Ugo Bechini (**) et Bernard Reynis (*)

La signature électronique transfrontalière des notaires : une réalité européenne.

La signature électronique[1], inventée dès 1976, semblait dans les années quatre vingt dix destinée à jouer un rôle déterminant dans les trafics on-line, elle n'a pourtant pas connu un essor significatif dans le monde des entreprises.[2] Il apparaît donc assez curieux que le notariat, un peu partout dans le monde, investisse dans la mise en œuvre d'architectures de signature électronique. Une évolution qui risque de surprendre, alors qu'il y a cinq ans le notariat européen se sentait menacé (même culturellement) par l'introduction de cette technologie; aujourd'hui, dans nombreux pays certains notaires en sont les fervents supporters.

Le phénomène a des racines profondes. La signature électronique est une technique qui permet beaucoup[3]. Elle permet de produire des documents transmissibles avec une grande facilité par Internet sans aucun risque de falsification. Elle permet à n'importe quel utilisateur d'un ordinateur connecté à Internet de contrôler en quelques secondes l'intégrité du document et l'identité de son auteur. Si l'apposition d'une signature électronique est une opération qui est en soi manifestement simple, elle implique cependant un effort d'organisation

(*) Notaire à Paris, membre du Conseil Supérieur du Notariat (France)
(**) Notaire à Gênes, président du Comité Franco-italien du Notariat Ligure et Provençal

Cet article (à quatre mains !) paraît simultanément, en langue italienne, sur la revue Notariato. .

[1] L'expression *signature électronique* désigne, dans cet article, les *signatures électroniques avancées basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature* selon la Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques Journal officiel n° L 013 du 19/01/2000 p. 0012 – 0020 (France : *signatures sécurisées* Loi du 13 mars 2000 : article 1316-4 du code civil et décret du 30 mars 2001)

[2] Hervé Morin, *Pourquoi la signature électronique reste lettre morte* Le Monde, 23 mai 2003

[3] Pour un approfondissement de ces arguments, en langue française : *Cliquer c'est signer* Bernard REYNIS JCP Not. 2000 n° 49, p. 1747 et *Vers l'authenticité électronique* Petites Affiches n° 65 du 2 avril 2001 Xèmes rencontres Notariat-Université. En langue italienne est disponible un volume qui a été distribué à cheval entre 2003 et 2004 à tous les notaires italiens : *Firme Elettroniche : questioni ed esperienze di diritto privato*, Collection Studi del Consiglio Nazionale del Notariato, Giuffrè, Milan 2003. Nous reprenons ici des arguments que nous avons déjà traités dans Bernard REYNIS, *Signature électronique et acte authentique, le devoir d'inventer*, relation au XXII Congrès annuel du Comité Franco-italien du Notariat Ligure et Provençal sur le thème *Actes authentiques en Europe et signature électronique* (Gênes 21/22/23 septembre 2001) http://web.tiscali.it/conoge/italofrancese/ge_re.htm (également dans JCP éd. N, 12 Oct. 2001, p.1494), et Ugo BECHINI, *Le frontiere del bit*, dans Notiziario Telematico Assonotai Campania, octobre 2002, http://www.assonotaicampania.it/notiziario5/notiziario_centr_inform.htm

initial que l'on ne doit absolument pas négliger. Il est en effet nécessaire de s'équiper d'un lecteur spécial de carte à puce. Il faut se faire identifier et certifier par une *Autorité de Certification,* recevoir et conserver avec soin les codes secrets. Il faut acheter et installer des logiciels spéciaux, aussi bien pour la gestion de la carte à puce que pour l'apposition et le contrôle des signatures. Pour éviter qu'une panne d'une machine empêche la production des documents souhaités en temps utile, il est nécessaire de répéter l'installation au moins sur un autre ordinateur. La certification doit ensuite être périodiquement renouvelée.

