

La signature électronique au banc de la jurisprudence

par Etienne MONTERO
Professeur ordinaire aux FUNDP (Namur)
Doyen de la Faculté de droit

Ce fut – c’est – un honneur et un plaisir de collaborer avec le professeur L. Ballon dans le cadre du comité de rédaction du *D.A. O.R.* Qu’il veuille bien trouver dans ces quelques lignes l’expression de mon estime et de ma gratitude. Il y verra aussi un clin d’œil puisque c’est dans «sa» revue qu’a été accueillie ma première étude sur la signature électronique⁽¹⁾. Depuis lors, plus de dix années se sont écoulées et les premières contestations se sont élevées en justice.

Le corpus jurisprudentiel en formation révèle des pratiques *a priori* surprenantes. À mille lieues des élucubrations du législateur européen et de la doctrine sur les signatures électroniques dites «avancées» et «qualifiées», il apparaît que les acteurs de terrain se contentent souvent de mécanismes de signature plutôt frustes : signatures manuscrites scannées, combinaison d’identifiant et mot de passe ou de carte et code PIN, simples e-mails... Ainsi s’exposent-ils à des contestations mais, comme on le verra, ils ne s’en sortent pas nécessairement mal. C’est là une des leçons des décisions commentées ci-après : un procédé de signature électronique élémentaire, assorti de mesures de sécurité appropriées, peut parfois suffire, sans qu’il soit besoin de recourir à un procédé sophistiqué telle la mythique signature numérique à double clé cryptographique certifiée par un prestataire de service de certification.

I. Des signatures électroniques «ordinaires» contestées

On s’attendait à ce que surgissent un jour des contestations à propos de contrats d’en-

vergure passés et signés électroniquement entre entreprises privées, mais il n’en est rien jusqu’ici : les litiges portés en justice sont exceptionnels. Par contre, il était moins prévisible qu’un abondant contentieux de la signature électronique voit le jour dans le contexte de recours contre des décisions administratives de refus d’accès au territoire ou d’éloignement d’étrangers⁽²⁾.

Cette avalanche de recours s’explique par le fait que l’Office des étrangers a fait le choix de produire et de conserver les originaux de ses décisions uniquement sous forme électronique⁽³⁾. À cet effet, il a implémenté un système de signature électronique original, résultant de la numérisation de la signature manuscrite du fonctionnaire compétent. Le procédé est simple. La signature manuscrite du fonctionnaire est scannée pour obtenir une image numérique de celle-ci. Il suffit par la suite d’importer cette image dans le document élaboré à l’aide d’un logiciel de traitement de texte et contenant la décision relative à l’étranger. Cette dernière est ensuite notifiée à l’intéressé(e) sous forme de copie imprimée du document d’origine (revêtue d’une copie de la signature manuscrite scannée). Comme l’on sait, pareille décision est susceptible d’annulation en cas de non-respect de quelque forme substantielle. Du pain béni pour les plaideurs, ce procédé suspect de signature ! Ainsi s’est manifestement installée l’habitude de contester la validité de décisions de refus d’accès ou d’éloignement sur l’invariable grief qu’elles ne sont pas valablement signées. À de nombreuses reprises, le Conseil du contentieux des étrangers a été amené à se prononcer sur la valeur du système de signa-

(1) D. GOBERT et E. MONTERO, «La signature dans les contrats et les paiements électroniques : l’approche fonctionnelle», *D.A. O.R.*, n° 53, 2000, pp. 17-39.

(2) *Cf.* loi du 15 décembre 1980 sur l’accès au territoire, le séjour, l’établissement et l’éloignement des étrangers, *M.B.*, 31 décembre 1980, p. 14584.

(3) Pour d’autres commentaires sur ces premiers cas de jurisprudence, J. VANDENDRIESSCHE, «An overview of some recent case law in Belgium in relation to electronic signatures», *Digital Evidence and Electronic Law Review*, vol. 7, 2010, pp. 90-100.

ture électronique utilisé par l'Office des étrangers⁽⁴⁾. Il est vrai qu'un arrêt du Conseil d'État du 8 mai 2009 a estimé insuffisantes les preuves avancées par ledit Office pour convaincre de la fiabilité de la signature en question⁽⁵⁾ (A). Ayant entretemps fourbi ses armes, l'Office des étrangers a obtenu du Conseil du contentieux des étrangers une appréciation en sens contraire. Qu'il nous suffise de présenter l'arrêt du 19 novembre 2009⁽⁶⁾, dont la motivation est particulièrement fouillée et auquel se réfèrent régulièrement les arrêts ultérieurs⁽⁷⁾ (B).

