InterPARES 2 Project

International Research on Permanent Authentic Records in Electronic Systems

Policy Cross-domain

Réflexions sur l'établissement et la conservation des actes authentiques

Rapport de synthèse
Rédigé par Isabelle de Lamberterie
Directeur de recherche au CNRS - CECOJI
au nom du groupe de travail

Juin 2001

Sommaire

Avant-propos

Le présent rapport est le fruit de la réflexion commune menée depuis six mois au sein des différents sous-groupes. Son auteur a tenté l'exercice difficile consistant à traduire les différentes sensibilités et à présenter les propositions faites par les uns et les autres.

Les points de convergence ne posent pas de difficultés. Il en est différemment des points de divergence. Il faut les prendre en considération avec les enjeux qu'ils sous-tendent.

Pour éclairer les débats, un travail de droit comparé a été réalisé [1]. Un certain nombre d'encarts renseignent sur les expériences des autres pays.

Ce rapport de synthèse est une ouverture vers les annexes qui présentent de façon plus précise et approfondie les différentes facettes des sujets traités.

Enfin, le rapporteur remercie chaleureusement tous les membres du groupe de travail pour leurs apports constructifs à ce travail collectif.

Isabelle de Lamberterie

[1] Ce travail a été réalisé par Tanguy Decaup, doctorant, sous la direction d'Isabelle de Lamberterie.

Introduction

"Le véritable progrès du droit consiste à régler l'organisation de la société de telle façon que chaque homme puisse vivre et agir en sécurité..." Ces réflexions de Georges Ripert dans son ouvrage sur "les forces créatrices du droit" sont aujourd'hui d'une actualité brûlante dans la société de l'information en construction. Actualité, car l'une des questions que rencontrent ceux qui ont en charge le processus de régulation est de répondre au besoin de sécurité dans un univers où l'usage des technologies engendre autant la fascination que l'inquiétude. Toutefois cette actualité s'inscrit dans une histoire où les théoriciens du droit ont depuis longtemps montré que le droit et la technique évoluent à des rythmes différents. Quand on parle de "sécurité" c'est autant de sécurité juridique que de sécurité technique dont il est question. La sécurité juridique passe par une certaine stabilité du droit et par conséquent par l'aptitude des règles générales à appréhender des objets nouveaux tout en restant indépendantes de l'évolution de la technique.

C'est cette démarche qu'a adoptée le législateur français dans la loi du 13 mars 2000, en élargissant à tous les actes (y compris les actes authentiques) l'adaptation du droit de la preuve aux technologies de l'information. La loi autorise, ainsi, que les actes authentiques soient dressés sur support électronique à condition d'être établis et conservés dans des conditions fixées par décret en Conseil d'Etat.

La mission du groupe de travail

Avant de fixer de telles conditions, la Direction des Affaires Civiles et du Sceau a souhaité que soit menée une réflexion préalable sur les questions que soulèvent l'établissement et la conservation des actes authentiques électroniques. Cette réflexion préalable a été confiée à un groupe de travail [2] qui, dans le cadre du Groupement d'intérêt public (GIP) Droit et Justice, a réuni des représentants des acteurs concernés par la production des actes authentiques (magistrats, greffiers, notaires, officiers d'état civil, huissiers, avocats), des spécialistes de la conservation et de l'archivage, des universitaires et des chercheurs et, bien entendu, des experts des différentes technologies susceptibles d'être utilisées.

Outre des réflexions particulières propres à chaque catégorie d'actes, c'est autour de quatre questions principales que le groupe de travail est invité à remplir une double mission de réflexion et de proposition.

1 - Comment préserver les garanties de fond offertes par l'authenticité (contrôle de la réalité du consentement, information des parties...) dans le cadre d'un acte dématérialisé[3]?

2 - Dans quelles conditions et suivant quelles modalités pourra être apposée la signature électronique de l'officier public et des parties sur l'acte authentique ?

3 - Comment assurer l'archivage et la conservation pour une durée illimitée de l'acte authentique dématérialisé ?

4 - Dans quelles conditions pourront être délivrés des copies des actes authentiques dématérialisés ? Quelle sera alors la force probante de ces copies ?

A travers ces questions très précises, il convient de dégager, en les transposant au droit de la preuve, quelques-unes des problématiques de fond de la régulation de la société de l'information.

Comment respecter les grands principes sur lesquels est fondé le droit de la preuve des

[2] Cette mission est la deuxième expérience de travail collectif sur le droit de la preuve. Un premier groupe de travail avait procédé à une réflexion sur l'écrit et la signature électronique qui a servi à la préparation de la loi du 13 mars 2000.