Il s'agit d'obstacles insignifiants pour ceux qui utilisent la signature électronique dans l'exercice de leur profession, et les notaires italiens se sont tous dotés de leur signature électronique en très peu de temps et sans rencontrer de grandes difficultés ; en France, la majorité des notaires sont aujourd'hui dotés de la carte REAL, outil de signature électronique dont l'autorité de certification est le Conseil Supérieur du Notariat et on peut penser que d'ici 2005, tous les notaires de France en disposeront [4]. Mais il serait vraiment inutile d'imposer une pareille obligation à tous ceux qui désirent seulement faire un peu de shopping on-line, notamment parce qu'il existe des systèmes plus simples, à commencer par le « SSL ». Ce système se base sur des technologies très similaires à celles qui permettent de faire fonctionner la signature électronique, mais contrairement à celle-ci, il ne requiert aucun effort d'équipement de la part de l'usager: le système est activé automatiquement par le navigateur, et l'usager est simplement informé, par des messages qui apparaissent sur l'écran, qu'une connexion protégée à été activée.

Le système SSL offre beaucoup moins que la signature électronique sécurisée[5] (celle des notaires): il ne permet pas d'identifier l'usager de manière vraiment

[4] L'avènement de TELE@CTES (cf. Ci-après) devrait conduire les récalcitrants à s'en doter sans tarder !

[5] La SE aussi bien que la signature manuscrite remplit deux fonctions de base : l'identification de l'auteur de base et l'expression du consentement du signataire au contenu de l'écrit (article 1316-4 du code civil français).
Le procédé de SE doit donc identifier le signataire, garantir le lien entre l'acte et la personne dont il émane et assurer l'intégrité de l'acte signé.
A l'heure actuelle, seules les SE basées sur la cryptologie d'infrastructure à clé publique (les signatures numériques) répondent aux exigences légales. En effet, ce procédé assure l'intégrité du message signé grâce à une fonction de hachage qui consiste à faire, à l'aide d'un logiciel intégré dans le dispositif de signature, un condensé du message que l'on chiffre à l'aide de la clé privée de signature et qui est logiquement lié au message électronique.
L'identification du signataire s'effectue par le biais d'un certificat électronique d'identification émis par un tiers. C'est l'autorité de certification qui délivre un certificat électronique établissant le lien entre le signataire et le bi-clé de signature. Ce certificat servira au destinataire à vérifier que c'est bien la personne qui dit avoir signé le document électronique qui l'a effectivement signé et que le message est intègre.
Le décret d'application du 30 mars 2001 précise la notion de SE sécurisée qui bénéficie de la présomption légale de fiabilité. Celui qui conteste la preuve de l'acte électronique en cause doit prouver que le procédé de signature n'était pas fiable. Ces SE sécurisées doivent répondre à des exigences juridiques et techniques, données dans le décret. Par exemple, la clé de signature doit être gardée sous le contrôle exclusif du signataire.

certaine et de documenter de manière objective les informations échangées. Il se limite à garantir deux choses à l'usager : l'identité du serveur avec lequel il est en communication (en général: celui du commerçant on-line) et la confidentialité des informations transmises. C'est très peu, mais suffisant pour convaincre un usager qui n'est pas particulièrement averti à introduire en toute confiance son numéro de carte de crédit, qui est par ailleurs la seule chose qui intéresse vraiment les fournisseurs dans le commerce électronique. Lesquels semblent donc pouvoir très bien se passer de la signature électronique sécurisée.

Les opérations financières importantes et les grands mouvements internationaux de capitaux s'effectuent, pour leur part, au sein de communautés fermées d'opérateurs professionnels (virements SWIFT par exemple). Il n'est absolument pas nécessaire (bien au contraire) que les documents en question soient lisibles et contrôlables de la part de quiconque. Une constatation assez analogue peut être faite en ce qui concerne les opérations de « home-banking »[6], lesquelles s'effectuent, seulement et exclusivement, entre le client et sa banque, sur la base de protocoles souscrits à un niveau contractuel (conventions sur la preuve).

La signature électronique ne semble pas mieux convenir aux évènements même d'une certaine importance, économique ou d'autres sortes, de la vie familiale. Les raisons en sont multiples. On imagine mal, encore, que de tels évènements (l'achat d'une voiture, par exemple) se réalisent entièrement on-line, et il est probable qu'on leur préfèrera un échange de documents traditionnels sur support papier. L'apposition d'une signature électronique est par ailleurs une opération facile, mais la simplicité de la souscription autographe fait défaut. Il s'agit de créer un fichier, de le mémoriser, de lancer le logiciel de signature, d'identifier le fichier désiré et de signer. Il suffit d'une inattention, d'un lapsus même dû à une inexpérience dans l'utilisation du système pour signer un fichier à la place d'un autre, ou bien un fichier qui n'a pas le contenu souhaité. Les spécialistes américains ont une définition sympathique pour ce genre de risques: *Grandma picks the bad password and loses her house*, « Grand-mère choisit un mauvais mot de passe et perd sa maison »[7]. En dernier lieu: la technologie de la signature électronique permet de vérifier, avec un degré de certitude incroyablement élevé, que la signature a été apposée avec une carte à puce bien précise. Cependant, qui peut garantir que cette carte à puce est réellement sous le contrôle de son vrai propriétaire ? Les hypothèses sont nombreuses, mais limitons nous à la plus évidente : un imposteur peut avoir trompé l'Autorité de Certification avec un faux, et s'être fait délivrer une carte à puce au nom d'une autre personne.