A. Arrêt du Conseil d'État du 8 mai 2009

En l'espèce, un ressortissant russe s'est vu notifier une décision du ministre de l'Intérieur du 11 décembre 2003 de refus d'asile avec ordre de quitter le territoire. La décision est attaquée pour violation des formes substantielles et du principe général de bonne administration. Est alléguée, en l'occurrence, l'absence de signature manuscrite de la personne habilitée à prendre pareille décision. Cette dernière indique qu'elle a été prise par «N.L., conseiller adjoint/adjunctadviseur», mais ne comporte aucune signature originale. Seule une signature qui a manifestement été numérisée à l'aide d'un scanner figure sur la décision.

Or, soutient le requérant, la signature s'entend de la marque manuscrite par laquelle le signataire manifeste habituellement son identité aux tiers. Cette signature manuscrite garantit l'authenticité de la décision et l'identité de son auteur. Il s'agit là d'une composante essentielle sans laquelle la décision administrative ne peut être tenue pour valide. Il est donc question de la méconnaissance d'une forme substantielle. La signature litigieuse ne peut pas davantage être considérée comme une signature électronique au sens des articles 2, 1° (signature électronique «ordinaire»)⁽⁸⁾, et 2, 2° (signature électronique avancée)⁽⁹⁾, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification⁽¹⁰⁾. En effet, argue le requérant, peuvent être ainsi analysés comme signature, la signature numérique et d'autres mécanismes techniques aptes à garantir l'authenticité de données transmises par voie électronique. La signature, simplement copiée en l'espèce par le biais d'un scanner, ne répond pas à la définition de la signature électronique (ordinaire) et moins encore à celle de la signature électronique avancée. À cet égard, il est fait référence à une opinion exprimée en doctrine, à propos de la signature scannée⁽¹¹⁾. Une telle signature scannée, qui a pu être placée par n'importe qui, ne permet pas de vérifier l'identité du véritable auteur de la décision, ni la qualité de cette personne, de sorte qu'il n'est pas exclu qu'elle ait été appo-

(4) Les arrêts du Conseil du contentieux des étrangers/Raad voor Vreemdelingenbetwistingen sont disponibles à l'adresse <http://www.rvv-ccce.be>.

(5) Arrêt du Conseil d'État du 8 mai 2009, n° 193.106.

(6) Conseil contentieux étrangers, 19 novembre 2009, n° 34364. Pour des arrêts antérieurs à cette date, voy. Conseil contentieux étrangers, 17 février 2009, n° 23088 et Conseil contentieux étrangers, 13 mars 2009, n° 24496, et leur commentaire par J. VANDENDRIESSCHE, étude précitée. *Adde* : Conseil contentieux étrangers, 24 février 2009, n° 23535; Conseil contentieux étrangers, 3 avril 2009, n° 5604.

(7) Entre autres décisions, voy. Conseil contentieux étrangers, 17 décembre 2009, n° 36074; Conseil contentieux étrangers, 14 octobre 2010, n° 49536; Conseil contentieux étrangers, 14 octobre 2010, n° 49537; Conseil contentieux étrangers, 8 février 2011, n° 55673.

(8) On entend par «signature électronique» : «une donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification».

(9) On entend par «signature électronique avancée» : «une donnée électronique, jointe ou liée logiquement à d'autres données électroniques, servant de méthode d'authentification et satisfaisant aux exigences suivantes :

- a) être liée uniquement au signataire;
- b) permettre l'identification du signataire;
- c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif;
- d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée».

(10) *M.B.*, 29 septembre 2001, p. 33070.

(11) P. LECOCQ et B. VANBRABANT, «La preuve du contrat conclu par voie électronique», *Act. Dr.*, 2002/3, p. 256.

sée par un fonctionnaire non mandaté. Par conséquent, la décision administrative du 11 décembre 2003 est entachée d'une irrégularité formelle et est donc nulle.

En réponse à ces arguments, l'Office des étrangers fait valoir que la signature électronique assortissant la décision originale est conforme aux conditions de la loi, en renvoyant pèle mèle à la loi du 20 octobre 2000⁽¹²⁾, qui a ajouté un alinéa 2 à l'article 1322 du Code civil, et aux articles 4, §4, et 4, §5, ainsi qu'à l'annexe 3, de la loi du 9 juillet 2001. Le requérant rétorque qu'il résulte de l'article 2 de la loi du 9 juillet que la signature électronique est un ensemble de données électroniques attachées à un document électronique qui est envoyé par voie électronique, alors que la décision notifiée se présente sous la forme d'un document papier expédié par la poste. Aussi est-il dans l'impossibilité de vérifier l'identité de l'expéditeur et l'authenticité du contenu. Encore croit-il judiciaire de verser au dossier quelques références qui, en réalité, n'ajoutent rien à son analyse⁽¹³⁾.

