l'atelier 1 de la branche « Consommateurs », relatif à la signature électronique et à la certification des sites, présidé par le Professeur Y. POULLET. Cet atelier regroupait des experts et personnes intéressées par le sujet issus du secteur tant privé que public, du barreau, du notariat, du monde universitaire, *etc*.

87 *Doc. parl.*, Ch. Repr., sess. ord. 14 avril 1999, n° 2141/1. Notons toutefois que le texte déposé au Parlement ne correspond pas à celui qui a été adopté le 12 juin 1998, et ne semble pas avoir été soumis à un Conseil des ministres depuis cette date. De plus, il n'a pas été relevé de caducité par la nouvelle majorité. Limitons-nous à mentionner la définition de la signature qui y est proposée : « Une signature au sens de cet article peut être un ensemble de données numériques pour autant qu'elle puisse être imputée à une personne déterminée et qu'elle établisse le maintien de l'intégrité de l'acte ». Pour le reste, nous commenterons principalement le texte adopté le 12 juin 1998, qui se trouve également dans le projet déposé au Parlement.

1. Le projet preuve : l'approche neutre

54. Le projet preuve part du constat que la jurisprudence reste très conservatrice quant à l'interprétation des règles de preuve et qu'il est nécessaire d'intervenir afin de faire évoluer celles-ci. Il poursuit principalement l'objectif de modifier les règles de preuve du Code civil afin qu'un document signé électroniquement puisse, moyennant le respect de certaines conditions, faire preuve au même titre qu'un écrit papier signé manuscritement.

En son article 3, le projet prévoit d'introduire une définition fonctionnelle de la signature à l'article 1322 du Code civil, libellée comme suit :

> *Est assimilé à une signature manuscrite l'ensemble de données issues de la transformation de l'écrit et dont ressort avec certitude l'identité de l'auteur et son adhésion au contenu de l'écrit.*

55. Cette définition suscite plusieurs commentaires.

D'emblée, on perçoit que la définition reprend les deux fonctions traditionnellement assignées à la signature classique. Elle doit identifier l'auteur de l'acte et permettre à ce dernier de manifester son consentement sur le contenu de celui-ci. La fonction d'intégrité n'est pas reprise expressément dans la définition[88]. Cependant, on doit la considérer comme sous-entendue : on n'imagine pas que l'on puisse adhérer à un acte susceptible d'être modifié par la suite sans que l'on s'en aperçoive. Ajoutons que la définition exige que ces fonctions ressortent avec *certitude* du mécanisme utilisé. Cela semble excessif, voire impossible à réaliser pratiquement[89]. Exiger une *certitude raisonnable* aurait été largement suffisant.

Par ailleurs, la définition conserve une distinction entre la signature manuscrite et d'autres formes de signature[90]. L'intérêt appréciable de cette distinction est probablement d'affirmer que peuvent désormais exister et être admises d'autres formes de signature que la signature manuscrite, sans toutefois balayer l'interprétation jurisprudentielle et doctrinale qui a été faite de cette dernière.

Ensuite, même si elle conserve une distinction entre la signature manuscrite et la signature électronique, la définition reste neutre sur le plan technologique. En effet, les mots « ensembles de données issues de la transformation de l'écrit » sont tellement larges qu'ils ne se limitent pas aux procédés techniques de signature digitale qui existent actuellement. La neutralité technologique découle également de l'approche fonctionnelle qui est faite de la signature[91].

Enfin, une signature électronique suppose une transformation de l'écrit[92]. En effet, il est nécessaire que l'ensemble de données soit le résultat d'une transformation, quelle qu'elle soit,

---

88 Elle se retrouve par contre dans la nouvelle définition inclue dans le projet 2141/1 déposé à La Chambre lors de la précédente législature. Rappelons également que l'avant-projet de loi luxembourgeois reprend expressément cette troisième fonction dans la définition de la signature électronique.

89 Aucun informaticien ne peut certifier qu'un mécanisme est fiable à 100 %, tout comme l'authenticité d'une signature manuscrite ne peut être prouvée à 100 %.

90 Cette distinction apparaît moins dans le nouveau projet.

91 Une réflexion comparable peut être faite pour le nouveau texte.

92 Cet élément n'apparaît malheureusement plus dans la nouvelle définition.

de l'écrit, de sorte que s'établisse un lien indissociable entre l'écrit et la signature, sans quoi on ne peut être sûr que c'est cet écrit qui émane du prétendu signataire.

