L'introduction de la signature électronique sans le Code Civil

Montero, Etienne

Published in:
Mélanges offerts à Marcel Fontaine

Publication date:
2003

Document Version
le PDF de l'éditeur

L'INTRODUCTION DE LA SIGNATURE ÉLECTRONIQUE DANS LE CODE CIVIL : JUSQU'AU BOUT DE LA LOGIQUE « FONCTIONNALISTE » ?

PAR

Étienne MONTERO

Professeur aux Facultés universitaires de Namur

La télématique s'accommode de l'Ordonnance de Moulins

M. FONTAINE [1]

INTRODUCTION

1. De la calligraphie... à la cryptographie. – La reconnaissance juridique de la signature électronique constitue un tournant comparable à celui opéré en 1566 par l'Ordonnance de Moulins. L'inversion de l'ancienne règle « témoins passent lettres » signait l'avènement d'une civilisation de l'écriture. Les lois du 20 octobre 2000 et du 9 juillet 2001 marquent, elles, l'entrée de notre droit dans l'ère de l'écriture... numérique.

L'idée de faire droit aux preuves informatiques par le biais soit d'un régime généralisé de preuve libre, soit d'une sollicitation des exceptions au principe de la prééminence de l'écrit signé a fait long feu [2]. Comme l'on sait, une autre solution s'est imposée, fondée sur une *approche fonctionnelle* des notions d'écrit et de signature. S'opposant à une interprétation formaliste de ces notions, la voie privilégiée met l'accent sur les fonctions dévolues à celles-ci, plutôt que sur leurs conditions dégagées par la doc-

[1] M. FONTAINE, « La preuve des actes juridiques et les techniques nouvelles », in *La preuve*, Colloque UCL, 1987, en conclusion.

[2] Sur les raisons du rejet de ces solutions, voy. l'exposé des motifs du premier projet preuve (« projet de loi visant à modifier certaines dispositions du Code civil relatives à la preuve des obligations »), *Doc. parl.*, Ch. repr., sess. ord. 1998-1999, 2141/1, spéc. p. 14.

trine et la jurisprudence dans un contexte historique où dominait le papier comme support des actes juridiques [3].

Tirant ainsi parti de l'absence de définition légale et de l'ouverture des concepts essentiels d'écrit et de signature, la réforme intervenue préserve les équilibres essentiels de notre droit de la preuve : le principe de la prééminence de la preuve écrite n'est pas mis en cause et les exceptions au principe sont maintenues à leur juste place [4]. Le droit de la preuve du XXI^e^ siècle s'inscrit donc sans véritable solution de continuité – apparemment – dans la ligne des principes fondamentaux déposés dans l'Ordonnance de Moulins, à ceci près que, désormais, l'écriture et la signature électroniques sont assimilées à l'écriture traditionnelle et à la signature tracée (de la main) sur le papier.

Que l'intervention du législateur se soit concentrée sur la signature électronique n'étonne guère dès lors que cette dernière constitue le point névralgique de la preuve des actes juridiques « dématérialisés ». L'admission de la signature électronique suppose, implicitement mais certainement, celle des formes électroniques de l'écrit et de l'acte sous seing privé. Ainsi émancipé de son traditionnel support papier, l'écrit sous forme électronique a fait son entrée dans le Code civil par la grande porte de la preuve littérale.

L'on n'a sans doute pas fini de mesurer les enjeux du passage d'une culture du papier à une culture du numérique. À cet égard, la reconnaissance juridique de la signature électronique ne constitue qu'un premier jalon. La doctrine n'y est pas restée insensible si l'on en juge par le nombre d'études consacrées au sujet [5], dont quelques-unes de notre plume [6]. Le sujet est

[3] *Ibid.*, spéc. pp. 14-15.

[4] *Ibid.*, spéc. p. 1 et p. 14.

[5] En doctrine belge, parmi les études les plus récentes, voy. R. MOUGENOT, *Droit des obligations – La preuve*, Tiré à part du *Répertoire notarial*, 3^e^ éd. revue et mise à jour par D. MOUGENOT, Bruxelles, Larcier, 2002, spéc. pp. 169-206 et pp. 224-228 (cité D. MOUGENOT, *La preuve*) ; J. STEENLANT, « De elektronische handtekening : voortaan juridisch erkend ! », *La Basoche* (à paraître) ; D. COUNYE, « De totstandkoming en het bewijs van de overeenkomst in een virtuele omgeving : overeenkomsten op afstand en de elektronische handtekening », in *Privaatrecht in de reële en virtuele wereld*, Anvers, Kluwer, 2002, pp. 43-83, spéc. pp. 78-82 ; L. GUINOTTE, « La signature électronique après les lois du 20 octobre 2000 et du 9 juillet 2001 », *J.T.*, 2002, pp. 553-561 ; D. GOBERT, « Cadre juridique pour les signatures électroniques et les services de certification : analyse de la loi du 9 juillet 2001 », *La preuve*, Formation permanente – CUP, 2002, vol. 54, pp. 83-172 ; E. ROGER FRANCE et E. DE GROOTE, « La valeur probante des signatures électroniques », *R.D.C.*, 2002, n° 3, pp. 185-203 ; B. DE GROOTE, « Het bewijs in de elektronische handel – Enkele bedenkingen », *A.J.T.*, 2001, pp. 881-901 ; J. DUMORTIER et S. VAN DEN EYNDE, « De juridische erkenning van de elektronische handtekening », *Computerr.*, 2001, pp. 185 et s. ; M.E. STORME, « De invoering van de elektronische handtekening in ons bewijsrecht – Een inkadering van en commentaar bij de nieuwe wetsbepalingen », *R.W.*, 2000-2001, pp. 1505-1525 ; P. LECOCQ et B. VANBRABANT, « La preuve du contrat conclu par voie électronique », in *Le commerce électronique : un nouveau mode de contracter ?*, Liège, Éditions du Jeune Barreau, 2001, pp. 51-137 ; T. VERBIEST et E. WÉRY (avec la collaboration de D. GOBERT et A. SALAUN), *Le droit de l'internet et de la société de l'information*, Bruxelles, Larcier, 2001 ; Y. POULLET et M. ANTOINE, « Vers la confiance ou comment assurer le développement du commerce électronique », in FRNB/KFBN, *Authenticité et informatique – Authenticiteit en informatica*, Bruxelles, Bruylant-Kluwer, 2000, pp. 344-380 ; 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.*, 1998, n° 4/5, pp. 285-310 ; D. MOUGENOT, « Droit de la preuve et technologies nouvelles : synthèse et perspectives », *Droit de la preuve*, Formation permanente – CUP, vol. XIX, octobre 1997, pp. 45-105 ; E. DAVIO, « Preuve et certification sur Internet », *R.D.C.*, 1997, pp. 660-670 ; ID., « Certification, signature et cryptographie », in E. MONTERO (éd.), *Internet face au droit*, Cahiers du CRID, n° 12, E. Story-Scientia, 1997, pp. 65-86.

[6] E. MONTERO, « Définition et effets juridiques de la signature électronique en droit belge : appréciation critique », *La preuve*, Formation permanente – CUP, 2002, vol. 54, pp. 41-82 ; D. GOBERT et E. MONTERO, « L'ouverture de la preuve littérale aux écrits sous forme électronique », *J.T.*, 2001, pp. 114-128 ; ID., « La signature dans les contrats et les paiements électroniques : l'approche fonctionnelle », *D.A./O.R.*, 2000/53, pp. 17-39.

[7] Étude citée à la note 1.

[8] Pour les aspects techniques des signatures électroniques, voy., parmi d'autres, A. JAMAR, « La sécurité des transactions – Introduction technique », in *Le commerce électronique : un nouveau mode de contracter ?*, Liège, Éditions du Jeune Barreau, 2001, pp. 21 et s. ; P. TRUDEL e.a., *Droit du cyberespace*, Québec, Thémis, 2000, chap. 19 ; J. DUMORTIER et P. VAN EECKE, « De nieuwe wetgeving over digitale en elektronische handtekening », in *Recente ontwikkelingen in informatica- en telecommunicatierecht*, Die Keure, 1999, pp. 1 et s. ; J. HUBIN, *La sécurité informatique, entre technique et droit*, Cahiers du CRID, n° 14, E. Story-Scientia, 1998, spéc. pp. 68-112 ; S. PARISIEN et P. TRUDEL, *L'identification et la certification dans le commerce électronique*, Québec, Éd. Yvon Blais Inc., 1996 ; D. SYX, « Vers de nouvelles formes de signature ? Le problème de la signature dans les rapports juridiques », *Dr. inform.*, 1986/3, pp. 133-147.

pourtant loin d'être épuisé : au fur et à mesure des précisions apportées surgissent de nouvelles interrogations... comme si chaque nouvelle lumière faisait mieux ressortir les ombres du tableau. Qu'il nous soit donc permis de récidiver, en hommage au professeur Fontaine, qui s'est illustré, en 1987 déjà, par une étude magistrale intitulée « La preuve des actes juridiques et les techniques nouvelles » [7]. Quinze ans plus tard, la doctrine ne cesse de se référer à cette contribution prémonitoire à bien des égards. L'on y trouve énoncés les principes essentiels – rappelés plus haut – qui ont guidé les promoteurs de la réforme du droit de la preuve.

2. Objet et limites du propos. – Comment faire du neuf sur un thème qui a déjà mobilisé tant de plumes... ou de souris ? Il n'est naturellement pas question de redire tout ce qui a déjà été dit. Aussi est-il exclu de décrire une fois encore les différents procédés de signature électronique [8],

mais aussi d'examiner par le menu les textes de droit européen[9] ou belge[10] y relatifs. Nettement plus ciblé, notre propos est de commenter l'introduction de la signature électronique dans le Code Napoléon. Conformément au vœu des instigateurs de ces mélanges, il s'agit, pour l'essentiel, de répondre à la question : convient-il de modifier l'article 1322, alinéa 2, du Code civil ? Dès lors qu'elle est relative à une disposition de facture si récente, pareille question prend des allures de provocation. Soit. Aussi, pour faire bonne mesure, au-delà d'une simple critique textuelle, nous tâcherons de fournir quelques clés de lecture de cette disposition audacieuse, mais aussi dense et énigmatique, « qui doit encore passer au banc de l'interprétation judiciaire »[11].

Mal emmanchée, la réforme dont question surprend d'emblée sur le plan de la *méthode* législative adoptée (chap. I). Au-delà, *le texte même* de l'article 1322, alinéa 2, appelle quelques remarques sur la forme et sur le fond : celles-ci concernent tant le domaine de la définition fonctionnelle (chap. II) que les conditions énoncées (chap. III). Enfin, *les effets* juridiques de la nouvelle disposition suscitent hésitations et controverses doctrinales[12], lesquelles pointent vers des questions plus fondamentales qui touchent au cœur de la réforme et constitueront le noyau de la présente contribution (chap. IV et V).

Chapitre I
Questions de méthode

3. La quadrature du cercle ? – Progressivement acquis à l'idée d'adopter une définition fonctionnelle de la signature électronique, le législateur belge a tôt fait de mesurer l'ambivalence de cette solution. L'avantage d'une telle définition, souple et ouverte, réside dans son aptitude à résister aux évolutions technologiques. Mais cette force fait aussi sa faiblesse. Cette seule

[9] Sur la directive, voy. M. Antoine et D. Gobert, « La directive européenne sur la signature électronique : vers la sécurisation des transactions sur l'Internet ? », *J.T.D.E.*, 2000, n° 68, pp. 73-78 et E. Caprioli, « La directive européenne n° 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électronique », *Gaz. Pal.*, 2000, pp. 5-17.