Ces considérations révèlent une certaine mécompréhension du concept de signature électronique. Il reste qu'elles ont fait mouche auprès du Conseil d'État qui estime insuffisamment convaincante la démonstration du défendeur suivant laquelle l'apposition d'une signature scannée peut être considérée en l'espèce comme une signature (électronique). De façon plus étonnante, il note également que le caractère manuscrit est un élément constitutif d'une signature ordinaire valable de sorte qu'aucune valeur ne peut être accordée aux cachets, empreintes ou autres formes par lesquelles la signature n'est pas apposée à la main. Il conclut que la décision attaquée présente un vice de forme et doit être mise à néant.

Sans doute l'Office des étrangers s'est-il juré qu'on ne l'y prendrait plus car, entre-temps, sa démonstration s'est considérablement enrichie comme le révèle la décision du Conseil du contentieux des étrangers qui retient à présent l'attention.

B. Arrêt du Conseil du contentieux des étrangers du 19 novembre 2009

Les faits et les griefs sont du même ordre que ceux de l'affaire portée devant le Conseil d'État. À l'issue d'une première audience, il a été décidé de reporter la discussion du premier moyen, fondé sur l'arrêt du Conseil d'État du 8 mai 2009, afin de permettre à la partie défenderesse de produire une note exposant les garanties techniques qui entourent la signature assortissant la décision administrative critiquée. C'est ainsi qu'a été versée aux débats une note émanant du directeur général ICT du SPF Intérieur concernant «l'utilisation et le fonctionnement du système de signature scannée dans l'application Evibel»⁽¹⁴⁾.

La décision, soigneusement motivée, du Conseil du contentieux des étrangers est riche d'enseignements. L'on peut en retenir les éléments suivants, librement sélectionnés et complétés par des précisions et références de notre cru :

1° La loi du 9 juillet 2001 trouve à s'appliquer dans le secteur public⁽¹⁵⁾. Argument peut être tiré du libellé de l'article 4, §3, dont il résulte que «le Roi peut, par arrêté délibéré en Conseil des ministres, soumettre l'usage des signatures électroniques dans le secteur public à des exigences *supplémentaires* éventuelles. (...)»⁽¹⁶⁾. Les travaux préparatoires du projet 322 sont très explicites à cet égard⁽¹⁷⁾. Pour sa part, la directive euro-

⁽¹²⁾ Loi du 20 octobre 2000 introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire, *M.B.*, 22 décembre 2000, p. 42698.

⁽¹³⁾ La première, tirée du site web du SPF Économie, PME, Classes moyennes et Énergie est trop générale, la seconde, une étude de M. STORME, concerne exclusivement la signature numérique à double clé cryptographique, dont il n'est pas question en l'espèce.

⁽¹⁴⁾ Evibel est le nom de l'application centrale utilisée depuis 2008 par l'Office des étrangers.

⁽¹⁵⁾ Point 3.10 de l'arrêt.

⁽¹⁶⁾ Souligné par nous.

⁽¹⁷⁾ *Doc. parl.*, Ch. repr., sess. ord., 1999-2000, 0322/001, p. 5. *M.B.*, 29 juillet 2001, p. 33070.

péenne sur les signatures électroniques⁽¹⁸⁾ enjoignait les États membres de faire droit aux signatures électroniques pour leur utilisation non seulement dans les relations d'ordre privé mais aussi dans le secteur public⁽¹⁹⁾. Les auteurs ont généralement soutenu, ajoutera-t-on, que la loi du 9 juillet 2001 a une portée universelle au sens où elle fixe le cadre juridique pour les signatures électroniques utilisées dans toutes les branches du droit, sans nécessité absolue de textes spécifiques complémentaires⁽²⁰⁾. Au contraire, l'article 1322, alinéa 2, du Code civil reconnaît la signature électronique sur le seul terrain de la preuve des actes sous seing privé.

2° L'Office des étrangers ne prétend en aucune façon qu'il soit fait usage d'une signature électronique avancée basée sur un certificat qualifié, ni même d'une signature avancée. Qui plus est, il ressort clairement de la note évoquée que le système n'est pas fondé sur l'utilisation de clés cryptographiques⁽²¹⁾.