Avec une telle définition, il ne fait nul doute que tout type de signature doit désormais être déclaré recevable par le juge. Il n'est donc plus possible de contester un document signé électroniquement au seul motif que la signature n'est pas manuscrite. Le juge doit en outre prendre le temps de vérifier si les fonctions sont remplies pas le mécanisme qui lui est présenté et de se prononcer sur la valeur probante qu'il accorde à ce dernier. Il appartiendra dans ce cas à celui qui se prévaut de l'acte signé de faire cette preuve. Etant donné la difficulté de celle-ci, il semble néanmoins que le juge devrait dispenser la partie de cette preuve lorsque l'acte signé n'est pas contesté par le signataire (même si la signature est sommaire ou réalisée à l'aide d'un mécanisme très peu sécurisé). L'absence de contestation pourrait être interprétée comme une ratification par le signataire du contenu de l'acte et comme une approbation qu'il émane effectivement de lui.

2. Le projet sur les autorités de certification : l'approche technologique

56. Le projet « autorités de certification » est technique et orienté du point de vue de la technologie[93]. En effet, il se limite au mécanisme de la signature digitale. La définition donnée à l'article 2, 1°, ainsi que l'exposé des motifs, ne font planer aucun doute à ce sujet :

> ***Article 2, 1°.*** *Signature digitale : le résultat de la transformation d'un ensemble de données numériques à l'aide d'une clé privée, de telle façon que l'identité du titulaire de la clé privée et l'intégrité des données numériques puissent être vérifiées à l'aide d'une clé publique certifiée par une autorité de certification.*

Le projet vise essentiellement à réglementer les activités des autorités de certification agréées. Nous ne nous attarderons donc pas sur celui-ci. Une disposition importante contenue dans ce projet (article 3, §5) doit toutefois être mise en évidence :

> ***Article 3, §5.*** *Sans préjudice des articles 1323 et suivants du Code civil, une signature digitale réalisée sur base d'un certificat émis dans les conditions fixées par la présente loi constitue une signature au sens de l'article 1322 du Code civil lorsqu'elle est appliquée à cette fin par une personne physique.*

Le régime sécuritaire qui entoure l'infrastructure de certification agréée est tel qu'il confère à la signature digitale un niveau de sécurité équivalent, voire supérieur, à la signature manuscrite. Dès lors, les conséquences juridiques liées à l'utilisation de la signature digitale doivent être les mêmes que celles qui sont actuellement attachées à l'usage de la signature manuscrite. Le message signé électroniquement à l'aide d'une signature digitale combinée à un certificat émis par une autorité de certification agréée doit constituer une signature au sens de la définition fonctionnelle de la signature qui est insérée dans le Code civil.

57. Cette clause d'assimilation consiste à créer une présomption (réfragable[94]) selon laquelle l'identité de l'auteur, son adhésion au contenu de l'acte ainsi que le maintien de l'intégrité de celui-ci ressortent avec certitude dès que la signature prend la forme d'une signature digitale combinée à un certificat émis par une autorité de certification agréée. Cette présomption

---

93 Ce projet de loi n'a jamais été publié officiellement.

94 La signature peut toujours être contestée par le prétendu signataire.

permet donc de dispenser celui qui se prévaut d'un tel document de faire cette preuve et de lui conférer une force probante qui s'impose au juge. Si le certificat est émis par une autorité de certification non agréée ou s'il ne s'agit pas d'un mécanisme de signature digitale, il appartiendra à celui qui se prévaut d'une signature électronique de prouver que le mécanisme utilisé permet de garantir l'identité, le maintien de l'intégrité et l'adhésion au contenu avec certitude.