En cet état, toute tentative d'assimiler une signature électronique ordinaire à une signature certifiée par un notaire doit être rejetée. Il n'existe aucune preuve du fait que le contenu du document est réellement celui souhaité par la partie qui l'a

---

[6] Expression italienne, en français : banque à domicile !

[7] L'expression est par ailleurs citée par Brad BIDDLE, *A short history of "digital signature" and "electronic signature" legislation,* dans Simson GARFINKEL and Gene SPAFFORD, *Web Security, Privacy And Commerce*, O'Reilly, Cambridge (Massachusetts, USA) 2001.

signé[8]. Mais encore, à la base de la relation qui existe entre un document donné et une personne physique se trouve l'identification du demandeur de la carte à puce, effectuée par l'employé de l'Autorité de Certification. Même en admettant que cette identification puisse être aussi fiable que celle effectuée par un notaire (ce qui n'est pas démontré[9]) une éventuelle erreur aurait des conséquences beaucoup plus graves, dans la mesure où elle permettrait de produire un nombre illimité de documents apocryphes[10].

Les raisons, rapidement évoquées ici, font qu'un grand nombre d'usagers potentiels manifeste un certain désintérêt pour la signature électronique, alors que ce sont exactement les mêmes raisons qui en font en outil très utile pour l'activité du notaire. Et il ne s'agit pas d'une formule à effet.

Tout d'abord, les risques sont minimisés :

Les cartes à puce sont remises par les autorités compétentes[11] directement au notaire, qui en est personnellement connu. Les probabilités que les cartes à puce tombent dans de mauvaises mains sont absolument théoriques. Le notaire est un professionnel (mieux encore : le professionnel par excellence) de la gestion des contrats, et il est parfaitement en mesure de maîtriser en toute sécurité le système de signature électronique.

Les privilèges spécifiques de la signature électronique sécurisée correspondent par ailleurs à des exigences inéluctables de l'activité notariale. Le document notarié est institutionnellement destiné à faire foi où que ce soit et avec effet *erga omnes*, il n'est donc pas possible de s'en remettre à des systèmes d'identification opérant au sein de groupes fermés d'usagers. La signature électronique doit

---

[8] Le jugement est également partagé par des specialistes américains parmi les plus influents. Particulièrement sévère le jugement de Jane K. WINN, *The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce*, dans *Idaho Law Review*, Volume 37, Issue 2 (2001), qui considère encore impraticable la *tentative d'associer une identité décrite sur un certificat de signature électronique à l'intention de la partie qui y est indiquée d'être considérée juridiquement liée aux contenus d'un document électronique* (tie an identity described in a digital signature certificate with the intention of the identified party to be bound to the contents of an electronic record). On cite ici à nouveau des juristes américains non pas par sujétion psychologique (il n'y aurait absolument aucune raison, tout au moins dans ce domaine!), mais parce qu'il est extrêmement révélateur que ces sentiments soient émis par des spécialistes qui agissent dans un contexte moins formaliste que celui de l'Europe continentale et qui ne connaît pas la rigueur du document notarié de type latin.

[9] Il suffit peut être de rappeler que VeriSign, société californienne leader mondial du secteur, a délivré a des imposteurs deux certificats au nom de Microsoft (excusez du peu!), le 29 et 30 janvier 2001 http://www.microsoft.com/technet/security/bulletin/MS01-017.asp.

[10] Brad BIDDLE (*Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure*, dans *San Diego Law Review,* 33, 1143, 1996) juge inopportune même l'ambitieuse association de la signature électronique avec la signature « authentique » apposée par le Notary Public américain, personnage sans aucune formation juridique et qui n'assume aucune responsabilité, sauf dans des cas limites, en ce qui concerne le contenu du document.