3° Le Conseil du contentieux des étrangers estime que la signature scannée qui figure sur la décision peut être considérée comme une signature électronique «ordinaire» au sens de l'article 2, 1°, de la loi du 9 juillet 2002. À l'appui de cette opinion, sont cités les travaux préparatoires du projet 322, sept extraits d'articles de doctrine très explicites, ainsi qu'un extrait du site web des autorités belges (eID Belgium)⁽²²⁾. En l'occurrence, il est question, en effet, d'une signature apposée, par voie électronique, sur un document qui est lui-même créé de manière électronique. Il est permis de penser, plus précisément, que l'image numérique de la signature manuscrite constitue «une donnée sous forme électronique jointe à d'autres données électroniques» (le fichier

contenant la décision administrative) «et servant de méthode d'authentification». Est abordée plus loin la question, centrale, de savoir si la signature scannée permet effectivement d'*authentifier* son auteur (*infra*, n° 7).

4° Le fait qu'un document se présente, au final, sous la forme d'une impression papier ne fait pas perdre le caractère électronique de la signature. L'autorité de plusieurs auteurs est invoquée en ce sens⁽²³⁾.

5° La signature scannée bénéficie du principe de non-discrimination⁽²⁴⁾, dont il résulte qu'une signature électronique ne peut être privée de son efficacité juridique ni refusée comme preuve en justice au seul motif qu'elle répond tout au plus à la définition de la signature électronique ordinaire⁽²⁵⁾.

6° Une signature électronique ordinaire peut être considérée comme l'équivalent d'une signature manuscrite pourvu qu'elle remplisse les fonctions traditionnellement dévolues à cette dernière, à savoir l'*identification* (du signataire) et la manifestation de son *adhésion au contenu* de l'acte. Ainsi qu'il a été noté par la doctrine, une troisième fonction découle de l'usage du papier comme support de la signature : en effet, le papier a pour propriété que toute modification ultérieure de l'acte peut être détectée de sorte qu'il contribue à l'intégrité du contenu de l'acte⁽²⁶⁾. Le Conseil du contentieux des étrangers observe qu'en l'espèce, le signataire de la décision est identifiable, sa signature étant associée à son nom écrit en toutes lettres à côté de la signature scannée, apposée au bas du document. Par ailleurs, le défendeur établit dans sa note qu'une fois l'image numérique de la signature intégrée au document reprenant la décision, celui-ci ne peut plus être modifié⁽²⁷⁾. On pré-

(18) 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 du 19 janvier 2000, p. 12.

(19) *Cfr* article 3, §7, et considérant n° 19 de la directive 1999/93.

(20) Parmi d'autres, P. LECOCQ et B. VANBRABANT, «La preuve du contrat par voie électronique», étude précitée; D. MOUGENOT, *Droit des obligations – La preuve*, Tiré à part du *Répertoire notarial*, 3^e éd. revue et mise à jour, Bruxelles, Larcier, 2002, p. 189.

(21) Point 3.11 de l'arrêt.

(22) Points 3.12 à 3.15.

(23) Point 3.16 de l'arrêt.

(24) Voy. la rédaction du principe de non-discrimination à l'article 5, §2, de la directive 1999/93 et à l'article 4, §5, de la loi du 9 juillet 2001.

(25) Points 3.17 à 3.19 de l'arrêt.

(26) Points 3.19 et 3.20 de l'arrêt.

(27) Point 3.21 de l'arrêt.

cisera encore que la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers ne prescrit nullement que la notification remise à l'étranger doit être signée. Son article 62 dispose, en effet, que « [les décisions administratives] sont notifiées aux intéressés, *qui en reçoivent une copie*, par (...), par un agent de l'Office des étrangers (...)»⁽²⁸⁾.

7° Le demandeur ne conteste pas que la signature numérisée est celle du fonctionnaire de l'Office des étrangers ni que ce dernier avait le pouvoir de rendre la décision. Il n'est pas davantage contesté que la décision imprimée et notifiée ne correspond pas au document d'origine. La question essentielle est, en définitive, celle de l'authentification : y a-t-il un mécanisme permettant de sécuriser le système en manière telle qu'une personne non autorisée ne puisse signer une décision en lieu et place d'une autre? À cet égard, le Conseil estime que la note technique évoquée plus haut décrit une procédure suffisamment fiable. L'argumentation du demandeur revient à affirmer que la signature scannée aurait été «piratée» par une personne non autorisée en vue de la prise d'une décision négative (par ex. en subtilisant l'identifiant et le mot de passe du fonctionnaire de l'Office des étrangers), mais il n'apporte aucun commencement de preuve en soutien de son assertion. Il ne démontre d'aucune façon que le système Evibel n'est pas fiable. Une signature manuscrite peut aussi être falsifiée de sorte qu'elle n'offre pas non plus une sécurité sans faille. Enfin, le demandeur ne convainc pas lorsqu'il insinue que la décision qui lui a été notifiée sur support papier pourrait ne pas correspondre à la décision originale sous forme électronique et que cette dernière, restée aux mains de l'Office des étrangers, pourrait être différente ou ultérieurement modifiée. La note présentée par le défendeur démontre à suffisance que le système est ainsi conçu qu'une fois la décision prise, elle ne peut plus être modifiée⁽²⁹⁾.