Cette présomption a également pour conséquence d'engager juridiquement le signataire. Que se passe-t-il si le prétendu signataire conteste d'avoir signé le document, invoquant qu'un tiers malveillant a réussi à voler sa clé privée, voire à découvrir celle-ci par « reverse engineering » ? Il peut toujours contester sa signature puisque la présomption est réfragable, mais il est vrai que la preuve de la fraude ne sera pas facile à rapporter. On pourrait dès lors croire que la personne qui signe électroniquement se trouve dans une position plus défavorable que la personne qui signe manuscritement puisqu'il est toujours loisible à cette dernière de désavouer sa signature, engageant ainsi la procédure de contestation d'écriture par laquelle un expert tranche la question, ce qui est moins possible pour le *signataire électronique*. Après réflexion, on constate que ce déséquilibre n'existe pas vraiment. En effet, le parallélisme avec la signature manuscrite et la procédure de contestation peut être difficilement fait car l'hypothèse de départ est différente: d'ordinaire, la signature manuscrite peut être imitée facilement par tout le monde. Il est logique que, face à ce risque potentiel de fraude, on donne la possibilité au prétendu signataire de contester sa signature. Dans un système d'accréditation, la donne est autre : le système mis en place est sécurisé en manière telle que le risque qu'un tiers découvre la clé privée du signataire est réduit à zéro, sauf négligence de ce dernier. Dans cette optique, il est juridiquement équitable de faire peser une présomption de responsabilité dans son chef.

58. On peut finalement s'interroger sur l'approche résolument technologique adoptée dans ce projet. Le gouvernement a manifestement fait un choix technologique en considérant que pour l'heure, seule la signature digitale combinée à un certificat émis par une autorité de certification agréée, peut être considérée comme présentant un niveau de sécurité satisfaisant, étant donné qu'elle est le seul procédé de signature à se voir accorder une force probante par la loi. Cela aura pour conséquence de contraindre le législateur à revoir systématiquement sa copie au fur et à mesure qu'apparaîtront des mécanismes de signature électronique jugés sécurisés. N'aurait-il pas été plus judicieux de confier cette tâche à un comité d'experts indépendants, qui serait chargé d'effectuer une veille du marché, et de se prononcer officiellement, le cas échéant, sur la fiabilité d'un mécanisme de signature électronique. Une telle décision aurait pour effet de donner force probante à ce dernier, la loi ayant au préalable reconnu cet effet aux décisions prises par le comité.

3. La complémentarité de ces deux projets

59. Il semble évident que les deux projets de loi belge sont indissociables.

Si seul le projet preuve est adopté, le législateur ne règle que le problème de la recevabilité des documents signés électroniquement, laissant le juge libre d'en apprécier la valeur probante. On a déjà vu, à l'occasion de l'analyse de l'arrêt de la Cour de cassation française du 2 décembre 1997, qu'il s'agissait d'une condition indispensable, mais insuffisante, pour marquer un progrès par rapport au régime actuel.

A l'inverse, le projet sur les autorités de certification, à lui seul, n'apporterait aucune solution juridique sur le plan probatoire car il renvoie à la modification du projet preuve, qui règle le problème de la recevabilité, préalable obligé à l'appréciation de la force probante, et dont il ne peut se passer. De plus, il méconnaîtrait l'approche neutre sur le plan de la technologie qui nous est imposée par la directive européenne sur la signature électronique.

Il est donc indispensable que le Parlement examine et vote simultanément ces deux projets, sans quoi ces lois resteraient lettre morte.

* * *

Réflexions finales

1° Manifestement l'approche fonctionnelle des notions d'écrit et de signature en vue d'y inclure certains écrits et signatures électroniques a conquis ses lettres de noblesse tant en doctrine qu'aux yeux de la plupart des législateurs. Cette méthode d'interprétation, on l'a vu, est désormais largement privilégiée en vue d'adapter le droit de la preuve aux techniques modernes. Son principal mérite est de suggérer combien le Code civil ménage d'ores et déjà une large place aux preuves informatiques, grâce à l'heureuse ouverture des concepts fondamentaux d'écrit et de signature. A telle enseigne qu'il paraît aujourd'hui évident que la réforme attendue pourra se faire sans modification substantielle des dispositions du Code civil relatives à la preuve.

2° La signature numérique, en particulier, est dès à présent jugée apte à remplir les fonctions traditionnellement assignées à la signature manuscrite. Mais il y a plus: les atouts de cette forme de signature sont tels que celle-ci permet en sus de réaliser des fonctions nouvelles, jamais dévolues à la signature classique. Au point que, dans les environnements électroniques, elle semble appelée à jouer un rôle réellement décisif et jusqu'ici inédit. Ce changement de perspective se marque nettement au niveau de la fonction d'identification de la signature. Cantonnée dans le champ probatoire, la signature manuscrite joue un rôle tout à fait mineur dans l'identification du cocontractant. Tout au plus sert-elle à établir *ex post*, en cas de contestation, les engagements dont ce dernier est tenu. En revanche, dans les réseaux de communication, la signature numérique permet d'identifier *a priori* l'interlocuteur et de s'assurer de son consentement. A ce titre, elle apparaît désormais comme une exigence inéluctable au niveau de la formation des actes juridiques. A cet égard, il n'est pas exagéré d'affirmer que la signature change radicalement de finalité.