[11] En France comme en Italie, les Chambres, par délégation du Conseil Supérieur du Notariat.

pouvoir être vérifiée par quiconque, dans la mesure où n'importe quel usager du Réseau peut avec une grande facilité s'assurer de l'intégrité du document et de sa véritable provenance. Elle peut voyager sur n'importe quel genre de réseau, même intrinsèquement douteux comme Internet, dans la mesure où toute tentative de falsification sera démasquée au moment de la vérification.

La signature électronique se présente donc comme un outil indispensable pour la circulation du document notarié sur Internet comme sur les Intranet sécurisés. Il n'est donc pas étonnant que le notariat italien soit par exemple en train d'effectuer une complète migration vers la technologie électronique en ce qui concerne la transmission des actes aux registres publics : pour les actes constitutifs et modificatifs de sociétés, l'élimination du papier est déjà complète, alors que en ce qui concerne la transmission des actes immobiliers au fichier immobilier et au cadastre la situation évolue de manière progressive sur le territoire italien. Le papier subsiste actuellement uniquement pour la transmission des documents aux fichiers immobiliers, et il est intéressant de savoir que la cause de ce retard est liée à une informatisation plus lente du système judiciaire italien par rapport aux études de notaires. Le fait que la conversion au système digital ait lieu plus rapidement en Italie que dans la patrie du Minitel constitue par ailleurs un petit paradoxe dont les italiens ne peuvent être qu'à moitié fiers : la meilleure efficience des structures bureaucratiques françaises, universellement reconnue[12], rend moins pressants, dans l'Hexagone, les efforts vers un renouvellement des procédures.

Le notariat français n'en est pourtant pas si loin : avec la carte REAL et l'Intranet Réal de la profession, les notaires se connectent au Fichier Central des Dispositions de Dernière Volonté et aux bases de données de la profession. Tous les notaires de France se connectent désormais au Serveur Professionnel des Données Cadastrales ; ils le font en sens unique et avec une liaison de type SSL, mais la carte REAL leur permettra dès 2006 d'alimenter directement par voie dématérialisée le fichier immobilier avec la procédure TELE@CTES. On peut regretter que l'absence du domaine de compétence réservée, dont bénéficient en revanche leurs confrères espagnols et italiens, pour la constitution de sociétés de capitaux ne les ait pas encore incité à mettre en œuvre, conjointement avec les greffes des tribunaux de commerce, une procédure électronique de transmission des statuts et des pièces nécessaires à l'immatriculation de sociétés. Il faut observer, à ce sujet, ainsi que l'a relevé récemment la Commission Européenne[13], qu'un tel dispositif[14] mis en œuvre par le notariat espagnol permet de constituer par acte notarié et d'immatriculer une société en moins de 72 heures en Espagne.

[12] À propos de ce jugement, le coauteur italien en assume l'entière responsabilité !

[13] Rapport de la Commission du 11.02.2004 au Conseil et au Parlement Européen sur la mise en oeuvre de la Charte européenne des petites entreprises COM(2004)64 final.

[14] www.circe.es/portal

Le notariat français se prépare néanmoins à utiliser ses outils de signature électronique avec d'autres fichiers publics : état civil, mairies (urbanisme) et espère ainsi combler son retard sur ses confrères italiens !

Cependant le problème reste que la diffusion du document notarié informatique se fait à l'intérieur de communautés fermées, au seul niveau national. Il ne faudrait pas en arriver à ce que l'on puisse transmettre des actes par Internet à un bureau qui se trouve à quelques mètres de l'Etude, et que l'on continue à recourir obligatoirement au papier pour envoyer la copie authentique d'une procuration à des milliers de kilomètres de distance, là où la transmission télématique serait plus utile.

Les instruments techniques qui permettent une utilisation transfrontalière de la signature électronique sont fort heureusement très simples, et en grande partie déjà disponibles.