[10] Cf. les références citées aux notes 5 et 6.

[11] Rappr. J. Devèze, « Vive l'article 1322 ! Commentaire critique de l'article 1316-4 du Code civil », in *Le droit privé français à la fin du XX^e siècle – Études offertes à P. Catala*, Paris, Litec, 2001, p. 529.

[12] Au passage, il sera difficile de ne pas faire quelque allusion à l'article 4, § 4, de la loi du 9 juillet 2001 tant les deux dispositions sont étroitement liées.

approche présente, en effet, l'inconvénient de reporter sur le juge le soin d'apprécier, au cas par cas, la réalisation des fonctions attendues, et de mettre dès lors le justiciable en situation de devoir emporter sa conviction. L'admissibilité comme preuve en justice des signatures électroniques s'en trouve assurée, mais la valeur probante des documents qui en sont munis demeure aléatoire. Ainsi est apparue la nécessité de pointer, parmi les techniques existantes, celles qui sont propres à rencontrer les fonctions énumérées dans la définition ouverte et techniquement neutre de la signature.

À la suite du législateur européen, la Belgique est arrivée à la conclusion que ces deux approches, apparemment contradictoires, ne sont pas incompatibles. Il a donc été décidé de les cumuler par l'adoption de deux textes complémentaires : un texte général visant à introduire dans le Code civil une définition fonctionnelle de la signature électronique et un texte plus technique, sous la forme d'une loi particulière, visant, d'une part, à désigner un mécanisme de signature électronique présumé apte à réaliser les fonctions attendues, d'autre part, à définir le cadre juridique des activités de certification.

Cette méthode doit être globalement approuvée, n'était-ce la manière et le partage des textes.

4. Une réforme bâclée ? – Pour mémoire, on rappelle qu'initialement deux textes avaient été préparés : un avant-projet de loi « visant à modifier certaines dispositions du Code civil relatives à la preuve des obligations »[13] et un avant-projet de loi « relative à l'activité d'autorités de certification agréées en vue de l'utilisation de signatures digitales »[14]. Devenu caduc au terme de la législature, le premier texte, largement remanié, a refait surface sous la forme – pour le moins curieuse – d'un amendement à la proposition de loi du 4 août 1999 « introduisant de nouveaux moyens de télécommunications dans la procédure judiciaire et extrajudiciaire » (projet « Bourgeois »)[15]. Cet amendement est à l'origine du nouvel alinéa de l'article 1322 du Code civil. Le projet ainsi amendé deviendra la loi du 20 octobre 2000 « introduisant l'utilisation de moyens de télécommunication *et de la signature électronique* dans la procédure judiciaire et extrajudiciaire »[16].

[13] *Doc. parl.*, Ch. repr., sess. ord. 1998-1999, n° 2141/1, p. 20.

[14] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, doc. 50 0322/001, pp. 44 et s.

[15] Amendement n° 12 (du gouvernement) à la Proposition de loi introduisant de nouveaux moyens de télécommunication dans la procédure judiciaire et extrajudiciaire (13 juin 2000), *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, doc. 50 0038/006, p. 1.

[16] *M.B.*, 22 décembre 2000, p. 42698.

Au total, les règles du Code civil relatives à la preuve ont donc été modifiées par le biais d'un amendement à une proposition de loi tendant à modifier... le Code judiciaire. La manière n'enchante guère sur le plan légistique [17]. On échappe difficilement à l'impression que cette réforme – importante ! – du droit de la preuve n'a pas reçu l'attention qu'elle méritait. Alors que l'amendement n° 12 avait déjà été introduit, les travaux préparatoires affirment encore que « la proposition de loi ne concerne pas le droit de la preuve » [18]. Inadvertance certes, mais qui n'en est pas moins symptomatique...

Le second texte, profondément remanié, lui aussi, par un amendement du 10 novembre 2000 [19], est devenu la loi du 9 juillet 2001 « fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification » [20]. Cette loi accorde un régime de faveur à la « signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique ». Sans préjudice des articles 1323 et suivants du Code civil, pareille signature – que nous appellerons, pour la facilité, « signature électronique qualifiée » – est assimilée de plein droit à une signature manuscrite, qu'elle soit réalisée par une personne physique ou morale (art. 4, § 4, de la loi). Pour le reste, comme l'indique son intitulé, la loi définit le régime juridique applicable aux activités des prestataires de service de certification (en abrégé, PSC), ainsi que les règles à respecter par ces derniers et par les titulaires de certificats.

5. Le partage de la matière. – L'idée de poser les principes essentiels dans le Code civil – sobrement retouché – et de renvoyer à une loi particulière pour le détail des aspects techniques est séduisante. Encore eût-il fallu que l'essentiel – rien que l'essentiel, mais tout l'essentiel – soit concentré dans le Code. Or il n'en est rien. L'article 1322 est excessivement laconique. Il donne une définition fonctionnelle de la signature électronique... mais on trouve deux autres définitions dans la loi du 9 juillet 2001 (art. 2, 1° et 2°). Il consacre le principe de non-discrimination de l'article 5, 2, de la directive, mais cette dernière disposition a également fait l'objet d'une retranscription littérale à l'article 4, § 5, de la loi. Enfin, il ne dit pas tout sur la question de la force probante des signatures

[17] En ce sens, D. MOUGENOT, *La preuve*, *op. cit.*, p. 187, n° 122-2.
[18] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, doc. 50 0038/008, p. 3.
[19] Amendement n° 1 du gouvernement, *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, doc. 50 0322/002.
[20] *M.B.*, 29 juillet 2001, p. 33070.

électroniques, qui est réglée pour partie également à l'article 4, § 4, de la loi. Il résulte de tout ceci que des questions essentielles sont réglées dans deux textes distincts, ce qui fait désordre et ne facilite guère leur lisibilité [21].

L'on aurait préféré que la question des effets juridiques (recevabilité et force probante) des signatures électroniques soit réglée dans un seul texte [22]. Ainsi, le Code civil aurait pu non seulement contenir une définition fonctionnelle de la signature électronique [23], mais aussi consacrer le principe de l'assimilation de plein droit d'une signature électronique répondant aux conditions fixées dans une loi particulière à une signature manuscrite. Ladite loi se serait bornée, pour sa part, à *préciser les conditions techniques* pour qu'une signature électronique soit assimilée de plein droit à une signature manuscrite et à définir le cadre juridique des services de certification.

Chapitre II

LE DOMAINE DE LA DÉFINITION FONCTIONNELLE

6. Une occasion manquée ? – Il est à remarquer que la définition fonctionnelle figurant à l'article 1322, alinéa 2, du Code civil se rapporte seulement aux signatures électroniques. La signature, dont on exprime les fonctions, doit consister, en effet, en un « ensemble de données électroniques ». Cette disposition ne permet dès lors pas de couvrir certaines formes de signature manuscrite ne satisfaisant pas aux conditions posées par la Cour de cassation (critère de la *marque habituelle* [24], nécessité de tracer la signature directement sur le document lui-même [25]), voire d'autres signes non électroniques (ainsi les empreintes digitales – non numéri-

[21] À ce propos, voy. les commentaires de L. GUINOTTE, *op. cit.*, pp. 559-560.
[22] Dans un sens analogue, voy. déjà les observations générales du Conseil d'État relatives au premier projet preuve : *Doc. parl.*, Ch. repr., sess. ord. 1998-1999, n° 2141/1, p. 22.
[23] Ou, mieux, de la signature « tout court ». Voy. ci-après, n° 6.
[24] Cass., 7 janvier 1995, *Pas.*, 1995, I, p. 456 ; Cass., 2 octobre 1964, *Pas.*, 1965, I, p. 106. Dans des arrêts ultérieurs, la Cour semble avoir assoupli le critère : Cass., 10 juin 1983, *T. Not.*, 1986, p. 309, note M. PUELINCKX-COENE ; Cass., 13 juin 1986, *Pas.*, 1986, I, p. 1269. Voy. aussi Liège, 5 juin 1996, *Pas.*, 1996, II, p. 92 ; *R.R.D.*, 1996, p. 567 ; Civ. Anvers, 7 septembre 1989, *T. Not.*, 1990, p. 109.
[25] Cass., 28 juin 1982, *Pas.*, 1982, I, p. 1286 ; *R.C.J.B.*, 1985, pp. 57 et s. et la note de M. VAN QUICKENBORNE, « Quelques réflexions sur la signature des actes sous seing privé » ; Trib. trav. Charleroi, 13 novembre 1995, *Chron. D.S.*, 1997, p. 247 ; J.P. Torhout, 12 septembre 1995, *D.C.C.R.*, 1994-1995, p. 465 ; *R.W.*, 1995-1996, p. 890.

sées – auraient pu bénéficier d'une prise en considération par le juge, celui-ci restant libre de constater que les conditions ne sont pas remplies).

La démarche suivie en France est tout autre dès lors que toutes les formes de signature – manuscrite, électronique ou autre – sont visées par la définition de l'article 1316-4 libellé comme suit : « La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. [...] Lorsqu'elle est électronique, elle consiste [...] ». Cette optique nous paraît plus conforme à la logique de l'approche fonctionnelle que celle privilégiée par le législateur belge [26]. Au plan des principes, il n'est guère heureux que la signature manuscrite et la signature électronique reposent sur des conceptions différentes, étant donné que la seconde se veut la transposition, dans l'univers électronique, des fonctions assignées à la première dans l'univers traditionnel [27].

Sans doute l'approche fonctionnelle pourrait-elle s'imposer, par la voie jurisprudentielle, en dehors de l'hypothèse visée au texte. Elle permettrait de s'écarter de la notion formaliste de la signature retenue par la Cour de cassation à une époque où il était seulement question de la signature manuscrite. À la réflexion, une définition fonctionnelle n'oblige pas nécessairement à remettre en cause l'acquis jurisprudentiel relatif à la signature manuscrite. Au moment d'apprécier si une telle signature satisfait aux fonctions attendues – identification et manifestation du consentement au contenu de l'acte –, le juge pourrait continuer de requérir qu'elle satisfasse aux exigences traditionnelles (critère de la signature habituelle, apposition au bas de l'acte sur support papier, etc.).

7. La portée des termes « pour l'application du présent article ». – Selon les documents parlementaires, cette restriction viserait à traduire l'adage *lex specialis derogat legi generali*. L'objectif est de ne pas toucher aux dispositions spécifiques relatives à la preuve ou aux prescriptions concernant la forme de certaines obligations contractuelles, telles que prévues par le Code civil lui-même ou par une réglementation spécifique. Autrement dit, la reconnaissance juridique de la signature électronique ne signifie pas que celle-ci puisse être utilisée pour l'application de toutes les règles de droit, y compris celles impliquant l'utilisation de documents papier (et de mentions manuscrites). En guise d'illustration, il est fait référence aux articles 970 (testament holographe) et 1326 (formalité dite du

[26] Voy. notre étude précitée « Définition... », p. 50, n° 11.
[27] En ce sens, D. MOUGENOT, *La preuve*, *op. cit.*, p. 164, n° 110.