Il est conclu que la décision est valablement signée et n'est entachée d'aucune irrégularité formelle.

II. De la théorie... à la pratique

Les affaires évoquées révèlent un hiatus apparent entre la théorie et la pratique. La doctrine consacrée à la signature électronique a fait la part belle à la signature numérique fondée sur la cryptographie asymétrique et répondant aux (lourdes) exigences de la signature dite «qualifiée». Le souci de sécurité juridique explique naturellement l'attention particulière portée à cette forme sophistiquée de signature qui bénéficie de l'assimilation automatique à la signature manuscrite⁽³⁰⁾. On en finirait presque par oublier qu'en imposant d'inscrire dans les droits nationaux le principe de non-discrimination, le législateur européen entendait qu'il puisse être fait droit à une variété de procédés de signature électronique. Il n'y a dès lors pas lieu de s'étonner que soient mobilisées diverses techniques de signature électronique dont le niveau de sécurisation peut varier en fonction des besoins, risques et enjeux des opérations concernées. Force est de constater que la signature qualifiée ne rencontre pas le succès escompté, tandis que le principe de non-discrimination dévoile des potentialités insoupçonnées.

Il se dégage aussi des arrêts commentés un malaise face à la signature électronique et une méconnaissance de son statut juridique. Une autre affaire, portée devant le tribunal de première instance de Hasselt, en témoigne⁽³¹⁾. Un contribuable introduit une déclaration régulière à l'impôt des personnes physiques via Tax-on-web. Curieusement, le montant des frais professionnels déductibles n'est pas enregistré dans le système de sorte qu'il n'en est pas tenu compte dans le calcul de l'imposition. Après réception de son avertissement-extrait de rôle, le contribuable introduit une

⁽²⁸⁾ Souligné par nous. À cet égard, voy. aussi, notamment, Conseil contentieux étrangers, 28 janvier 2011, n° 55100; Corr. Bruxelles (ch. cons.), 20 septembre 2007, *T. Vreemd.*, 2008, liv. 3, p. 211.

⁽²⁹⁾ Points 3.22 à 3.27 de l'arrêt.

⁽³⁰⁾ Article 4, §4, de la loi du 9 juillet 2001.

⁽³¹⁾ Civ. Hasselt, 28 janvier 2010, *Cour. fisc.*, 2010, liv. 4, p. 363, note.

réclamation, envoyée sous forme électronique via Certipost⁽³²⁾. Cette déclaration est déclarée irrecevable par le directeur régional au motif qu'elle n'est pas signée. À juste titre, le tribunal rejette le point de vue du fisc, fondé sur un arrêt de la Cour de cassation⁽³³⁾, selon lequel la réclamation aurait dû être signée car il s'agit d'un «acte de procédure». En effet, depuis les lois de réforme du contentieux en matière fiscale des 15 et 23 mars 1999, le directeur a perdu sa fonction juridictionnelle; il agit désormais en tant qu'autorité administrative de sorte que la réclamation introduite auprès de lui n'est plus un acte de procédure. Ainsi le tribunal évite-t-il de se prononcer sur le fond : la réclamation était-elle valablement signée? À cette question, il doit incontestablement être répondu par l'affirmative dès lors que la réclamation était revêtue d'une signature électronique créée par la carte d'identité électronique du contribuable. Or, cette dernière met en œuvre une signature numérique à double clé cryptographique, fondée sur la technologie RSA et une infrastructure à clé publique. Censée répondre aux conditions de la signature électronique qualifiée, elle bénéficie du régime d'assimilation de plein droit à la signature manuscrite.

Il est vrai que la complexité et les contradictions du cadre juridique de la signature électronique ne facilitent guère sa bonne compréhension⁽³⁴⁾. Cela étant, le pessimisme n'est pas de mise étant donné l'issue heureuse des procédures engagées devant le Conseil du contentieux des étrangers. Venons-en, à ce propos, aux autres enseignements qui se dégagent des arrêts du Conseil du contentieux des étrangers.