En premier lieu, il est nécessaire que la signature électronique d'un notaire soit vérifiable par l'usager du document (qui, en général, sera un autre notaire) de manière simple et rapide. La vérification peut être effectuée à travers Internet, en consultant le site de l'Autorité de Certification [15]. À noter que le certificateur du notaire n'est pas un opérateur commercial quiconque, mais l'organisation professionnelle à laquelle il appartient : *le Conseil Supérieur* en France, le *Consiglio Nazionale* en Italie, et ainsi de suite. Ce choix répond à des exigences bien précises. Avant tout, une plus grande sécurité dérivant du rapport personnel et direct entre le certificateur et le certificat, tel que déjà mis en évidence. Pour que le document notarié puisse jouir de toute son efficacité, il est ensuite nécessaire de pouvoir vérifier non seulement que le document provient d'une personne physique bien précise, mais encore que cette personne physique précise est un notaire en exercice. Pour y parvenir les notariats de l'UINL sont en train d'adopter une solution radicale mais absolument efficace : les organisations centrales des différents notariats certifient uniquement des notaires en exercice. Après avoir vérifié que la signature de Madame X ou *del Signor Y* est certifiée par le Conseil Supérieur ou par le *Consiglio Nazionale*, nous savons que X ou Y est un notaire en exercice, dans la plénitude de ses fonctions. Dans le cas de suspension ou de cessation du notaire la signature est, respectivement, suspendue ou révoquée, et ceci apparaît au moment de la vérification.

Cependant quelques problèmes demeurent.

Dans de nombreux pays [16], le notaire n'est pas autorisé à utiliser les documents provenant de l'étranger qui n'ont pas été dûment légalisés ou revêtus d'Apostille. À défaut d'une intervention normative, de quelle sorte qu'elle soit, ceci rend particulièrement difficile l'utilisation de documents signés de manière électronique.

[15] Pour une expérience pratique visiter la page http://web.tiscali.it/conoge/test

[16] Parmi lesquels l'Italie et la France.

Heureusement entre de nombreux pays, c'est justement le cas entre la France et l'Italie[17], la légalisation et les Apostilles ont été supprimées. Il n'y a donc aucune raison pour que cette suppression ne soit pas appliquée au document sur support électronique. Ceci fait de nos deux pays les candidats rêvés pour mettre en pratique la signature électronique notariée transfrontalière: il s'agit en effet des deux seuls pays qui disposent d'architectures notariales de signature effectives et qui ne rencontrent aucun obstacle sur le plan du statut du document.

En second lieu, si le document sur support électronique (en général: une procuration) peut voyager en toute sécurité sur Internet, il devra ensuite être normalement utilisé pour la rédaction d'un acte notarié traditionnel sur papier, et joint à celui-ci. La question est un peu plus compliquée qu'elle n'apparaît à première vue. La signature électronique consiste, en ultime analyse, en un rapport mathématique entre la signature elle-même et le document signé[18]. Une fois que le document est transféré sur papier, ce rapport mathématique se perd. Il n'est donc plus possible de vérifier la signature, ce qui signifie qu'il n'est plus possible de vérifier qui a signé le document et si par la suite le document a été altéré. En bref : une fois que le document est imprimé, il n'est plus signé[19].

La solution à ce problème doit visiblement se trouver dans les législations notariales de chaque Pays, mais nous souhaitons proposer avec force une indication de principe. Il est de la compétence du notaire, en tant qu'officier public de la preuve, de fournir un témoignage privilégié sur le fait que le document sur support électronique, au moment de son utilisation, a été vérifié et que la vérification a donné un résultat positif. Si la version imprimée a elle aussi perdu ses caractéristiques techniques intrinsèques, elle pourra conserver la valeur juridique qui lui est propre sur la base d'une déclaration du notaire attestant la conformité du texte imprimé par rapport à celui où est apposée la signature électronique, dûment vérifiée.

Et ceux qui en ressentent le besoin, pourront sans aucun doute profiter de l'occasion pour une petite revanche contre l'ordinateur omniprésent en rédigeant l'attestation avec le bon vieux et fidèle stylo...

---

[17] Convention de Bruxelles 25 mai 1987.

[18] Pour être plus précis, le rapport existe entre la signature et l'hash du document, mais il s'agit d'un détail technique qui dans notre cas est sans intérêt.

[19] On ne peut même pas penser de récupérer (par exemple à travers un scanner) le document sur papier : entre autre, il suffit d'un dixième de millimètre de désalignement dans la mise en page pour produire un fichier différent, qui ne passera pas le contrôle. Pour résoudre le problème des solutions qui sont sans aucun doute intéressantes ont été proposées, comme *Paper e-Sign*, mais, à l'état actuel, aucune d'entre elles n'est un standard affirmé.