« bon pour ») du Code civil, qui demeurent intégralement applicables, mais également aux législations relatives au chèque, au billet à ordre et à la lettre de change. Dans ces hypothèses, une signature électronique est naturellement exclue, en attendant une adaptation des dispositions concernées.

Cela étant, la restriction évoquée est mal libellée à un double titre :

- le champ d'application des signatures électroniques n'est pas limité à l'article 1322 : l'intention du législateur est clairement de rendre les articles 1323 et 1324 également applicables aux écrits et signatures électroniques [28] ;
- il faut considérer, en réalité, que l'article 1322 est susceptible de s'appliquer à tous les actes sous seing privé (y compris, par exemple, ceux visés par l'article 1326 C. civ.). En soi, la restriction est inapte à écarter l'article 1322, alinéa 2, dans les hypothèses concernées par l'article 1326. C'est plus précisément par application du principe *lex specialis*... que la signature électronique (1322, al. 2) est exclue, dans ces hypothèses. En d'autres termes, il ne s'agit pas de réserver les signatures électroniques aux seuls cas où l'article 1322 trouve à s'appliquer, mais de laisser subsister les régimes qui requièrent expressément des mentions manuscrites. Cette intention aurait été mieux rendue par une expression du genre : « Hormis les exceptions prévues par des dispositions légales particulières, peut satisfaire... ».

Cela étant, le problème d'interprétation évoqué perd de son acuité depuis l'adoption de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information. L'article 16 de cette loi admet, en effet, des « équivalents électroniques » à la signature manuscrite, aux mentions manuscrites et à d'autres exigences de forme associées au support papier, requises non seulement *ad probationem* mais aussi *ad validitatem* [29].

[28] Voy., en ce sens, les observations formulées par le service juridique de la Chambre au sujet de l'amendement n° 12, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, doc. 50 0038/008, pp. 33-34, qui conclut : « Cela est en contradiction avec le texte de l'amendement qui limite le champ d'application des signatures électroniques à l'article 1322 du Code civil. »
[29] *M.B.*, 17 mars 2003, p. 12962. Pour un premier commentaire, voy. M. DEMOULIN et E. MONTERO, « Le formalisme contractuel à l'heure du commerce électronique », in *La théorie générale des obligations, suite*, Formation permanente – CUP, vol. 57, octobre 2002, pp. 97-181.

Chapitre III
LES EXIGENCES POSÉES PAR L'ARTICLE 1322, ALINÉA 2, DU CODE CIVIL

8. Preuve, certitude et vraisemblance. – L'article 1322, alinéa 2, du Code civil pose une double exigence d'imputabilité et d'intégrité, suivant une formulation apparemment inspirée par un arrêt de la Cour de cassation française du 2 décembre 1997 [30]. L'énoncé de ces conditions suscitent des réserves tant au niveau terminologique que sur le fond [31].

Avant de les aborder, il n'est pas inutile de rappeler que la preuve en droit ne poursuit pas les mêmes objectifs que la preuve en science ou en histoire. Elle n'en a ni l'esprit ni les procédés [32]. Aucune preuve juridique ne confère une certitude absolue, mais seulement une probabilité [33]. En droit, la preuve est liée à la contestation et a pour but de convaincre le juge. Or celui-ci est obligé de statuer [34] : même lorsqu'il n'a pas de certitude, il doit trancher le litige, en se contentant, le cas échéant, d'une vraisemblance ou de simples probabilités. Cette observation générale ne devrait pas être perdue de vue tant il est vrai que, méfiants à l'égard de l'informatique, d'aucuns sont naturellement portés à revoir à la hausse leurs exigences à l'égard des preuves qui en sont issues, oubliant un peu vite les limites et les imperfections liées au support papier [35].

Dans cet ordre d'idées, pour revenir à la disposition qui nous occupe, le Conseil d'État a critiqué, à juste titre, l'utilisation du terme « certitude », jugé « excessivement précis », dans la première mouture de l'article

[30] Cass. fr. (com.), 2 décembre 1997, D., 1998, p. 192, note D. MARTIN ; *J.C.P.*, G, 1998, II 10 097, p. 1105, note L. GRYNBAUM ; *J.C.P.*, E, 1998, p. 178, note T. BONNEAU ; *J.C.P.*, G, 1998, aperçu rapide par P. CATALA et P.-Y. GAUTIER, p. 905.

[31] Dans ce point III, nous reprenons certaines réflexions émises dans une étude antérieure précitée « Définition... », pp. 65 et s.

[32] À ce sujet, les célèbres notes de BARTIN à la 5e édition du texte (qu'il ne voulut pas modifier) d'AUBRY et RAU, *Droit civil français*, t. XII, 5e éd., 1922, § 749, notes. Voy. aussi Ph. MALAURIE et L. AYNÈS, *Droit civil – Introduction générale*, Paris, Cujas, 1991, spéc. pp. 101-102, nos 308 et s.

[33] Étymologiquement, prouver vient du latin *probare*, dont dérivent aussi les termes « probable », « probabilité », etc.

[34] Art. 5 C. jud.

[35] À ce sujet, M. DEMOULIN et E. MONTERO, « La conclusion des contrats par voie électronique », in M. FONTAINE (dir.), *Le processus de formation du contrat – Contributions comparatives et interdisciplinaires à l'harmonisation du droit européen*, Bruxelles-Paris, Bruylant-L.G.D.J., 2002, p. 719, n° 35 ; E. CAPRIOLI et R. SORIEUL, « Le commerce international électronique : vers l'émergence de règles juridiques transnationales, *J.D.I.*, 2, 1997, p. 383.

1322, alinéa 2 [36], d'autant que « l'intention des auteurs du texte en projet [n'était] pas d'empêcher toute contestation sur cette identité ou cette adhésion dès qu'elles sont attestées par un procédé » de signature électronique [37].

On gardera donc précieusement en mémoire, dans la suite de l'exposé, que les conditions posées par l'article 1322, alinéa 2, doivent s'apprécier raisonnablement : le procédé de signature électronique doit attester avec une fiabilité suffisante – sans certitude (absolue) [38] – l'identité de l'auteur de l'acte, son adhésion au contenu et la maintien de l'intégrité du contenu de l'acte.

9. L'imputabilité. – Il ressort des travaux préparatoires de la loi du 20 octobre 2000 que la *condition d'imputabilité* est censée recouvrir les fonctions classiquement dévolues à la signature, à savoir l'*identification* (du signataire) et la manifestation de son *adhésion au contenu* de l'acte [39]. D'emblée, l'on peut regretter que les fonctions d'identification et d'adhésion ne soient pas expressément mentionnées à l'article 1322, alinéa 2. L'intérêt d'une définition fonctionnelle de la signature électronique n'est-il pas précisément d'égrener les différentes fonctions assignées à celle-ci ?

9-1°. L'identification. – À notre avis, il n'y avait pas lieu de préférer la notion – abstraite et fuyante – d'imputabilité à celle – concrète et précise – d'identification. L'on y perd en précision dès lors qu'un contenu semble pouvoir être « imputé » – qu'est-ce à dire précisément ? – à une personne, *sans que celle-ci puisse être désignée avec assurance comme son auteur.*

L'identification ferait référence au lien matériel existant entre un texte et son auteur. L'imputabilité, quant à elle, viserait plutôt à désigner la per-

[36] « Est assimilé à une signature manuscrite l'ensemble des données issues de la transformation de l'écrit et dont il ressort *avec certitude* l'identité de l'auteur et son adhésion au contenu de l'écrit » (souligné par nous).

[37] Avis du Conseil d'État, *Doc. parl.*, Ch. repr., sess. ord. 1998-1999, 2141/1, p. 28, soulignant avec pertinence la contradiction entre l'intention et le texte : « Il ne se comprendrait pas, en effet, que le procédé désigne avec certitude l'auteur de l'acte et que l'auteur désigné puisse néanmoins, malgré cette certitude, ne pas le reconnaître comme sien. »

[38] Les documents parlementaires parlent de « certitude raisonnable ». Cf. *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, doc. 50, 0322/001, p. 14.

[39] Justification de l'amendement n° 12 (du gouvernement) à la proposition de loi introduisant de nouveaux moyens de télécommunication dans la procédure judiciaire et extrajudiciaire (13 juin 2000), *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, doc. 50 0038/006, p. 11, et le rapport fait au nom de la commission de la Justice par Bart SOMERS (30 juin 2000), *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, doc. 50 0038/008, p. 30.

sonne apte à rendre compte d'un fait ou d'un acte. Cette notion, typique en droit pénal, renverrait à un lien d'intentionnalité ou de responsabilité. Ces considérations ont conduit le Sénat français à préférer, dans un souci de clarté, « ne pas substituer la notion d'imputabilité à celle de l'identification de la personne dont émane le document » [40].

9-2°. L'adhésion au contenu de l'acte. – L'imputation de la signature à une personne déterminée implique-t-elle nécessairement l'imputation à cette dernière du contenu de l'acte signé ? Par ailleurs, l'imputabilité d'un contenu implique-t-il de soi la volonté d'y adhérer ? Qu'en est-il, en d'autres termes, de l'*animus signandi* ?

Également absente dans la directive du 13 décembre 1999, la fonction d'adhésion au contenu de l'acte apparaissait clairement dans la première version de la proposition de directive [41], ainsi que dans le premier projet belge [42].

Notre première interrogation, énoncée ci-avant, est d'autant plus aiguë que n'apparaît pas explicitement, dans l'article 1322, alinéa 2, la nécessité d'un lien, sinon physique, au moins logique, entre l'acte et la signature. On observe en effet que, s'écartant du texte de la directive (« une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques [...] » [43]), le législateur belge se contente d'« un ensemble de données électroniques pouvant être imputé à une personne déterminée [...] ».

Lorsqu'il est question d'une signature numérique fondée sur la cryptographie asymétrique, la signature est le résultat d'une transformation de l'écrit par application d'une clé de chiffrement. En pareil cas, on conçoit assez aisément que l'imputation d'un ensemble de données électroniques à une personne déterminée puisse impliquer son adhésion au contenu de l'acte. Mais cette déduction repose, de toute évidence, sur un présupposé tech-

[40] Rapport de M. Charles JOLIBOIS, au nom de la commission des lois, n° 203 (1999-2000), disponible sur le site www.legifrance.gouv.fr.

[41] Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques, *J.O.C.E.*, n° C 325 du 23 octobre 1998, p. 1 : « Aux fins de la présente directive, on entend par signature électronique une signature sous forme numérique intégrée, jointe ou liée logiquement à des données, utilisée par un signataire *pour signifier son acceptation du contenu des données* [...] ».

[42] Avant-projet de loi « visant à modifier certaines dispositions du Code civil relatives à la preuve des obligations », *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 2141/1, p. 20.

[43] Art. 2, 1. À ce propos, voy. les observations formulées par le service juridique de la Chambre au sujet de l'amendement n° 12, *Doc. parl.*, Ch. repr., sess. 1999-2000, doc. 50 0038/008, p. 32.

nique, qui n'a pas vraiment sa place dans une définition fonctionnelle de la signature. En tout état de cause, il n'est guère possible d'accorder une valeur juridique à une signature électronique si elle n'est pas jointe ou liée logiquement au contenu sur lequel l'auteur marque son consentement [44].