[3] Un point de vocabulaire : Dans la logique de la loi du 13 mars 2000 qui reconnaît la valeur d'un écrit, quel que soit son support, il nous a semblé plus opportun – dans la suite du rapport et dans la mesure du possible - de parler de support informatique ou électronique pour l'acte authentique plutôt que de « dématérialisation », bien que ce terme soit culturellement associé au support informatique.

actes authentiques ? Comment répondre aux besoins de sécurité technique et juridique ? Comment établir un cadre juridique qui réponde au besoin de sécurité technique pour lutter contre les risques engendrés par la circulation de ces actes dans l'univers numérique et qui n'hypothèque pas l'avenir en ménageant la pérennisation des actes authentiques électroniques dans un futur lointain inconnu ? Ce sont ces problématiques qui ont servi de trame à l'organisation du travail du groupe.

La méthodologie employée

Compte tenu de la diversité des participants (représentative, entre autres, de la diversité des actes authentiques), la démarche adoptée pour le travail du groupe imposait une double exigence : appréhender les spécificités de chaque type d'actes authentiques tout en dégageant leurs caractéristiques communes. Une approche théorique du concept d'authenticité a, donc, servi de point de départ avant de faire le point sur les expériences concrètes de l'utilisation de l'électronique pour les actes authentiques. Il s'est agi ensuite d'analyser les trois étapes de la vie d'un acte authentique : établissement, utilisation (circulation, mise à jour, mention en marge, …), conservation à plus ou moins long terme. Cette analyse s'est appuyée à la fois sur les expériences de terrain et sur les réflexions internationales concernant ces questions. Les échanges entre les expériences respectives et le recoupement des questionnements plus théoriques ont été très riches et ont permis de tirer les fils des différentes positions dans un premier rapport qui se voulait fidèle aux travaux du groupe. Ce rapport a fait réagir les uns et les autres. Il a aussi permis de mûrir certaines questions et de défricher des pistes qui n'avaient pu qu'être ébauchées. Le contexte lui aussi a évolué.

Cette mission, comme cela a été évoqué ci-dessus, participe à l'adaptation du droit au nouveau cadre de la société de l'information français et européen. Il convient, donc, de replacer les problèmes posés dans le contexte des autres textes en préparation tant dans le cadre national qu'international. Jusqu'à présent cette mise en contexte n'était pas évidente faute d'information sur les autres initiatives. De plus, contrairement à la question de présomption de fiabilité de la signature électronique, il ne s'agissait pas de transposer un texte européen. En effet, le législateur français a devancé ses partenaires de l'Union et a pris, le premier, une initiative originale pour répondre à un besoin réel [4]. De ce fait, le travail effectué fait œuvre de précurseur avec les limites de l'exercice.

Depuis la rédaction du rapport intérimaire, le contexte s'est éclairci avec la publication du

[4] Exemples étrangers

Tant les règles uniformes de la CNUDCI (Commission des Nations Unies pour le droit commercial international) sur les signatures électroniques dans leur dernier état de septembre 2000 que la directive communautaire du 13 décembre 1999 fixant un cadre commun sur les signatures électroniques envisagent la dématérialisation de l'écrit et la reconnaissance de la signature électronique pour les actes sous seing privé uniquement. Ainsi, les législations de pays américains ou asiatiques s'inspirant très largement du premier texte et les lois de transposition du second par les Etats membres de l'Union européenne ont pour cadre général l'acte sous seing privé dans la perspective du commerce électronique.

L'étude des législations étrangères permet de tirer trois enseignements. D'abord, certains pays excluent expressément l'application de ces dispositions à l'acte authentique (ex. : Belgique, Luxembourg ou Suède). D'autres ensuite la passent totalement sous silence (ex. : Allemagne). Ce silence doit être interprété davantage comme leur exclusion implicite (exception faite de certaines lois encore en cours de procédure législative ou dont l'accès aux travaux préparatoires s'est révélé très délicat) que comme un oubli du législateur étranger de se prononcer sur ce point. Ces deux hypothèses d'exclusion expresse ou implicite constituent la quasi-totalité des exemples étrangers étudiés. Enfin, de très rares législations souhaitent expressément envisager l'acte sous seing privé et l'acte authentique sous la forme électronique (et subséquemment la signature qui y est attachée) mais sans toujours prévoir pour autant de dispositif particulier propre à répondre aux spécificités de l'acte authentique (ex. : Autriche, Espagne ou certains Etats américains).