III. L'administration de la preuve électronique, entre pragmatisme et rigueur

Profitant de leur pouvoir souverain d'appréciation de la valeur des éléments de preuve produits, les juridictions prennent en considération, avec un évident pragmatisme, l'ensemble des éléments portés à leur connaissance pour décider de la valeur probatoire des documents présentés. S'il n'est pas inédit, ce pouvoir d'appréciation n'en revêt pas moins une importance tout à fait singulière dans l'administration de la preuve électronique. L'on sait, par exemple, que la valeur probante des témoignages et présomptions dépend largement de la souveraine appréciation du juge. Mais celle-ci se focalise pour ainsi dire sur les éléments de preuve produits en tant que tels (indices et déclarations des témoins). En matière de preuve électronique, cette appréciation a une portée plus large. Elle s'étend à l'ensemble du cycle de vie du document contesté. Autrement dit, c'est tout le processus de création-conservation-gestion du document numérique qui est pris en compte dans l'appréciation des preuves.

S'agissant de la signature proprement dite, on note aussi une différence essentielle suivant qu'elle se présente sous une forme manuscrite ou électronique. Dans le premier cas, le juge est rarement invité à se prononcer sur la validité du signe. Si, par exception, une contestation s'élève à ce propos, elle s'apparente à un simple problème juridique de qualification que le juge peut aisément trancher seul⁽³⁵⁾. En pratique, 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,

(32) Plus précisément, il a fait usage du service de «recommandé hybride» de Certipost. Schématiquement, ce service fonctionne comme suit : le message signé est envoyé, par voie électronique, sur la plateforme de Certipost; le prestataire l'imprime et le remet aux services postaux; l'expéditeur reçoit un récépissé de dépôt à La Poste; quant au destinataire, il reçoit le recommandé des mains du facteur à son domicile et signe un accusé de réception; le contenu du recommandé, le récépissé de dépôt à La Poste et, le cas échéant, l'accusé de réception, les avis de refus de réception ou de non-délivrance sont conservés, un temps, par Certipost.

(33) Cass., 6 octobre 2000, *F.J.F.*, n° 2000/289.

(34) Entre autres études critiques, voy. E. MONTERO, «L'introduction de la signature électronique dans le Code civil : jusqu'au bout de la logique fonctionnaliste?», *Mélanges offerts à Marcel Fontaine*, Bruxelles, Larcier, 2003, pp. 179-210.

(35) Ainsi peut-il estimer que tel signe ne constitue pas une signature valable pour divers motifs : soit le signe est illisible; soit il n'a pas été apposé directement sur l'acte mais par le truchement d'un papier carbone, d'une photocopie ou d'une télécopie...; soit il ne manifeste pas l'adhésion de son auteur au contenu de l'acte (eu égard à son emplacement...).

sa validité est assurée. Sauf rares exceptions⁽³⁶⁾, on n'a jamais eu à se préoccuper de la fiabilité de la signature sur papier, ni du procédé utilisé. En revanche, le débat portant sur la validité d'une signature électronique ordinaire, voire avancée, conduit à des vérifications plus complexes dont l'issue est imprévisible. En cas de contestation, il y a ici lieu de convaincre le juge que le mécanisme utilisé remplit effectivement les fonctions classiques de la signature. À cet effet, il devra souvent faire appel à un expert pour évaluer la validité du procédé utilisé, avec les inconvénients qui en découlent en termes de coût et d'allongement des délais de procédure.

En toute hypothèse, l'approche est résolument pragmatique : aucune preuve électronique ne saurait être écartée sur la base de simples considérations abstraites. Tout document ou signature électronique peut passer la rampe pourvu qu'il remplisse les fonctions qu'on en attend. L'embryon de jurisprudence relative à la preuve électronique en est une illustration, qu'il soit question de documents électroniques assortis d'une signature scannée⁽³⁷⁾ ou de simples e-mails⁽³⁸⁾. Où l'on voit aussi la nécessité de documenter soigneusement le processus de dématérialisation par une rigoureuse politique d'archivage. Pratiquement, en effet, il sera difficile de convaincre un juge de la valeur probatoire des documents électroniques produits sans une bonne documentation du processus de numérisation, de conservation et, le cas échéant, de

datation électronique de ceux-ci. À cet égard, l'on ne saurait trop insister sur l'intérêt de se doter d'un cadre juridique pour les « services de confiance » tels l'archivage et l'horodatage des documents électroniques⁽³⁹⁾. Les acteurs du marché réclament avec force des règles et garanties claires en la matière. Dès 2004, l'Observatoire des Droits de l'Internet a plaidé en ce sens⁽⁴⁰⁾.