Par ailleurs – à propos de notre seconde interrogation –, il ressort de la jurisprudence (notamment celle relative à la place de la signature [45]) que la présence d'une signature que l'on peut rattacher à une personne déterminée ne dispense pas le juge de rechercher si cette dernière a effectivement voulu marquer son adhésion au contenu de l'acte. On ne saurait donc estimer que l'imputabilité de la signature implique *en tout état de cause* l'adhésion au contenu. En revanche, la signature *reconnue ou non contestée* crée une présomption *juris et de jure* que le signataire a donné son consentement au contenu de l'acte [46]. En pratique, on considérera que l'*animus signandi* se manifeste, par exemple, lors de la saisie, par le signataire, du code secret permettant l'activation de sa clé cryptographique. Néanmoins, il n'est pas exclu qu'un juge estime, en cas de contestation, que telle signature électronique, bien qu'imputable à telle personne, n'atteste pas son intention de s'approprier le contenu de l'acte [47]. Même si cette condition n'est pas inscrite explicitement dans le texte [48], elle y figure implicitement sous la notion d'imputabilité éclairée par les travaux préparatoires, et se déduit, du reste, de la théorie générale de la signature.

10. Le maintien de l'intégrité. – On se demande si le législateur belge a eu raison d'exiger que toute signature électronique soit apte à établir le *maintien de l'intégrité du contenu de l'acte*. Pareille fonction, si elle s'avère une qualité incontestable de la signature numérique fondée sur un

[44] Rapport de M. Charles JOLIBOIS, au nom de la commission des lois, n° 203 (1999-2000), précité.

[45] Cf. N. VERHEYDEN-JEANMART, *Droit de la preuve*, Bruxelles, Larcier, 1991, pp. 240-242, n°s 508 et s., et les réf.

[46] M. VAN QUICKENBORNE, « Quelques réflexions sur la signature des actes sous seing privé », note sous Cass. (3e ch.), 28 juin 1982, *R.C.J.B.*, 1985, pp. 65 et s., spéc. pp. 69-70, n°s 5 et 6. Les travaux préparatoires de la loi du 20 octobre 2000 confirment explicitement ce point de vue général. Cf. justification de l'amendement n° 12 (du gouvernement) à la proposition de loi introduisant de nouveaux moyens de télécommunication dans la procédure judiciaire et extrajudiciaire (13 juin 2000), *Doc. parl.*, Ch. repr., sess. 1999-2000, doc. 50 0038/006, p. 11, et le rapport fait au nom de la commission de la Justice par Bart SOMERS (30 juin 2000), *Doc. parl.*, Ch. repr., sess. 1999-2000, doc. 50 0038/008, p. 30.

[47] Voy. aussi *infra*, n° 11 et note 59.

[48] Comp. avec la loi de l'Utah (applicable aux seules signatures numériques) qui assimile la signature digitale à la signature manuscrite, sous diverses conditions, notamment « if that digital signature was affixed by the signer with the intention of signing the message » (art. 46-3-401, b).

cryptosystème asymétrique [49], devait-elle pour autant être posée comme une exigence de toute forme de signature électronique ?

Tout se passe comme si l'intangibilité du contenu de l'acte instrumentaire ne pouvait résulter que du mécanisme de signature. Sans doute ce postulat, et l'exigence qu'il sous-tend, est-il tributaire d'une technique bien précise : encore et toujours... la signature numérique fondée sur la cryptographique asymétrique. Faut-il y déceler une entorse à la neutralité technologique prônée par le législateur européen... et belge ? L'hésitation est permise : force est d'admettre que le texte est potentiellement susceptible de concerner divers procédés. Mais il est clair que ses rédacteurs ont constamment eu à l'esprit un modèle mental précis.

Selon divers experts consultés, la garantie d'intégrité peut être assurée, dans un environnement électronique, par des procédés techniques autres que celui de la signature. Il existe effectivement divers moyens [50] de protéger et d'assurer le maintien de l'intégrité d'un document expédié par le biais de l'internet. Pourquoi donc confier obligatoirement à la signature le soin d'assurer une fonction – le maintien de l'intégrité – qui relève logiquement de l'écriture [51] ?

Certes, dans l'état actuel des choses, la signature numérique à clés asymétriques est le procédé *le plus apte* à garantir le *maintien de l'intégrité du contenu de l'acte*. Néanmoins, autre chose est de constater qu'il en *est* actuellement ainsi, autre chose de décider qu'il *doit* en *être* nécessairement ainsi.

À notre sens, il eût mieux valu poser le maintien de l'intégrité comme condition de l'acte sous seing privé électronique, sans exiger que cette intégrité résulte du mécanisme de signature [52].

Il importe peu, en définitive, que l'intégrité de l'acte invoqué en justice soit fonction de l'écriture, du support ou de la signature. Dès lors que l'intégrité de l'acte est attestée et que le mécanisme de signature utilisé par les parties permet de les identifier et d'exprimer leur adhésion, faut-il dénier à ce dernier la qualité de signature au motif qu'il n'établit pas, par lui-même, le maintien de l'intégrité du contenu de l'acte ?

[49] D. GOBERT et E. MONTERO, *op. cit.*, *D.A./O.R.*, spéc. pp. 23-24, n^os^ 22 et 23.

[50] Utilisation de programmes de cryptage, de systèmes de formatage difficile à découvrir, de mots de passe, etc.

[51] Rappr. J. DEVÈZE, *op. cit.*, p. 536.

[52] Opinion déjà exprimée dans notre étude précitée « Définition... », p. 72, n° 40, et suivie par D. MOUGENOT, *La preuve*, *op. cit.*, p. 194.

Envisagée un moment en Belgique, avant d'être abandonnée [53], la solution qui a notre préférence a été retenue par le législateur français [54].

Chapitre IV
LES EFFETS CONFÉRÉS PAR L'ARTICLE 1322, ALINÉA 2, DU CODE CIVIL

11. Principes. – Il ressort des travaux préparatoires que l'article 1322, alinéa 2, du Code civil peut être regardé, au minimum, comme la transposition du principe de non-discrimination de la directive (art. 5, 2). Pratiquement, cela signifie que le juge est tenu de prendre en considération tout ensemble de données électroniques présenté comme une signature. Il ne peut priver d'efficacité juridique une signature électronique au seul motif que la signature se présente sous forme électronique ou ne remplit pas chacune des conditions de la signature électronique qualifiée.

On conviendra néanmoins que, sans le secours des travaux préparatoires, l'on n'est guère porté à analyser l'article 1322, alinéa 2, comme la transposition de l'article 5, 2, de la directive [55]. Au demeurant, suite à un amendement déposé *in extremis*, l'article 4 de la loi du 9 juillet 2001 a été complété par un paragraphe 5, lequel reproduit littéralement l'article 5, 2, de la directive [56]. Par ailleurs, l'article 1322, alinéa 2, ne se contente pas

[53] Cf. l'article 3 de l'avant-projet de loi « visant à modifier certaines dispositions du Code civil relatives à la preuve des obligations », *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 2141/1, p. 20.

[54] Cf. l'art. 1316-1 C. civ. : « L'écrit sous forme électronique est admis en preuve [...] sous réserve [...] et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. » Par ailleurs, l'article 1316-4, alinéa 2, prévoit, d'une part, que la signature électronique doit consister en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle se rattache (outre qu'elle doit satisfaire aux autres fonctions assignées à toutes les formes de signature par l'article 1316-4, alinéa 1^er^), et institue, d'autre part, une présomption réfragable de fiabilité au profit des signatures électroniques créées dans des conditions fixées par décret. Seules ces dernières signatures (c'est-à-dire, en l'occurrence, les signatures électroniques « qualifiées ») se voient assigner une fonction de maintien de l'intégrité de l'acte.

[55] Cet article énumère une série de motifs bien précis, en prévoyant que le juge ne pourrait se contenter de les invoquer pour refuser l'efficacité juridique et la recevabilité comme preuve en justice d'une signature électronique. Cf. la note suivante.

[56] L'article 4, § 5, de la loi du 9 juillet 2001 s'énonce comme suit : « Une signature électronique ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice au seul motif :
– que la signature se présente sous forme électronique, ou
– qu'elle ne repose pas sur un certificat qualifié, ou

d'interdire toute discrimination arbitraire à l'égard des signatures électroniques ; il fixe, en outre, les conditions positives auxquelles le juge est autorisé à assimiler une signature électronique ordinaire à une signature manuscrite.

En l'absence de contestation relative à une signature électronique – c'est-à-dire vraisemblablement dans l'immense majorité des cas –, le juge sera tenu de lui reconnaître les mêmes effets juridiques qu'une signature manuscrite, ce qui signifie que le document électronique auquel est liée cette signature est élevé au rang d'acte sous seing privé ; à ce titre, il est recevable en justice (art. 1341 C. civ.) et fait pleine foi de son contenu (art. 1319, 1320 et 1322 C. civ.)[57].

Qu'en est-il en cas de contestation ? Concrètement, le débat judiciaire peut tourner autour de deux questions distinctes[58] : une première question est de savoir si tel procédé utilisé constitue une signature valable. En matière de signature traditionnelle, ce simple problème juridique de qualification peut être aisément tranché par le juge. Ainsi peut-il estimer que tel signe ne constitue pas une signature valable pour divers motifs[59]. En cas de signature valable, une seconde question peut surgir : cette signataire est-elle imputable au signataire apparent ? Il est encore loisible à ce dernier de dénier son écriture et d'inciter le demandeur à recourir à la procédure de vérification d'écritures.

La signature électronique peut donner lieu au même double débat. Tout d'abord, le juge peut être invité à se prononcer sur la qualification de tel procédé. C'est ici que s'apprécie tout l'intérêt de l'article 4, § 4, de la loi du 9 juillet 2001 – et la grande différence entre une signature électronique qualifiée et une signature électronique ordinaire[60] ! En effet, une signature électronique qualifiée est assimilée automatiquement à une signature manuscrite ; à cet égard, les vérifications à effectuer par le juge

– qu'elle ne repose pas sur un certificat délivré par un prestataire accrédité de service de certification, ou

– qu'elle n'est pas créée par un dispositif sécurisé de création de signature. »

[57] L. Lecocq et B. Vanbrabant, *op. cit.*, n° 96 ; E. Montero, « Définition... », *op. cit.*, pp. 61-62. Comp. D. Mougenot, *La preuve*, *op. cit.*, p. 199.

[58] Voy., à cet égard, l'exposé particulièrement éclairant de D. Mougenot, *La preuve*, *op. cit.*, p. 225, n° 158-1.

[59] Soit le signe est illisible, soit il n'a pas été apposé directement sur l'acte (papier carbone, photocopie, télécopie, etc.), soit il ne manifeste pas l'adhésion de son auteur au contenu de l'acte (eu égard à son emplacement...).

[60] Comp. D. Mougenot, *La preuve*, *op. cit.*, p. 199.

seront *simples et objectives*[61]. En revanche, dans le cadre de l'article 1322, alinéa 2, les vérifications seront *plus complexes et subjectives* : le juge devra vérifier si le procédé de signature qui lui est présenté satisfait aux conditions d'imputabilité et d'intégrité. Il jouit, à cet égard, d'un incontestable pouvoir d'appréciation en ce qui concerne le niveau d'imputabilité et de garantie d'intégrité dont il se satisfait. Pourvu qu'il motive sa décision, de façon cohérente, eu égard aux conditions de l'article 1322, alinéa 2, on conviendra que sa marge de manœuvre est appréciable à l'heure de reconnaître ou non la validité du procédé de signature électronique. Au cas où le procédé est estimé valable, le prétendu signataire peut encore dénier sa signature et obliger la partie qui invoque l'acte à demander une vérification d'écritures. Cette possibilité lui est ouverte en toute hypothèse, selon nous (*infra*, n°s 13 et s.).