Toutefois l'on peut s'attendre à de rapides développements concernant l'acte authentique électronique dans les législations étrangères dans un proche avenir. Preuve en est par exemple sur le plan communautaire de la directive du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information qui doit être transposée avant le 17 janvier 2002. Cette directive oblige en effet les Etats membres à supprimer toutes interdictions ou restrictions concernant l'utilisation des contrats électroniques, y compris leur archivage. Certaines restrictions pourront toutefois être maintenues s'agissant de contrats devant être établis sous la forme authentique ou qui requièrent l'intervention de professions exerçant une autorité publique. On peut sans nul doute s'attendre à de réelles avancées sur les étapes de l'existence de l'acte authentique électronique et des signatures qui y sont attachées.

décret transposant la directive sur la signature électronique. On relève, aussi, à de multiples reprises, une certaine distanciation par rapport à une technique spécifique répondant, a priori, au besoin de sécurité.

- Dans le cadre international, la CNUDCI a présenté, dans ses travaux préparatoires pour le projet de loi type sur les signatures électroniques, plusieurs techniques de signatures (autres que la signature électronique cryptographique). Le souci d'égalité de traitement des différents procédés s'inscrit dans la même logique que la prise en compte de l'indépendance technologique du cadre normatif.

- La réflexion a également été approfondie sur la question de la conservation pérenne de la signature électronique, de la signature sécurisée et, plus largement, sur les questions d'archivage électronique à long terme.

Aujourd'hui, le présent rapport tient compte de toute cette valeur ajoutée. Les propositions vont plus loin qu'il y a quelques mois. Elles invitent aussi à une grande prudence pour ne pas figer ce qui peut très vite ne plus répondre aux finalités.

C'est dans cet esprit d'ouverture, de relativité et autant que possible d'absence de parti pris qu'a essayé de travailler le rédacteur de ce rapport. Rien n'aurait pu être fait sans la richesse des débats, sans l'esprit de coopération des uns et des autres, sans l'acceptation des règles du jeu du travail pluridisciplinaire.

On soulignera aussi la bonne circulation de l'information entre les membres du groupe, le pragmatisme dont chacun a su faire preuve dans les mises en commun, enfin le respect de la confidentialité indispensable pour échanger sans inquiétude.

Les services du GIP ont beaucoup contribué à la qualité des travaux en mettant à disposition leur site intranet.

Que tous soient ici remerciés très chaleureusement.

Première partie - Les données de l'authenticité

Introduction

De nombreux auteurs, parmi les plus grands civilistes, ont apporté leur contribution à la notion d'authenticité. Cette notion est aussi au cœur de la préoccupation des officiers publics qui ont en charge l'établissement des actes authentiques. Si l'acte notarié apparaît comme le modèle type de l'acte authentique, l'importance des autres types d'actes authentiques (jugements, actes de l'état civil, actes d'huissier...) doit aussi être rappelée.

Toutefois, comme le relève Pierre Leclercq "l'incertitude la plus grande tient à la question de savoir si l'on peut prétendre reconnaître et expliciter une notion commune de l'acte authentique, dématérialisé ou non, pour l'ensemble des professions ayant capacité de l'établir "[5]. Ces propos pessimistes et réalistes montrent la difficulté de l'exercice.

Plus modeste, le propos dans le cadre de ce rapport est de cerner la notion et les contours de l'authenticité pour mieux comprendre la problématique de l'acte authentique électronique. Il n'était possible, ici, de faire qu'un bref rappel des différentes sources permettant de nourrir une réflexion tant sur l'acte authentique en général que sur l'acte authentique électronique en particulier. Partant des définitions transversales du *Vocabulaire juridique* [6] ainsi que des analyses propres à certaines des catégories d'actes, il s'agira de cerner quelques-uns des concepts clés liés à l'authenticité et de rappeler les principes sur lesquels se construit l'authenticité quel que soit le support ou le procédé utilisé (1). Sur la base de ces *données externes*, le groupe a été amené à réagir et à apporter sa *propre contribution* à la réflexion sur l'acte authentique électronique. Il l'a fait sous plusieurs formes : lecture des textes, proposition d'interprétation, réflexions prospectives (2).

1 - Les concepts clés liés à l'authenticité : les points essentiels communs à tous les actes authentiques

Comme le rappelle J.-M. Olivier, "l'acte authentique est d'abord et fondamentalement celui qui a été reçu par officiers publics" et cette condition vaut pour tous les actes authentiques [7].