La signature numérique remplit une autre fonction nouvelle et de première importance: la vérification du maintien de l'intégrité d'un acte au cours de l'échange mais aussi, dans la durée, au niveau de sa conservation. Cette fonction est essentielle en vue d'assurer la fiabilité des flux de données et des échanges contraignants étant donné la structure peu sécurisée des réseaux ouverts.

3° Si la théorie dite des équivalents fonctionnels permet d'asseoir l'idée que les textes du Code civil font déjà droit aux preuves informatiques, une intervention du législateur s'avère néanmoins opportune et même nécessaire. En effet, le commerce électronique est déjà une réalité, mais il est clair que son essor est compromis tant que ne seront pas levées les incertitudes juridiques concernant la valeur probante accordée aux écrits et signatures électroniques. La confiance et la sécurité juridique indispensables ne peuvent s'accommoder de la seule œuvre, inévitablement lente et parcellaire, des cours et tribunaux.

Le législateur serait bien avisé de consacrer formellement l'équivalence de principe entre la signature électronique et la signature manuscrite. A cet égard, on ne saurait trop insister sur certaines recommandations.

Tout d'abord, il évitera d'adopter une définition de la signature qui conduise à l'abolition des développements jurisprudentiels et doctrinaux antérieurs relatifs à la signature manuscrite. Aussi préférera-t-il maintenir la distinction entre signature manuscrite et d'autres formes de signature, et s'attacher à préciser les conditions d'assimilation de celles-ci à celle-là.

Ensuite, le législateur se gardera de freiner les évolutions technologiques en privilégiant des solutions techniques qui pourraient rapidement s'avérer obsolètes. Un principe de neutralité eu égard aux divers procédés de signature électronique devrait guider son intervention. Dans cet ordre d'idées, le législateur sera attentif à la distinction entre recevabilité et force probante. La reconnaissance de la recevabilité des signatures électroniques représente une avancée appréciable, mais insuffisante.

Consacrer la recevabilité de l'écrit signé électroniquement revient à déclarer celui-ci *admissible à titre de preuve*, en ce sens que le juge ne peut l'écarter en considération de sa seule nature informatique. Cependant, à ce stade, le législateur ne se prononce pas sur la force probante des écrits dépourvus d'une signature manuscrite. Ainsi subsiste, en tout cas, la nécessité de convaincre le juge d'accorder à pareil document une force probante égale à celle de l'acte sous seing privé. A cet effet, il revient à celui qui produit en justice un document assorti d'une signature électronique de démontrer la fiabilité de ce type de preuve, c'est-à-dire son aptitude à remplir les fonctions traditionnelles de l'acte sous seing privé. Une telle preuve est redoutable et soumise à l'appréciation du juge qui l'accueillera en fonction des cas d'espèce et de son attitude à l'égard des nouvelles technologies.

Il importe dès lors que le législateur prenne nettement position sur les formes de signature électronique auxquelles il confère même force probante que celle attribuée à la signature manuscrite. Autant le législateur se doit d'être *neutre* sur le terrain de la *recevabilité*, pour permettre au juge d'accueillir et d'apprécier tout procédé de signature, autant il convient qu'il opère des *choix technologiques précis* à l'heure de se prononcer sur la *force probante* puisqu'il s'agit alors, précisément, de dispenser le juge de semblable appréciation.

Enfin, il incombe au législateur de déterminer le statut, les missions et les responsabilités des autorités de certification, ainsi que les conditions de leur accréditation. Il est fondamental de définir rigoureusement le cadre juridique dans lequel s'inscrira l'intervention de ces tiers de confiance, dont a vu le rôle décisif pour refermer en quelque sorte les environnements ouverts en vue de pouvoir y nouer des relations juridiques contraignantes.

Didier GOBERT
Assistant à la faculté de droit de Namur
Chercheur au CRID
Cofondateur de *e*-Consult

Etienne MONTERO
Professeur à la faculté de droit de Namur