Si l'on s'en tient, pour l'instant, à la qualification du procédé de signature, force est déjà d'observer deux importantes différences entre la signature manuscrite et la signature électronique. Premièrement, la signature manuscrite réserve normalement peu de surprise : pourvu qu'elle consiste en la marque habituelle du signataire et qu'elle soit tracée au bon endroit, sa validité est assurée. La signature électronique est nettement plus imprévisible. À défaut d'une signature électronique qualifiée, l'on a vu qu'en cas de contestation, il revenait au juge d'apprécier l'aptitude du procédé à établir l'imputabilité et le maintien de l'intégrité. La marge de manœuvre laissée au juge entraîne une insécurité juridique, qui est pratiquement négligeable en présence d'une signature traditionnelle. On peut s'en plaindre. Toujours est-il que cette incertitude est consubstantielle à la doctrine des équivalents fonctionnels[62]. Celle-ci enseigne l'équivalence entre la signature électronique et la signature manuscrite, à condition que la première remplisse les fonctions traditionnellement dévolues à la seconde. En vérité, tout sépare les deux formes de signature : au point de départ, pourrait-on dire, une signature électronique n'est précisément pas l'équivalent

[61] Si la signature est certifiée par un prestataire *accrédité*, le juge pourra se borner à constater cette accréditation (laquelle *suppose* le respect des exigences des annexes I, II et III de la loi du 9 juillet 2001). Si la signature est délivrée par une autorité de certification *non accréditée*, le respect des exigences énoncées dans les trois annexes de la loi devrait être démontré ; toutefois, en pratique, il est envisageable de limiter l'ampleur des vérifications à effectuer. En ce sens et pour une explication plus détaillée, voy. L. Lecocq et B. Vanbrabant, *op. cit.*, p. 119-121, n°s 106 et 107 ; M.E. Storme, *op. cit.*, p. 1519, n° 45 ; L. Guinotte, *op. cit.*, p. 558.

[62] L'autre solution était de créer un corps de règles spécifiques et extrêmement précises pour la preuve électronique. L'insécurité relative inhérente à l'approche fonctionnelle est, somme toute, le prix à payer pour la sauvegarde de l'unité du droit de la preuve.

d'une signature manuscrite... Le Code civil ne s'est jamais préoccupé de la fiabilité de la signature sur papier ni du procédé utilisé[63]. Or, ces questions deviennent essentielles en matière de signature électronique: il y a lieu de convaincre le juge que le mécanisme utilisé remplit effectivement les fonctions classiques de la signature. C'est ici qu'intervient la seconde grande différence: alors qu'en matière de signature manuscrite, le juge peut trancher seul et aisément la question de la qualification – simple question juridique –, il devra souvent faire appel à un expert pour apprécier la validité d'un procédé de signature électronique. Des différences analogues se marquent aussi sur le terrain de la vérification d'écritures (*infra*, n^os^ 13 et s.).

12. Les procédés *a priori* concernés par l'art. 1322, al. 2, C. civ. – Dans l'esprit du législateur, une diversité d'*ensemble[s] de données électroniques* devraient pouvoir satisfaire à l'exigence d'une signature[64]. D'autant qu'une liberté d'appréciation est laissée au juge quant au degré d'imputabilité et d'intégrité dont il se satisfait[65]. L'on songe aux procédés suivants: un simple e-mail (qui contiendrait, par exemple, des données très personnelles à son auteur apparent), un bon de commande complété et envoyé directement sur le web (avec indication d'un code d'identification « client » ou de diverses données telles que le nom, l'adresse géographique et électronique, un numéro de carte de crédit, etc.)[66], etc. On peut y ajouter la diversité des signatures numériques, que l'on aperçoit de plus en plus souvent, jointes à des messages échangés par le biais de l'internet. Plus ou moins fiables, ces signatures reposent sur l'utilisation de deux clés complémentaires, sans toutefois pouvoir être regardées comme des signatures électroniques « qualifiées ». L'article 1322, alinéa 2, devrait surtout permettre de rattraper des signatures numériques à double clé cryptographique qui, pour l'une ou l'autre

[63] Sauf rares exceptions (la griffe, les empreintes digitales, la signature à main guidée, etc.).

[64] Cf. l'exposé des motifs du premier projet preuve, *Doc. parl.*, Ch. repr., sess. ord. 1998-1999, 2141/1, spéc. p. 2 (« Le présent projet de loi fraye par contre un chemin à l'utilisation de signatures électroniques en général ») et p. 16 (« Actuellement, la technique la plus connue est celle de la signature digitale, basée sur la cryptographie. La description contenue dans l'article proposé ne se limite toutefois pas au procédé de la signature digitale afin de donner l'opportunité à de nouvelles techniques de se développer »).

[65] Ce pouvoir d'appréciation a souvent été confirmé au cours des travaux préparatoires, notamment par le ministre. Cf., par exemple, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, doc. 50 0038/008, p. 35.

[66] Cf. L. LECOCQ et B. VANBRABANT, *op. cit.*, pp. 117-118, n^os^ 102 et 103.

raison (clés non certifiées[67], absence de certificat qualifié, clés conçues au moyen d'un dispositif insuffisamment sécurisé de création de signature, etc.), ne peuvent bénéficier du régime de faveur institué par l'article 4, § 4, de la loi du 9 juillet 2001.

Profitant de la marge de manœuvre qui lui est reconnue, le juge pourrait se montrer plutôt accueillant – surtout dans un premier temps – en ce qui concerne ces divers modes d'identification, et ce, en dépit de leur fiabilité relative. Ainsi, il serait excessif de dénier toute force probante à l'écrit assorti d'une signature électronique ordinaire pour le seul motif qu'elle n'a pas été créée par un dispositif sécurisé[68]. Le juge pourrait reconnaître la qualité de signature à des mécanismes peu sécurisés, mais qui, à son estime, permettent d'établir avec une *fiabilité suffisante* (*supra*, n° 8) l'identité du signataire présumé et son adhésion au contenu de l'acte. Délicate sera toutefois l'évaluation de leur aptitude à établir le maintien de l'intégrité du contenu de l'acte. Pour peu qu'elle soit appréciée strictement, cette dernière condition devrait souvent s'avérer problématique au regard des signatures non « qualifiées ».

On peut le regretter, d'autant que cette exigence est discutable en son principe (*supra*, n° 10). Elle fait obstacle à la mise en place d'une politique juridique qui verrait d'un bon œil la cohabitation de plusieurs niveaux de sécurisation des signatures électroniques en fonction des usages qui en sont faits et des enjeux de l'opération contestée.

Toutefois, nous avons suggéré d'envisager le critère du maintien de l'intégrité, non comme une fonction de la signature, mais comme une condition de recevabilité de l'acte sous seing privé électronique. Remarquons, du reste, que le terme « établissant » utilisé à l'article 1322, alinéa 2, laisse au juge une plus grande marge d'appréciation (et est donc plus en conformité avec la directive) que si l'on avait opté pour le terme « garantit »[69].

[67] L'on songe notamment aux signatures numériques fondées sur PGP (*Pretty Good Privacy*). Téléchargeable gratuitement sur l'internet, ce programme permet à tout internaute de générer une paire de clés et de diffuser lui-même sa clé publique (chaque utilisateur dispose de toute une collection de clés publiques réunies dans un fichier appelé « trousseau de clés publiques »). PGP n'a pas techniquement besoin de l'intervention d'une autorité de certification pour être exploité. Cf. H. BITAN, « La signature électronique: comment la technique répond-elle aux exigences de la loi? », *Gaz. Pal.*, 2000, p. 1280.

[68] Entendez: qui satisfait aux exigences de l'annexe 3 de la loi du 9 juillet 2001.

[69] En ce sens, voy. les observations formulées par le service juridique de la Chambre au sujet de l'amendement n° 12, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, doc. 50 0038/008, p. 33.

Chapitre V
DÉNÉGATION DE SIGNATURE ET VÉRIFICATION D'ÉCRITURES

13. Controverse. – Sans contester la validité du mécanisme de signature électronique, le défendeur peut-il encore affirmer ne pas avoir signé ? La question est vivement controversée en doctrine.

L'hésitation ne porte pas sur les signatures visées par l'article 1322, alinéa 2, du Code civil. L'auteur présumé d'une signature électronique non qualifiée a le loisir de dénier sa signature, obligeant ainsi le demandeur à recourir éventuellement à une vérification d'écritures [70]. Cette solution – indiscutable et indiscutée – ressort explicitement des travaux préparatoires relatifs à l'article 1322, alinéa 2, du Code civil [71]. Selon une opinion, « cette vérification d'écritures *se confondra* le plus souvent avec l'opération consistant à vérifier l'imputabilité de l'acte. En vidant, éventuellement au terme d'une expertise, la question si le message qui lui est soumis est bien imputable à l'une des parties au procès, le juge aura *ipso facto* procédé à une vérification d'écritures » [72]. Selon une autre opinion, la question de la validité de la signature doit se résoudre *in abstracto* (le procédé présenté est-il suffisamment fiable pour permettre d'identifier telle personne ?), tandis que la vérification d'écriture à proprement parler suppose une vérification *in concreto* (dans le cas d'espèce, est-ce bien le prétendu signataire qui a utilisé le procédé ?) [73]. Dans cette optique, l'on peut penser qu'avec le temps et l'expérience – et la constitution progressive d'un *corpus* jurisprudentiel –, le juge pourra trancher (parfois ? souvent ?) la question de la validité sans expertise, auquel cas la vérification d'écritures retrouvera un intérêt spécifique.

[1] Sur cette procédure, P. ROUARD, *Traité élémentaire de droit judiciaire privé*, t. IV, Bruxelles, Bruylant, 1980, pp. 37 et s., n^os^ 33 et s. Voy. aussi A. FETTWEIS, *Manuel de procédure civile*, 2^e^ éd., Faculté de droit de Liège, 1987, p. 362, n° 485.

[1] Cf. justification de l'amendement n° 12 (du gouvernement) à la proposition de loi introduisant de nouveaux moyens de télécommunication dans la procédure judiciaire et extrajudiciaire (13 juin 2000), *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 0038/006, p. 12. Voy. aussi le rapport fait au nom de la commission de la Justice par Bart SOMERS (30 juin 2000), *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 0038/008, p. 33. Voy. aussi l'avis du Conseil d'État sur le premier projet preuve : *Doc. parl.*, Ch. repr., sess. ord. 1998-1999, 2141/1, p. 28 : « Leur intention [des auteurs du projet] semble bien être, conformément à l'équivalence dont il vient d'être question ci-dessus, de ne conférer de force probante à l'acte envisagé que si l'auteur accepte d'y reconnaître sa marque, ainsi qu'il est dit à l'alinéa 1^er^ de l'article 1322. »

[2] P. LECOCQ et B. VANBRABANT, *op. cit.*, p. 116, n° 100.

[3] D. MOUGENOT, *La preuve*, *op. cit.*, p. 225, n° 158-1.