Toutefois, il ne suffit pas de la *présence* d'un officier public pour qu'un acte soit authentique. J.-M. Olivier précise que l'officier public a le droit d'instrumenter *là où* l'acte a été dressé et quand les solennités requises ont été respectées. C'est ainsi, poursuit cet auteur, que l'authenticité est subordonnée à des conditions particulières, *variables* selon les divers actes authentiques.

Enfin, l'acte authentique produit trois effets principaux : sa force probante jusqu'à inscription de faux, sa date certaine et sa force exécutoire. Du fait de ces effets, mais pas uniquement, les actes authentiques doivent être conservés de manière quasi illimitée. Ce besoin de conservation guidera la réflexion et déterminera certaines des propositions conclusives du groupe.

De cette présentation très synthétique de l'authenticité, on reprendra les points essentiels qui sont communs à tous les actes authentiques et qui en constituent les éléments substantiels : d'une part la présence de l'officier public sans lequel il ne peut y avoir authenticité, d'autre part la signature de l'acte par l'officier public et suivant les cas par les parties à l'acte qui est - plus qu'une solennité requise - l'une des composantes de cet acte. Les autres solennités requises présentées par J. Flour comme "des rites extérieurs et contingents" [8] sont spécifiques à chaque catégorie d'actes authentiques. Du fait de ces spécificités, la question se pose de savoir si ces formalités spécifiques relèvent ou non du cadre

[5] Rapport de synthèse à la journée du 11 décembre 2000 organisée par les notaires (à compléter)

[6] G. Cornu, *Vocabulaire juridique*, Association Henri Capitant, PUF, 8ème édition, 2000.

[7] Jean-Michel Olivier, "L'authenticité en droit positif français", *Les Petites Affiches*, 28 juillet 1993, pp. 12-21

[8] J. Flour, "Sur une notion nouvelle de l'authenticité Commentaire des articles 11 et 12 du décret n° 71-941 du 26 novembre 1971", *Répertoire Defrenois*, 1972, 1ère partie, p. 981.

du décret prévu à l'article 1317 ou dans le cadre d'une révision des décrets propres à chaque type d'acte authentique. Nous en traiterons dans la suite du rapport.

1.1 - La place de l'officier public

C'est tout d'abord le Code civil qui détermine le rôle de l'officier public. L'article 1317, alinéa 1 donne une définition générale de l'acte authentique : « L'acte authentique est celui qui a été reçu *par les officiers publics* ayant le droit d'instrumenter dans le lieu où l'acte est rédigé, et avec les solennités requises ».

Cette définition légale générale est reprise par la doctrine :

« Authentique » : « Se dit plus techniquement, par opposition à l'acte sous seing privé, de l'acte qui, étant reçu ou parfois seulement dressé par un officier public compétent, selon les formalités requises, fait foi par lui-même jusqu'à inscription de faux » [9].

« Authenticité » : « Qualité (spécialement force probante) dont est revêtu un acte du fait qu'il est reçu ou au moins dressé par un officier public compétent, suivant les formalités requises » [10].

« Dressé » (adj.) : « Etabli, rédigé ; se dit surtout d'un acte (contrat, constat, procès-verbal) établi par un officier public soit sur ses propres constatations soit sur les déclarations ou volonté d'un tiers » [11].

A travers ces différentes sources, on relèvera l'exigence d'une *présence physique* de l'officier public.

Celui-ci est un témoin privilégié de l'apposition des signatures. L'expression "reçu" apparaît, alors comme l'un des concepts les plus importants de la notion d'authenticité[12].

« Reçu » (adj.) : « Se dit de l'acte qui est rédigé par un officier public, mais conformément aux volontés ou aux déclarations des parties contractantes ou comparantes, ex. : acte reçu par un notaire, un officier de l'état civil) » [13].

Malgré l'importance attachée à cette réception par la personne investie de mission de service public, on a pu relever les exceptions à ce principe général (dans des textes particuliers à chaque type d'actes) tant pour les actes notariés (avec l'habilitation des clercs même si celle-ci a été encadrée) [14] que pour les actes d'état civil (délégations aux agents communaux) [15].

[9] Idem, p. 89.

[10] Idem, p. 89.

[11] Idem, p. 312.

[12] Voir J. Flour, op. cit., p. 980 ; J-.M. Olivier, op. cit., p. 15.

[13] G. Cornu, *Vocabulaire juridique*, op. cit., p. 728.

[14] Voir sur ce point l'article de J. Flour (op. cit.) qui explique de façon convaincante l'articulation entre l'authenticité et la présence physique du notaire.