L'absence de cadre juridique représente un frein au développement de ces services. Dans la mesure où les coûts liés à l'archivage électronique ne sont pas négligeables, les entreprises souhaitent naturellement des indications *précises* sur les méthodes susceptibles d'être reconnues par le législateur. Les acteurs du marché (tant les prestataires d'archivage électronique que les entreprises qui envisagent de recourir à leurs services) ont ainsi exprimé le souhait que le législateur clarifie les points suivants : *stipuler la validité du recours à l'archivage électronique*, à certaines conditions, lorsque la loi exige, de manière expresse ou tacite, la conservation d'un document; permettre aux entreprises qui le souhaitent d'*archiver elles-mêmes leurs documents en interne*, sans recourir aux services d'un tiers⁽⁴¹⁾; *permettre la numérisation des documents papier*, puis la destruction des originaux, tout en accordant une valeur juridique aux copies numérisées; enfin, *définir les critères de qualité auxquels doivent répondre les prestataires de services d'archivage électronique* pour être reconnus comme fiables. Il ne s'agit pas seule-

⁽³⁶⁾ On songe aux débats relatifs à la griffe, aux empreintes digitales, à la signature à main guidée... Cfr D. MOUGENOT, *op. cit.*, pp. 165 et s.

⁽³⁷⁾ Cfr les arrêts du Conseil du contentieux des étrangers commentés.

⁽³⁸⁾ Cfr, par ex., Bruxelles (16^e ch.), 24 août 2010, inédit, R.G. n° 2007/AR/2896 et surtout Gand (7^e ch. bis), 10 mars 2008, *D.A. O.R.*, 2009/91, p. 314, note E. MONTERO, «À propos de la valeur probante des e-mails», *T.G.R.-T.W.V.R.*, 2009, liv. 1, p. 28, note G.-L. BALLON, «De bewijswaarde van een mailbericht», *Computerr.*, 2008, p. 303, note P. VAN EECHE et E. VERBRUGGE, «De bewijswaarde van e-mails verzonden via interne systemen». En jurisprudence française, voy. notam. Cass. fr. (1^{er} ch. civ.), 30 septembre 2010, disponible sur www.legalis.net, *Comm. com. électr.*, 2010, n° 129, p. 40, note E. CAPRIOLI; Cass. fr. (2^e ch. civ.), 1^{er} juillet 2010, *Comm. com. électr.*, 2010, n° 105, obs. E. CAPRIOLI; Cass. (2^e ch. civ.), 25 juin 2009, *Comm. com. électr.*, 2009, n° 107, obs. E. CAPRIOLI; Cass. fr. (2^e ch. civ.), 4 décembre 2008, disponible à l'adresse <http://www.legifrance.gouv.fr> (rubrique Jurisprudence judiciaire), *Comm. com. électr.*, 2009, n° 19, obs. E. CAPRIOLI.

⁽³⁹⁾ Le recommandé électronique dispose d'un cadre juridique depuis l'adoption de la loi du 13 décembre 2010 modifiant la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges et modifiant la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *M.B.*, 31 décembre 2010, p. 83267.

⁽⁴⁰⁾ Avis n° 3 relatif aux pistes pour renforcer la confiance dans le commerce électronique (1^{er} juin 2004), http://www.internet-observatory.be/internet_observatory/pdf/advice/advice_fr_003.pdf.

⁽⁴¹⁾ Il serait discriminatoire de ne reconnaître une valeur légale qu'aux documents archivés par un tiers conformément à certaines règles de l'art, et de nier toute valeur légale aux mêmes documents, archivés selon les mêmes règles, mais en interne, par l'entreprise concernée.

ment de fixer les obligations et responsabilités à charge des prestataires de services de confiance, mais aussi de prévoir un certain nombre de présomptions ou d'assimilations en faveur des documents issus de services ou de systèmes conformes aux exigences inscrites dans la loi. Un premier pas avait été fait en ce sens avec l'adoption de la loi du 15 mai 2007 fixant un cadre juridique pour certains prestataires de services de confiance⁽⁴²⁾. Néanmoins, l'essentiel du dispositif devait figurer dans des arrêtés royaux d'exécution... jamais adoptés. Autant dire que, pratiquement, tout reste à faire en la matière.