Vivement discutée est, par contre, la possibilité de dénier une signature électronique qualifiée. Étant donné la haute fiabilité de pareille signature – et, partant, la diminution des risques de fraude –, une partie de la doctrine se demande s'il est opportun de laisser au signataire la possibilité d'un désaveu [74]. Selon certains, l'organisation d'un partage des risques viendrait d'ores et déjà se substituer aux possibilités de dénégation de signature au sens des articles 1323 et 1324 du Code civil [75]. Pratiquement, plusieurs auteurs considèrent *de lege lata* que, sauf hypothèse marginale (voy. ci-après), une signature électronique qualifiée ne peut être déniée tant que le titulaire du certificat n'a pas demandé la révocation de celui-ci. Il est donc lié par l'acte signé au moyen de sa clé privée, quitte à se retourner contre l'usurpateur [76].

Dans l'hypothèse d'une « fausse paire de clés » et d'un faux certificat [77], il existerait même une présomption de signature (*i.e.* le certificat ferait foi jusqu'à preuve du contraire). La personne qui soutient que la clé privée utilisée pour signer le document n'est pas la sienne ne pourrait se borner à dénier sa signature. C'est à elle qu'il appartiendrait de demander une vérification d'écriture suivant la procédure fixée par les articles 883 et suivants du Code judiciaire. Telle serait d'ailleurs la seule hypothèse dans laquelle une vérification d'écritures *stricto sensu* pourrait trouver place [78].

Cette présentation nous paraît en contradiction avec les choix fondamentaux qui ont présidé à la réforme du droit de la preuve.

14. Dans la logique des prémisses de la réforme. – Nous sommes d'avis que l'auteur présumé d'une signature électronique – quel que soit le procédé utilisé – peut dénier son écriture et obliger le demandeur à recourir éventuellement à une procédure de vérification d'écritures. Au demeurant,

[4] Voy., parmi d'autres, L. GUINOTTE, *op. cit.*, p. 558.

[5] E. ROGER FRANCE et E. DE GROOTE, *op. cit.*, p. 200, n° 50 ; M. E. STORME, *op. cit.*, p. 1519, n° 46, *initio* ; J. DUMORTIER et S. VAN DEN EYNDE, *op. cit.*, p. 193 et note 44 ; J. STEENLANT, article précité.

[6] *Ibid.* Le désaveu ne serait pas possible au motif que l'acte a effectivement été signé à l'aide de sa clé privée. Autrement dit, il ne pourrait contester avoir signé puisque sa clé privée a été mise en œuvre. Cette argumentation discutable (exposée notamment par J. STEENLANT, article précité) procède d'une vision éminemment statique de la signature, qui ignore la dimension psychologique de l'acte de signer. Que reste-t-il de l'*animus signandi* ? À notre sens, signer, c'est, ici, mettre en œuvre sa clé privée... en vue de s'identifier et de marquer son consentement au contenu de la convention.

[7] Quelqu'un se fait passer pour un autre et, au nom de cette autre personne, obtient un certificat et signe un acte juridique avec une troisième personne.

[8] M. E. STORME, *op. cit.*, p. 1519, n° 46, 1°, qui semble approuvé par J. STEENLANT (article précité) et par E. ROGER FRANCE et E. DE GROOTE, *op. cit.*, p. 200, n° 50.

l'article 4, § 4, *initio*, de la loi du 9 juillet 2001 réserve expressément la possibilité de désavouer une signature électronique qualifiée.

La solution contraire signifierait un alignement du régime probatoire de l'acte sous seing privé électronique sur celui de l'acte authentique traditionnel. Pareille interprétation bouleverserait le droit de la preuve – perspective que les promoteurs de la réforme n'ont précisément pas voulue [79] ! – et serait en contradiction flagrante avec la philosophie qui est à la base de la réforme [80]. En effet, contrairement à ce qui a toujours été proclamé [81], il n'y aurait donc pas *équivalence* entre la signature électronique et la signature manuscrite, mais *supériorité* de la première sur la seconde ! Pour le dire encore autrement, il n'y aurait pas assimilation [82] de l'acte sous seing privé électronique à l'acte sous seing privé traditionnel (sur support papier), mais *supériorité* du premier sur le second [83].

L'interprétation dénoncée perd de vue, selon nous, l'alinéa 1er de l'article 1322. La (re)lecture de H. De Page est, à cet égard, des plus utiles [84]. La différence fondamentale entre l'acte sous seing privé et l'acte authentique réside en ce que le premier est dépourvu de toute force probante quant à son origine – il ne prouve rien, il ne constitue pas une preuve – *tant qu'il n'est pas reconnu ou légalement tenu pour tel* (art. 1322, al. 1er) [85]. Celui auquel on oppose un acte sous seing privé peut donc toujours se borner à désavouer son écriture ou sa signature (art. 1323 C. civ.), ou, si l'acte émane d'un de ses auteurs, à déclarer qu'il ne connaît pas la signature. En toute hypothèse, une dénégation pure et simple suffit pour qu'aucune foi ne s'attache à un acte sous seing privé. Il incombe alors à celui qui invoque l'acte d'en rétablir la force probante en prouvant l'authenticité de la signature, au besoin par le recours à une demande en vérification d'écritures [86] [87]. L'acte authentique, au contraire, ne doit pas être reconnu : parce qu'il a fait l'objet de constatations par un officier public, il jouit d'emblée d'une force probante provisoire (l'origine de l'écriture est susceptible de preuve contraire, mais par la seule voie de l'inscription de faux).

Pour le reste, les deux types d'actes sont pratiquement sur le même pied. L'acte sous seing privé reconnu (ou tenu pour tel) « a la même foi » que l'acte authentique (art. 1322, al. 1er) : ils prouvent, dans la même mesure, la sincérité du *negotium* constaté ; ils sont l'un et l'autre susceptibles de preuve contraire. La seule différence réside dans le *mode d'administration* de cette preuve. Dans l'acte authentique, les mentions couvertes par l'authenticité (*i.e.*, outre l'origine des écritures, toutes les constatations faites par l'officier public *ex propriis sensibus*) ne peuvent être contredites, par une partie ou un tiers, que par le biais de la procédure d'inscription de faux. Sous cette réserve, la sincérité des déclarations des parties, dans les deux types d'actes, peut être combattue par tous les moyens légaux, à savoir, *inter partes*, dans le respect de l'article 1341 du Code civil, et par les tiers, par toutes voies de droit (y compris par témoignages et présomptions) [88].

En substance, l'acte sous seing privé est, en soi, dépourvu de toute force probante ; il n'acquiert force probante – qui est alors égale à celle conférée par la loi à l'acte authentique – *que s'il est reconnu ou doit être légalement tenu pour tel*. Par conséquent, il suffit donc à celui à qui on oppose un acte sous seing privé de dénier son écriture ou sa signature pour imposer à celui qui s'en prévaut de demander, le cas échéant, une vérification d'écriture. La solution est inverse en matière d'acte authentique qui fait foi par lui-même de l'écriture de celui dont il émane, et a, dès lors, force probante jusqu'au moment où la preuve de sa fausseté éventuelle est acquise.

[79] Cf. l'exposé des motifs du premier projet preuve, *Doc. parl.*, Ch. repr., sess. ord. 1998-1999, 2141/1, spéc. p. 1 (« sans cependant réformer fondamentalement les principes essentiels de notre droit de la preuve ») et p. 14 (« il convient de repenser nos règles juridiques en matière probatoire de façon à ce que, tout en maintenant l'équilibre des intérêts qu'elles entendaient assurer, elles ne constituent pas un obstacle au développement des nouvelles technologies »).

[80] Cf. *ibid.*, spéc. pp. 14-15 : « Tout en maintenant le principe de la légalité des preuves et la prééminence de l'écrit consacrée à l'article 1341 du Code civil, il convient plutôt, par une analyse fonctionnelle des concepts d'écrit, de signature et d'original, de repenser les règles existantes de façon à les ouvrir aux moyens de preuve issus des nouvelles technologies de l'information. »

[81] Voy. encore, par exemple, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, doc. 50 0038/006, p. 2.

[82] Nonobstant la terminologie employée à l'art. 4, § 4, de la loi du 9 juillet 2001.

[83] Rappr., *mutatis mutandis*, J. Devèze, *op. cit.*, p. 541.

[84] H. De Page, *Traité élémentaire de droit civil belge*, t. III, Bruxelles, Bruylant, 1967, pp. 749 et s., nos 739 et s., *passim* et spéc. no 747.

[85] L'on sait que cette reconnaissance ne doit pas être expresse : elle résulte généralement de l'absence de dénégation formelle de sa part, soit de son silence lorsque l'acte est produit en justice.

[86] Dans l'ancien droit, la procédure de vérification d'écritures était même obligatoire préalablement à toute action en justice sur la base de l'acte. Depuis le Code civil, cette procédure ne s'impose que si l'acte est dénié.

[87] En jurisprudence, voy., par exemple, Comm. Hasselt, 14 octobre 1997, *R.W.*, 1997-1998, p. 1271 ; Civ. Louvain, 20 mai 1992, *Pas.*, 1992, III, p. 78 ; Civ. Charleroi (1re ch.), 5 mars 1991, *J.T.*, p. 819.

[88] Pour davantage de précisions (notamment quant à la date des actes), H. De Page, *op. cit.*, spéc. no 747. Voy. aussi, N. Verheyden-Jeanmart, *op. cit.*, p. 271 et s., nos 574 et s. ; D. Mougenot, *La preuve*, *op. cit.*, pp. 221-222, no 153.

Bref, étant donné la volonté affichée de sauvegarder l'équilibre du droit de la preuve et dans la logique de la théorie des équivalents fonctionnels, force est d'admettre qu'en matière d'acte sous seing privé, une signature électronique doit pouvoir être désavouée, en toute hypothèse[89], par le signataire apparent, auquel cas il appartient à celui qui invoque l'acte de demander que le juge procède à une vérification d'écritures conformément à la procédure prévue aux articles 883 et suivants du Code judiciaire.

15. Des dénégations abusives sont-elles à craindre ? – Ces conclusions ruinent-elles le régime de faveur institué au bénéfice de la signature électronique qualifiée ? Sont-elles de nature à compromettre l'essor de la signature et du commerce électroniques ? Doit-on redouter des dénégations abusives (pour se libérer des liens d'un contrat...), ainsi qu'une multiplication des procédures en vérification d'écritures ? Nous ne le pensons pas.

Il est permis de s'en remettre à la sagesse du juge. Celui-ci dispose, en effet, d'un large pouvoir d'appréciation à l'heure de statuer sur l'authenticité d'un écrit désavoué par la personne à laquelle il est opposé. Il décide librement s'il est nécessaire de recourir à la vérification d'écritures pour trancher, et il peut s'en passer lorsque les éléments de fait produits et leur valeur probante lui semblent suffisamment sûrs[90]. En tout état de cause, s'il décide de procéder à la vérification d'écritures, il n'est pas tenu d'ordonner une expertise[91]. Aux termes de l'article 889 du Code judiciaire, il peut ordonner toutes les mesures d'instruction opportunes pour l'établissement de sa conviction. La preuve de l'authenticité de l'écrit signé peut être administrée par n'importe quel moyen : titres, témoignages, interrogatoires sur faits, etc.[92]. Par exemple, des témoins peuvent attester l'absence du signataire au moment où l'acte a été établi...