[15] La possibilité de délégation est critiquée par Jean Carbonnier qui considère que celle-ci vide le principe de l'authenticité (ces propos sont cités par J. Audier, "Vie privée et acte de l'état civil", *Etudes offertes à P. Kayser*, tome I, p. 8, n° 16).

1.2 - La notion de signature [16]

On présentera ici la *définition générale* de l'article 1316-4 al.1, puis compte tenu, des possibilités offertes aujourd'hui par les technologies de l'information, les précisions apportées par le législateur pour appliquer à la signature électronique, les conditions de l'article 1316-4 al.1. Pour compléter cette présentation, on reprendra les définitions de la directive sur la signature électronique et celles du décret de transposition.

1.2.1 - La définition générale de l'article 1316-4 et les précisions relatives à la signature électronique

Cette notion est un des points clés de l'établissement des actes (authentiques ou sous seing privé). La signature d'un acte est d'après les termes de l'article 1316-4 "nécessaire à la perfection d'un acte juridique" qui "identifie celui qui l'appose" et manifeste son consentement aux obligations qui découlent de cet acte. De plus, "quand elle est apposée par un officier public, elle confère l'authenticité à l'acte".

Cette définition de la signature prend en compte sa fonction quels que soient les moyens ou le procédé utilisé pour signer (manuscrite, électronique ou autres...).

Pour la signature électronique, sans poser de condition supplémentaire, le texte précise en quoi ce type de signature doit consister : "...Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache" (art.1316-4 al.2).

Enfin le législateur organise une présomption simple de fiabilité (jusqu'à preuve du contraire), "lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie dans des conditions fixées par décret en Conseil d'Etat " (art.1316-4 in fine).

1.2.2 - Les définitions de la directive et du décret sur la signature électronique

Bien que notre propos soit ici, principalement, de cerner la définition juridique de la signature électronique, le contexte normatif et la transposition de la directive sur la « signature électronique » imposent de reprendre de façon ordonnée les différents sens - y compris techniques - qui ont pu être donnés au terme « signature électronique ».

- La signature électronique dans la directive

Dans la directive 1999/93/CE du 13 décembre 1999 *sur un cadre communautaire pour les signatures électroniques* des définitions précises donnent (à l'article 2) les sens dans lesquels sont entendus dans ce texte les termes "*signature électronique*" et "*signature électronique avancée*".

Il convient de souligner cette double définition sur laquelle le groupe de travail a porté son attention.

"Signature électronique", une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthodes d'authentification »

"Signature électronique avancée" une signature électronique qui doit satisfaire aux exigences suivantes :

---

[16] Les questions de terminologie sont le préalable essentiel à toute étude de notions juridiques qui plus est dans une perspective comparatiste. Dans ce domaine, les confusions, contresens et « faux-amis » sont nombreux. Pour exemple, la terminologie de « signature électronique » recouvre plusieurs acceptions selon les législations. Soit, elle renvoie au concept même de signature à partir duquel le législateur s'attache aux fonctions qu'elle remplies quel que soit le support (c'est le cas de la directive du 13 décembre 1999). Soit, elle définit dans l'esprit du législateur un type particulier de signature électronique dans une perspective non plus ici notionnelle mais technique (ex. : dans les lois italienne et allemande, les termes « signatures électroniques » ne recouvrent en réalité que la seule signature digitale. Cette signature ne constitue qu'un exemple de signature électronique et correspond à une technique particulière pour signer électroniquement. Si elle est, dans l'exemple allemand, consacrée légalement, c'est uniquement pour des raisons d'état de la technique et de faisabilité. Mais on ne peut réduire, et donc confondre, le concept et la terminologie de signature électronique à la seule technique de la signature digitale reposant sur une infrastructure à clés publiques, laquelle recouvre d'ailleurs encore plusieurs niveaux de sécurité).

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

- La signature électronique dans le décret du 31 mars 2001 (n° 2001-272) pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique

On retrouve dans le décret de transposition de la directive cette distinction entre d'une part la signature électronique et d'autre part la signature électronique sécurisée (pour "avancée").

«Art. 1er Au sens du présent décret, on entend par :
1. "*Signature électronique*" : une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil»
2. "*Signature électronique sécurisée*" : une signature qui satisfait, en outre, aux exigences suivantes :
- être propre au signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable»

- L'efficacité juridique de la signature électronique (ni sécurisée ni avancée)

La juxtaposition de ces deux définitions prend toute son importance à la lecture de l'article 5-2 de la directive. Cet article impose aux Etats de veiller « à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique aux seuls motifs que -la signature se présente sous forme électronique ....» ou qu'elle ne réponde pas aux différentes conditions nécessaires à la signature électronique avancée.