IV. *Quid* en matière d'actes sous seing privé?

Les affaires tranchées devant le Conseil du contentieux des étrangers ont la particularité que les contestations portent sur la signature du fonctionnaire de l'Office des étrangers. L'on peut se demander si l'utilisation d'une signature scannée pourrait aussi convenir dans les relations contractuelles privées. Dans ce cas, le problème se présente en des termes différents.

D'abord, c'est la personne à qui l'on oppose un acte qui pourrait désavouer sa *propre* signature, auquel cas celui qui invoque l'acte peut demander une vérification d'écriture.

Ensuite, dans les hypothèses où la recevabilité de la preuve est régie par l'article 1341 du Code civil, la signature doit satisfaire aux conditions de l'article 1322, alinéa 2, du Code civil. À cet égard, on se heurte à la condition que la signature électronique soit apte à établir le *maintien de l'intégrité du contenu de l'acte*. Si pareille fonction est une qualité incontes-

table de la signature numérique fondée sur un cryptosystème asymétrique, la plupart des autres procédés de signature électronique sont inaptes à satisfaire une telle exigence. Tout se passe comme si l'intangibilité du contenu de l'acte instrumentaire ne pouvait résulter que du mécanisme de signature. Or, la garantie d'intégrité peut être assurée par des procédés techniques autres que celui de la signature. Le système Evibel de l'Office des étrangers en est une bonne illustration. On peut imaginer un système analogue dans le secteur privé (recours à un archivage sécurisé, assuré en interne ou par un prestataire professionnel). Pourquoi donc confier obligatoirement à la signature le soin d'assurer une fonction – le maintien de l'intégrité – qui relève logiquement de l'écriture⁽⁴³⁾? Il eût mieux valu poser le maintien de l'intégrité comme condition de recevabilité de l'acte sous seing privé électronique, sans exiger que cette intégrité résulte du mécanisme de signature⁽⁴⁴⁾.

En réalité, il importe peu 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 la signature utilisée permet d'identifier son auteur et exprimer son adhésion, faut-il dénier à celle-ci la qualité de signature au motif qu'elle n'établit pas, par elle-même, le maintien de l'intégrité du contenu de l'acte? À cet égard, le législateur français a été plus avisé, en disposant que «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»⁽⁴⁵⁾.

L'article 1322, alinéa 2, du Code civil devait permettre d'accueillir une grande variété de mécanismes de signature électronique. Sa

⁽⁴²⁾ M.B., 17 juillet 2007, p. 38587.

⁽⁴³⁾ Rapp. 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. 536.

⁽⁴⁴⁾ Opinion déjà exprimée dans notre étude «Définition et effets juridiques de la signature électronique en droit belge : appréciation critique», in *La preuve*, Formation permanente – CUP, vol. 54, mars 2002, p. 72, n° 40, et suivie par D. MOUGENOT, *La preuve*, *op. cit.*, p. 194.

⁽⁴⁵⁾ Article 1316-1 du Code civil. 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 (autre 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.

rédaction maladroite est, malheureusement, un obstacle à la reconnaissance de mécanismes peu sécurisés mais aptes à établir avec une *fiabilité suffisante* les fonctions traditionnelles de la signature (identification et adhésion).

V. Réflexion finale

Enfin, on relève qu'en divers arrêts, le Conseil du contentieux des étrangers fait explicitement référence au principe d'équivalence fonctionnelle. Cette approche est intéressante dans la mesure où, en l'espèce, il avait retenu, à juste titre, la définition de la signature électronique « ordinaire » figurant à l'article 2, 1^o, de la loi du 9 juillet 2001. Or, celle-ci ne précise pas les conditions à vérifier pour déterminer si la donnée sous forme élec-

tronique jointe à d'autres données électroniques permet effectivement d'assurer « l'authentification » du signataire.

Cette approche fonctionnelle a été expressément consacrée par le législateur belge, d'une part, dans le champ de la preuve des actes sous seing privé (article 1322, alinéa 2, du C. civ.), d'autre part, en ce qui concerne le traitement des exigences légale ou réglementaire de forme prescrites dans le cadre d'un processus contractuel⁽⁴⁶⁾. Qu'il y soit fait référence pour apprécier une signature utilisée dans le contexte d'une *procédure administrative* est révélateur du caractère somme toute très naturel de la démarche inhérente au principe d'équivalence fonctionnelle. De là à voir dans les articles 1322, alinéa 2, du Code civil et 16 de la loi du 11 mars 2003 des expressions d'un principe plus général, il n'y a qu'un pas...

⁽⁴⁶⁾ Voy., en particulier, l'article 16, §1^{er} et l'article 16, §2, 2^e tiret (concernant l'exigence de signature), de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information.