Aussi, sur le plan pratique, convient-il de nuancer la portée du principe suivant lequel celui qui invoque l'acte supporte la charge de la preuve. Il serait effectivement choquant que le titulaire du certificat qualifié puisse se borner à dénier sa signature, tandis que tout le fardeau de la preuve pèse-

[89] Y compris dans l'hypothèse évoquée plus haut des fausses clés et du faux certificat. Qu'est-ce à dire d'ailleurs qu'il existerait, en ce cas, une présomption de signature ? Qu'il appartiendrait au signataire présumé qui la conteste de recourir à l'inscription de faux (et non de solliciter une vérification d'écritures) ? Pareille interprétation bouleverserait le droit commun de la preuve.

[90] Cass. (1re ch.), 7 mars 2002, *Larcier cass.*, 2002, n° 1264 (somm.).

[91] Cass. (1re ch.), 25 octobre 1991, R.G. 7328.

[92] Cf. Liège (11e ch.), 8 février 1999, *Rev. trim. dr. fam.*, 2001, p. 773.

rait sur les seules épaules du demandeur[93]. En réalité, dans la recherche et l'administration des preuves, le juge joue un rôle actif et dispose d'un pouvoir d'initiative étendu[94]. Ainsi peut-il inviter toutes les parties à collaborer activement à l'administration des preuves.

Faut-il le redire, au civil, prouver c'est établir une vraisemblance suffisante pour convaincre le juge qui reviendra alors vers l'autre partie pour lui offrir de faire apparaître une vraisemblance de signe contraire (*supra*, n° 8)[95]. Or, *a priori*, la signature électronique qualifiée, paraît émaner du prétendu signataire. Tout porte donc à penser qu'en pratique, ce dernier tentera d'apporter spontanément des éléments de preuve de nature à étayer ses dires car il sait qu'il est plus habile d'empêcher une conviction de se former que de renverser une conviction qui a pris corps. Aussi s'efforce-t-il d'invoquer avec sérieux, preuves à l'appui, un dysfonctionnement du système ou une collusion entre son adversaire et le prestataire de service de certification ou encore de démontrer l'invraisemblance de sa signature (à l'aide de témoins attestant son absence au moment où l'acte a été établi, par exemple). S'il parvient à faire naître un doute dans l'esprit du juge, celui-ci pourra encore ordonner, comme on l'a vu, diverses mesures d'instruction... et ce n'est que si, *in fine*, demeure un doute irréductible sur l'imputabilité de la signature à celui qui l'a déniée que l'acte sous seing privé sera écarté des débats comme le serait un acte sur support papier. En ce sens, l'affirmation suivant laquelle la partie qui invoque l'acte supporte la *charge* de la preuve signifie, non pas tellement que l'*administration* des preuves incombe à elle seule, mais plutôt qu'elle supporte, au final, le *risque* de la preuve, entendant par là le risque de la perte du procès lorsque le juge se heurte à un doute persistant[96].

L'ensemble de ces considérations nous inclinent à minimiser les risques de dénégations abusives. Encore faut-il ajouter que, bien souvent, le signa-

[93] Spéculant ainsi sur le parti à tirer du risque technoscientifique que le demandeur aurait à supporter.

[94] Loin de devoir de contenter des preuves offertes, il a le pouvoir – et le devoir – d'ordonner toutes les mesures d'instruction utiles : expertise, enquête, production de documents, même détenus par des tiers (l'on songe ici à l'autorité de certification). Il peut aussi appuyer sa décision sur des « données d'expérience commune ». À cet égard, voy. notamment D. MOUGENOT, *La preuve*, *op. cit.*, p. 72 ; E. KRINGS, « L'office du juge : évolution, révolution ou tradition », *J.T.*, 1993, pp. 17 et s.

[95] D. MOUGENOT, *La preuve*, *op. cit.*, p. 81, n° 17 ; N. VERHEYDEN-JEANMART, *op. cit.*, n° 66. Voy. aussi D. AMMAR, « Preuve et vraisemblance – Contribution à l'étude de la preuve technologique », *Rev. trim. dr. civ.*, 1993, p. 499.

[96] Voy., *ad generalia*, D. MOUGENOT, *La preuve*, *op. cit.*, p. 93, n° 27 ; N. VERHEYDEN-JEANMART, *op. cit.*, n° 69.

taire ne retirera aucun bénéfice de sa dénégation de signature (électronique qualifiée) étant donné que, par l'effet des règles de responsabilité, il sera néanmoins tenu d'assumer les conséquences de l'acte juridique qu'il prétend ne pas avoir signé.

16. Le réflexe de la responsabilité sur l'efficacité du désaveu de signature. – Au cas où une signature électronique qualifiée a été déniée avec succès, la partie qui invoque l'acte – dont elle ne parvient pas à établir l'existence – devrait être déboutée de sa demande. En principe... car tout n'est pas nécessairement perdu pour le demandeur... Le débat pourra se déplacer sur le terrain des responsabilités et venir tempérer, voire gommer, l'effet du désaveu.

C'est ici qu'apparaît une autre différence – de taille ! – entre la signature manuscrite et la signature électronique. Jusqu'ici, le seul risque de fraude était l'imitation de signature : or, on voit mal comment on aurait pu reprocher une faute dans le chef du prétendu signataire et le tenir pour responsable des conséquences de la fraude.

En matière de signature numérique, la fraude la plus vraisemblable est l'hypothèse de l'usurpation de clé privée. Dans une telle hypothèse, une négligence du signataire apparent n'est pas à exclure dès lors qu'il est logiquement tenu de préserver la confidentialité de sa clé privée. Dans ce cas, si le désaveu de signature conduit à écarter des débats l'acte invoqué, le demandeur peut encore chercher à mettre en cause la responsabilité du signataire.

Si l'on a affaire à une signature électronique ordinaire (visée par l'article 1322, alinéa 2, du Code civil), c'est le droit commun de la responsabilité aquilienne qui trouvera à s'appliquer [97]. En particulier, il faudra démontrer l'existence d'une faute dans le chef du signataire apparent. À cet égard, la jurisprudence aura à définir les obligations de prudence incombant au titulaire de clés cryptographiques pour assurer la confidentialité de sa clé privée [98]. En l'absence de faute, encore pourra-t-on songer

[97] Il n'y a pas lieu de se référer à la loi du 9 juillet 2001 (notamment à son article 19). Cette loi ne traite des questions relatives à la responsabilité qu'à propos des certificats émis par des PSC qui délivrent au public des certificats présentés comme qualifiés ou qui garantissent publiquement de tels certificats ; pour les prestataires qui délivrent des certificats ordinaires (qui ne sont pas présentés comme qualifiés), le droit commun de la responsabilité trouve à s'expliquer. Cf. *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, doc. 50 0322/001, p. 36. *A fortiori*, dans les cas où il est fait usage de clés non certifiées.

[98] Sans doute les exigences formulées évolueront-elles à mesure que les techniques se perfectionnent et se répandent. Ainsi le juge pourrait-il ériger en faute le fait d'avoir enregistré

à faire application de la théorie du mandat apparent pour fonder l'obligation du signataire apparent d'exécuter la convention qu'il n'a pas signée. Il sera souvent difficile de nier que le soi-disant mandant a contribué – fût-ce de manière non fautive – à la création de l'apparence [99].

Si l'on a affaire à une signature électronique qualifiée, il y a lieu de se référer à l'article 19 de la loi du 9 juillet 2001. À notre sens, même si l'acte a été signé par l'usurpateur de la clé privée avant que le titulaire du certificat ne demande la révocation de ce dernier, une dénégation de signature reste possible. Si ce débat n'est pas à exclure, il est vrai néanmoins qu'il est susceptible de se prolonger sur le terrain de la responsabilité.

À défaut d'avoir demandé la révocation du certificat et *pourvu qu'une faute puisse concrètement lui être reprochée* [100], le signataire apparent est responsable du préjudice occasionné au cocontractant de l'usurpateur. Ainsi pourra-t-il être tenu de réparer, sur un fondement aquilien, le dommage résultant de la non-conclusion du contrat. Gageons que, le plus souvent, une telle faute pourra être retenue dans son chef. *Quid* s'il a demandé la révocation du certificat, avec une extrême célérité, dès la découverte du vol du support de la clé privée [101], mais que le voleur a fait usage de la clé volée dans l'intervalle de temps ? Dans ce cas, sa responsabilité pourrait théoriquement ne pas être retenue. Encore la théorie du *mandat apparent* pourrait-elle trouver à s'appliquer ici aussi avec les conséquences que l'on sait.

sa clé privée sur le disque dur d'un ordinateur, au lieu d'une carte à puce protégée par un code secret, ou d'avoir laissé traîner la carte... et le code secret, ou demain, le fait de ne pas lui avoir associé un système de reconnaissance biométrique.

[99] Sur les conditions d'application de la théorie de l'apparence, voy., parmi d'autres, P. Wéry, *Le mandat*, Tiré à part du *Répertoire notarial*, Bruxelles, Larcier, 2000, pp. 246-250 ; S. Stijns, D. Van Gerven et P. Wéry, « Chronique de jurisprudence. Les obligations : les sources (1985-1995) », *J.T.*, 1996, pp. 694-696, n^os^ 12 et s., et les réf. citées. Pour une discussion sur le statut de l'imputabilité de la situation apparente au comportement du mandant parmi les conditions de l'apparence comme source d'obligations, voy. la même chronique, spéc. n° 13 et les réf. citées.

[100] D'après l'exposé des motifs, l'on aurait affaire à une responsabilité à base de faute : « Différentes obligations pèsent sur le titulaire du certificat. Sa responsabilité pourrait être engagée en cas de manquement à une des obligations qui lui sont imposées par ou en vertu de la présente loi et notamment [...] ». Cf. *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, doc. 50 0322/001, p. 40. Les termes de l'article 19, § 1^er^, de la loi du 9 juillet 2001 ne nous semblent pas déterminants pour avaliser la thèse d'une responsabilité sans faute. En ce sens, D. Mougenot, *La preuve*, *op. cit.*, p. 227 ; D. Gobert, « Cadre juridique... », *op. cit.*, p. 154 ; L. Lecocq et B. Vanbrabant, *op. cit.*, p. 125, n° 112.

[101] Soit dès qu'a pu s'insinuer dans son esprit un doute quant au maintien de la confidentialité de sa clé privée (cf. les termes de l'art. 19, § 2, de la loi).

Si le signataire apparent a demandé la révocation du certificat à temps (*i.e.* avant utilisation de la clé privée usurpée), il ne pourra être tenu pour responsable à l'égard du cocontractant malheureux. Si ce dernier a omis de consulter le registre électronique, il devra supporter les conséquences de sa négligence [102]. À moins qu'il ait diligemment consulté le registre électronique, mais que la révocation n'y a pas été enregistrée par le prestataire de service de certification : en pareil cas, le cocontractant pourra mettre en cause la responsabilité du prestataire [103].

Parmi les situations envisageables (et habituellement envisagées), il nous reste à évoquer, d'une part, celle des fausses clés et faux certificat obtenus et utilisés au nom d'un autre, d'autre part, celle d'un déchiffrement frauduleux à partir de la clé publique qui lui est complémentaire.