L'article 1 du décret du 31 mars 2001, en renvoyant à la première phrase du 2è alinéa de l'article 1316-4 [17] transpose cette recommandation en donnant une définition de la signature électronique autonome par rapport à l'usage d'un procédé de signature (par ex. la cryptographie) qui, par ailleurs, a le mérite de permettre de garantir que le document signé n'a pas fait l'objet d'altération.

Nous reviendrons sur ce point crucial dans les développements sur la signature des actes authentiques.

2 - Les réflexions du groupe de travail sur les données de l'authenticité

Le groupe de travail a tenu à apporter ses contributions spécifiques - *et plurielles* - à l'approche de l'authenticité. On trouvera dans les rapports particuliers sous la plume de M. P. Henry-Bonniot [18] les résultats d'un travail sur les questions fondamentales relatives à l'acquisition de l'authenticité pour les différents actes authentiques [19]. Le notariat a aussi exprimé ses positions. Certains des membres du groupe se sont exprimés en tenant compte de la spécificité de certains types d'actes authentiques. Il faut donc relativiser et remettre en contexte ces contributions. Nous ne ferons ici que reprendre les grandes lignes de ces développements, ainsi que ceux d'autres participants au groupe de travail qui mettent l'accent sur la variété des actes authentiques qui, à côté du modèle type de l'acte notarié, sont concernés par l'acte authentique électronique.

2.1 - La diversité des actes authentiques

On reprendra ici succinctement le panorama général des actes authentiques dressé par le Conseil supérieur du notariat [20] qui apporte un éclairage tant sur la diversité des actes authentiques que sur leurs caractéristiques communes.

Les actes authentiques peuvent être regroupés autour de trois catégories : les actes à caractère administratif, les actes judiciaires et extrajudiciaires, les actes de juridiction volontaire [21].

Les actes à caractère administratif sont dressés par un fonctionnaire dans les limites de ses attributions et dans l'étendue de son ressort. Parmi ceux-ci seront plus largement étudiés les actes de l'état civil.

Les actes judiciaires et extrajudiciaires : il s'agit principalement des jugements quelle que soit la juridiction. Il s'agit aussi des actes des huissiers faits en vertu d'une délégation de la loi, des actes dressés par les greffiers et même des rapports d'expertise établis en vertu d'une délégation de justice.

Les actes de juridiction volontaire : pris à l'initiative des parties, ces actes sont dressés par un officier public compétent pour constater un acte ou un fait juridique. Il s'agit, principalement, des actes notariés [22]. Ce peut être aussi un acte de l'état civil [23].

---

[17] " .....Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache".

[18] Voir Rapports particuliers, notes du sous-groupe "Jugements".

[19] Le Conseil du notariat n'était pas représenté dans ce groupe qui réunissait par ailleurs toutes les autres professions concernées.

[20] Voir le rapport remis par le Conseil supérieur du notariat in Rapports particuliers.

[21] Cette typologie est reprise de D. Montoux, J. Cl. Not. Form. acte Notarié, fasc. A5.

[22] L'article 1 de l'ordonnance du 2 novembre 1945 accorde un monopole aux notaires pour recevoir tous

2.2 - L'acquisition et les critères de l'authenticité

- Les objets de l'authenticité

Pour cerner la notion « d'actes authentiques » le groupe de travail s'est attaché à décrire les différents « objets » de l'authenticité (constat d'un fait, d'un consentement, d'une décision…) et le mode d'intervention de l'officier public sans lequel il ne peut y avoir d'actes authentiques. Les actes authentiques répondent à des conditions de forme qui conditionnent pour certaines d'entre elles la validité de l'acte entre autres la présence physique de l'officier et des parties. Enfin, en ce qui concerne les effets de l'authenticité, sur le terrain de la preuve, l'acte authentique fait foi jusqu'à inscription de faux (1319 CC), sous réserve des limites du champ de l'authenticité. L'acte authentique peut, aussi, être revêtu de la force exécutoire et ses conditions de conservation répondent à des règles particulières.