Il est encore heureux, dans ces deux hypothèses, que le signataire présumé puisse dénier sa signataire, comme nous le préconisons. En outre, on voit mal qu'il puisse engager sa responsabilité aquilienne sur la base d'une faute prouvée. Il ne devrait pas davantage être tenu d'exécuter la convention sur le fondement de la théorie du mandat apparent qui pourra être écartée assez facilement, à défaut d'imputabilité de l'apparence au soi-disant signataire.

Dans la première situation évoquée, on ne voit pas pourquoi la vérification d'écritures serait « pratiquement impossible et donc absurde » [104]. À la demande du juge, le PSC devrait pouvoir prouver qu'il a effectivement vérifié l'identité du signataire apparent à l'heure de délivrer un certificat à son nom. En l'espèce, le problème se situant clairement au niveau de l'enregistrement, le PSC échouera dans cette preuve, auquel cas on aura pu « vérifier » qu'il ne s'agissait pas de la clé (ni de la signature) du signataire présumé. Le prestataire devra dès lors indemniser le cocontractant victime du dommage subi en raison de la non-conclusion du contrat et réparer aussi le dommage éventuellement subi par le signataire apparent. Si la fonction d'enregistrement avait été déléguée à un tiers, le PSC disposera ensuite d'un recours en responsabilité contre ce tiers [105].

[102] Cf. L. 9 juillet 2001, art. 13, § 2, al. 2.

[103] Cf. L. 9 juillet 2001, art. 12 à 14, spéc. art. 14, § 2. Pour d'autres hypothèses marginales, voy. notre étude « Définition... », *op. cit.*, p. 78.

[104] M. Stormé, *op. cit.*, p. 1519, n° 46, 2°.

[105] Le prestataire de service de certification n'est pas tenu d'assurer seul toutes les étapes du processus de certification. Il peut se référer, pour la collecte des informations, aux renseignements détenus par des autorités d'enregistrement. Toutefois, il répond, à l'égard des utilisateurs des certificats, du dommage qui est la conséquence des obligations qui lui sont imposées par ou en vertu de la loi. Cf. *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, doc. 50 0322/001, p. 21 et p. 28.

En ce qui concerne la seconde situation, l'on sait que ce genre d'opération est *pratiquement* impossible à réaliser dans un temps et avec des moyens raisonnables. En principe, pour avoir une chance de casser une clé de chiffrement, il est nécessaire de mobiliser des centaines d'ordinateurs interconnectés, ce qui est peu concevable à moins d'un enjeu de taille. Aussi, s'appuyant sur un expert, le juge pourra-t-il apprécier la *vraisemblance* de l'allégation du signataire apparent moyennant une mise en balance des ressources (matérielles, humaines, financières) nécessaires pour briser la clé avec les intérêts en jeu. Il pourra aussi renforcer sa conviction par d'autres biais : témoignages et pièces attestant l'absence du signataire apparent au moment où la convention litigieuse a été signée. En outre, ce dernier devrait pouvoir se dégager de toute responsabilité en cas de déchiffrement de sa clé privée par cryptanalyse, sans faute de sa part [106]. Nous sommes favorables à cette solution, en l'absence de texte légal clair prévoyant une responsabilité fondée sur le risque. Un auteur estime que le signataire apparent aura du mal à dégager sa responsabilité étant donné l'invraisemblance de l'hypothèse [107]...

Conclusion

17. Une cohérence imparfaite. – Il existe naturellement des différences entre la signature manuscrite et la signature électronique. Nous en avons épinglé certaines au passage. Au demeurant, si rien ne distinguait les deux formes de signature, proclamer leur équivalence n'aurait eu aucun sens. En particulier, la validité d'une signature électronique est plus aléatoire que celle d'une signature manuscrite car une discussion peut toujours s'élever à propos du procédé utilisé et de sa fiabilité, entendant par là son aptitude à remplir les fonctions attendues. Autant de préoccupations relativement inédites.

L'on sait que l'article 1322, alinéa 2, du Code civil s'inspire de la théorie des équivalents fonctionnels. L'intérêt de cette approche est de faire

[106] En ce sens, D. Gobert, « Cadre juridique... », *op. cit.*, p. 154 ; L. Lecocq et B. Vanbrabant, *op. cit.*, n° 114. *Contra* : M.E. Stormé, *op. cit.*, n° 46 ; E. Roger France et E. De Groote, *op. cit.*, n° 50 : ces auteurs estiment que le titulaire du certificat est responsable, même sans faute de sa part, tant qu'il n'a pas fait révoquer son certificat.

[107] D. Mougenot, *La preuve*, *op. cit.*, p. 227. Remarquons néanmoins que la question de la responsabilité ne se présente précisément que si le juge a estimé l'hypothèse vraisemblable et écarté l'acte sous seing privé électronique des débats.

l'économie de règles spécifiques – techniques et tatillonnes [108] – pour encadrer les mécanismes de signature électronique, et, partant, de préserver l'unité du droit de la preuve. Le prix à payer est la nécessité de convaincre le juge que telle signature électronique – contestée – émane effectivement de telle personne. L'exercice peut s'avérer embarrassant tant pour les parties que pour les juges appelés à vérifier si les fonctions de la signature sont satisfaites. À cet égard, l'attitude qui sera adoptée par ces derniers représente une grande inconnue. Se montreront-ils cléments ou rigoureux dans l'appréciation des conditions posées par la loi ? Il faut espérer l'élaboration de critères sûrs et une certaine unité de la jurisprudence. À défaut, grand est le risque de retomber dans les incertitudes liées à un régime de liberté des preuves que l'on a précisément répudié [109].

Il n'apparaît pas évident de satisfaire pleinement à la théorie des équivalents fonctionnels, en allant jusqu'au bout de la logique qui la sous-tend. En témoigne, à divers égards, le texte même de l'article 1322, alinéa 2.

D'abord, la logique suggérait, nous semble-t-il, de privilégier une définition fonctionnelle de la signature « tout court », au lieu de se borner à fixer les fonctions attendues de la seule signature électronique, dès lors que le postulat de départ est l'unité de la notion de signature. Ensuite, on ne retrouve clairement et distinctement énoncée, dans la définition fonctionnelle, aucune des deux fonctions traditionnellement dévolues à la signature – l'identification de l'auteur et la manifestation de son adhésion au contenu de l'acte –, ce qui est pour le moins paradoxal. Enfin, l'on y trouve énoncée, en revanche, une fonction nouvelle : le maintien de l'intégrité du contenu de l'acte. En tant qu'elle est assignée à toute forme de signature électronique, cette exigence paraît discutable et est de nature à reléguer dans un néant juridique nombre de procédés de signature électronique.

18. Jusqu'au bout de la logique fonctionnaliste. – En tâchant toujours de jouer – jusqu'au bout – le jeu de l'équivalence fonctionnelle, on est conduit à considérer que, si les conditions sont réunies aux yeux du juge (ou non contestées), la signature électronique ordinaire a la même force probante que la signature manuscrite. De ce point de vue, elle ne se distingue pas de la signature électronique qualifiée.

[108] Pas tout à fait puisque le législateur belge a finalement choisi de cumuler les deux approches dans deux textes distincts (*supra*, n° 3).

[109] Cf. D. MOUGENOT, *La preuve*, *op. cit.*, p. 195 et la référence à F. GONTHIER, « Réflexion sur la notion d'écrit », *J.C.P.*, éd. not., 1999, pp. 1781 et s.

Dans la même logique, nous pensons que toute signature électronique – fût-elle qualifiée – doit pouvoir être déniée purement et simplement par son auteur apparent, auquel cas il incombe à celui qui invoque l'acte de demander une vérification d'écritures. Celle-ci consiste, comme l'on sait, à vérifier si l'acte sous seing privé a été réellement écrit et signé par la personne à qui on l'oppose. Contrairement à ce qui a parfois été suggéré, cette procédure ne nous apparaît pas si inadaptée à la matière (même si elle sera menée différemment que par le passé). Il s'agit, ici aussi, de « vérifier » si l'acte (électronique, en l'occurrence) émane bien du signataire apparent. Cela semble *a priori* possible pourvu que l'on partage notre interprétation souple des articles 883 à 894 du Code judiciaire et des règles relatives à l'*administration* des preuves (*supra*, n° 15). Il reste que celui qui invoque l'acte supporte, *in fine*, le *risque* de la preuve. Oui... et cette solution n'a rien de choquant : si un doute très sérieux persiste dans l'esprit du juge à propos de la sincérité de la signature électronique (fût-elle qualifiée) de celui auquel on oppose l'acte – circonstance rarissime –, il nous paraît socialement équitable et juridiquement cohérent que le prétendu signataire ne soit pas lié par l'acte.

Encore doit-il pouvoir répondre, le cas échéant, des ruptures de confidentialité de sa clé privée. Ainsi, le débat relatif à l'imputabilité de l'écriture et de la signature à son auteur prétendu pourra se poursuivre sur le terrain de la responsabilité.

19. Un colosse aux pieds d'argile. – Toutes les signatures électroniques, en effet, ont leurs fragilités, comme la signature manuscrite, du reste. Aussi sophistiquées soient-elle, les signatures numériques fondées sur la cryptographie asymétrique et sur des infrastructures à clés publiques ont leurs points faibles, le principal étant le risque lié à la conservation de la clé secrète. Si le titulaire perd la maîtrise de sa clé privée et ne fait pas révoquer son certificat, il s'expose à voir engager sa responsabilité.

Apparaît ici une question inédite sous l'empire de la signature traditionnelle et qui confère une tournure nouvelle à la question du désaveu de signature.

Il convient néanmoins de distinguer soigneusement ces deux questions, qui se posent dans un ordre chronologique précis : la question de la dénégation de signature, toujours possible, est première ; si le désaveu est couronné de succès, se pose alors celle de la responsabilité éventuelle du titulaire. *De lege lata*, nous ne pensons pas que l'organisation, dans la loi du 9 juillet 2001, d'une répartition des responsabilités entre PSC et titulaires de certificat ait pour effet de priver qui que ce soit de la possibilité de

dénier sa signature. Ainsi, nous rejetons l'idée, parfois soutenue, selon laquelle le titulaire du certificat non révoqué ne serait pas admis à dénier sa signature en faisant valoir qu'un autre a usurpé et utilisé sa clé privée.

Nous pensons, par ailleurs, qu'il s'agit d'une responsabilité fondée sur la faute, dûment prouvée, du titulaire du certificat (à moins de pouvoir le condamner à exécuter la convention par application de la théorie du mandat apparent). Il ne nous paraît pas souhaitable, pour l'heure, de retenir la responsabilité aquilienne du titulaire du certificat lorsque la perte de maîtrise de sa clé privée est intervenue complètement à son insu et sans faute aucune de sa part (déchiffrement par cryptanalyse ; vol du support suivi d'une demande de révocation sans retard dès la prise de conscience du vol, etc.). Nous recommandons l'attentisme en cette matière. Avant d'instaurer une responsabilité sans faute, sous la forme d'un partage des risques, il faudrait être convaincu que le droit commun ne donne pas satisfaction. Il est trop tôt pour prendre attitude sur ce point.

Les signatures électroniques – et singulièrement la signature électronique qualifiée, que l'on pare de toutes les vertus – auront-elles le succès escompté, spécialement auprès du grand public ? Il faudrait que leur obtention et leur mise en œuvre ne soient ni trop lourdes, ni trop complexes, ni trop onéreuses. Et là-dessus, nous sommes titillé par quelque doute...