- Les critères de l'authenticité

Mme Guyon-Renard et M. Hubert - se fondant sur leur expérience des actes de l'état civil - remarquent que ces critères sont différents selon que l'on se situe lors de la « création » ou lors de « l'exploitation » [24] de l'acte authentique. Ils relèvent que lors de la création, il faut attacher autant d'importance à la *solennité* comme à la *vérification* de la déclaration des faits, de l'identité des personnes déclarantes ou parties à l'acte et au consentement de celles-ci, qu'aux *signatures*. Lors de « l'exploitation », seule la signature de l'officier de l'état civil qui s'engage, non pas sur ce qui lui a été relaté ou ce qu'il a constaté, mais sur l'existence de l'acte et sur la conformité de la copie à l'acte qu'il détient, est exigée.

Cette différence est-elle opératoire pour la détermination des conditions d'établissement et de conservation des actes authentiques électroniques, objet du décret de l'article 1317 ? Nous reviendrons sur ce point dans la deuxième partie de ce rapport.

Le Conseil national du notariat rappelle que l'authenticité est : « Etymologiquement, l'acte authentique est celui qui se suffit à lui-même, qui agit par lui-même ». Cette définition est tirée du Traité général du notariat : « acte qui, sans pouvoir être contesté et sans faire appel à d'autres autorités, se suffit à lui seul pour accomplir son objet propre » [25].

- La force probatoire de l'acte authentique

"L'acte authentique fait foi jusqu'à inscription de faux des faits que l'officier public y a énoncés comme les ayant accomplis lui-même ou comme s'étant passés en sa présence dans l'exercice de ses fonctions." (Cass. civ. 1, 26 mai 1964, *D.*, 64.627). En revanche, la véracité des faits qui ont été déclarés à l'officier public fait foi jusqu'à preuve contraire (article 13 du décret du 3 août 1962 : "Les copies et extraits des actes de l'état civil portant la date de leur délivrance et revêtus de la signature et du sceau de l'autorité qui les aura délivrés feront foi jusqu'à inscription de faux").

- La présence d'un ou plusieurs officiers publics

En règle générale - comme le relève Eric Caprioli [26] - la présence d'un seul officier public est nécessaire. Mais, des exceptions existent (par exemple pour la révocation de testament, il faut en sus de la présence du notaire, celle d'un notaire en second ou de deux témoins, cf. article 9 de la loi du 25 ventôse an XI encore en vigueur). Il faudra s'intéresser à ces particularités pour les actes authentiques électroniques (c'est-à-dire soit exclure ces cas particuliers du passage au

les actes et contrats auxquels les parties doivent ou veulent assurer le caractère d'authenticité attaché aux actes de l'autorité publique.

[23] Voir infra la notion d'acte de l'état civil

[24] Par « exploitation » sont entendues ici la communication des copies ou extraits ainsi que la conservation et la mise à jour. Le terme utilisé par les spécialistes de l'état civil est contesté par le Conseil supérieur du notariat qui s'inquiète des dérives possibles dans la mesure où le mot "exploitation" renvoie à la technique et non pas à un concept juridique.

[25] Traité général du notariat, tome 6, fasc. notaires-notariat, p. 2912-70 n° 2.

[26] Remarques préliminaires sur le projet de décret aux regard des textes législatifs et réglementaires en vigueur - mai 2000

support électronique, soit déterminer un procédé offrant les mêmes garanties).

- Les délégations spécifiques

En matière d'actes d'état civil et d'actes notariés, les textes réglementaires reconnaissent la possibilité de délégations spécifiques pour des actes particuliers (comme les déclarations de naissance par exemple). Toutefois, il est important de rappeler que pour les actes notariés la signature par le notaire ne peut jamais faire l'objet d'une délégation. Il sera nécessaire de s'attacher aux éventuelles incidences de ces textes dans le cadre de l'établissement des actes authentiques concernés.

Pour les actes d'état civil : l'article 6 du décret n° 62-921 du 3 août 1962 modifié (délégation strictement entendue pour certains actes d'état civil par l'officier public à un fonctionnaire). La signature de l'acte d'état civil par une personne habilitée conformément à la loi confère à l'acte concerné (en général les déclarations de naissance ou de décès) son caractère authentique.

Pour les actes notariés : les délégations aux clercs de notaires (habilitation : cf. décret n° 99-1088 du 15 décembre 1999 relatif aux conditions d'établissement par les notaires identification précise, ...) relèvent d'un régime spécifique. Etant noté que seule la signature du notaire (et non du clerc) confère son authenticité à l'acte. Ce type de délégations pourra-t-il être maintenu dans le cadre des actes authentiques sous forme électronique ?

2.3 - La notion d'authentification source d'ambiguïté

Ce terme a été malheureusement utilisé par la pratique et le monde de la technique comme une traduction de l'anglais « authentication ». Il est important de distinguer le sens juridique de l'authentification (identification et adhésion au contenu d'un acte) du sens technique qui se limite aux moyens mis en œuvre pour atteindre l'identification « authentication » [27]. Dans le *Vocabulaire juridique*, l'authentification est « l'opération (contemporaine de la rédaction d'un acte) consistant à **conférer l'authenticité** à cet acte, spécialement à observer les formes dont dépend celle-ci » . Alors que l'utilisation du terme authentification par la technique comprend le «procédé matériel ou électronique visant à établir de manière formelle et intangible l'identification des parties à un échange ou une transaction électronique....» [28].

L'authentification est aussi entendue par les informaticiens comme une «opération d'habilitation et de reconnaissance d'une carte à mémoire par un serveur de sécurité» [29].

On relèvera les risques de confusion qui découlent de l'utilisation de ces expressions sans préciser s'il faut les entendre au sens technique ou juridique.

2.4 - La notion de signature électronique

- La distinction entre les différentes signatures

Le groupe a souligné l'importance d'une distinction entre d'une part la signature de l'officier public et d'autre part la signature des parties, comparants, déclarants. Ces différentes signatures ne remplissent pas les mêmes fonctions et il s'agit de les traiter chacune avec leur caractères propres.

C'est principalement la signature de l'officier instrumentant qui est essentielle. C'est lui qui atteste, en apposant sa signature qu'elle soit ou non électronique, avoir accompli toutes les vérifications nécessaires sur l'identité des parties, sur leur capacité, sur leur connaissance éclairée de la portée de leurs engagements, la liberté de leur consentement. C'est enfin cette signature qui authentifie l'acte.

La signature des parties, si elle est importante sociologiquement et juridiquement (comme

[27] Voir A. de la Presle, "Authentification et certification. Signature électronique" in *La nouvelle donne du commerce électronique*, Rapport de la mission "Commerce électronique" présidée par F. Lorentz, éd. de Bercy, 1998.

[28] Glossaire établi par AFCEE/EDIFRANCE, Observatoire de commerce et des échanges électroniques annexé au Rapport de la mission "Commerce électronique" présidée par F. Lorentz, éd. de Bercy, 1998.

[29] Idem.

une formalité) ne joue pas le même rôle. Si elle atteste de leur identité et de leur adhésion à l'acte, cette identité et cette adhésion sont aussi attestées par la signature de l'officier publique.

- Les techniques de signature électronique

Nous renverrons, pour l'analyse comparée des techniques utilisables aux exemples donnés par J.-F. Blanchette [30]. Par ailleurs les fiches comparatives sur les autres législations en vigueur montrent l'état de réflexion sur ce sujet dans les pays concernés [31].

Nous reprendrons ici les réflexions qu'ont inspirées au groupe le nouveau cadre normatif : loi du 13 mars 2000, directive sur la signature électronique, décret de transposition de la directive en application de l'article 1316-4 in fine.

Il ressort des différents textes présentés ci-dessus :

1) Qu'il faut toujours utiliser un procédé fiable d'identification garantissant le lien entre la signature et l'acte auquel celle-ci s'attache.

2) Que le concept de « signature électronique » ne doit pas être confondu avec le procédé ou dispositif de création et de vérification de signature utilisé. Ce concept dépend à la fois du procédé, des techniques auxquelles ce procédé [32] fait appel ainsi que de l'environnement humain qui participe à sa réalisation (qualité des personnes signant).

3) Que l'usage d'un dispositif de création et de vérification de signature sécurisée répondant aux critères de la directive et du décret (procédé de certification à clé publique) permet de présumer la fiabilité.

4) Que d'autres procédés peuvent être utilisés et qu'il faudra pour que ceux-ci bénéficient de la présomption de fiabilité qu'ils fassent l'objet de décrets. Ces procédés devront toujours apporter les garanties que l'identité du signataire et l'intégrité de l'acte sont assurées.

- Certification et légalisation de signature

L'utilisation par le monde de la technique du terme « certificat » défini par la directive « signature électronique » [33] peut être source de confusion. Le certificat électronique qualifié ne doit pas être confondu avec la signature. Il est important de rappeler que la certification de signature a un sens précis. Le professeur G. Cornu entend par certification de signature une espèce de légalisation, la légalisation étant « l'opération par laquelle un agent public compétent atteste la véracité de la signature apposée sur un acte public ou privé et, au moins dans le premier cas, la qualité en laquelle le signataire a agi ainsi que, le cas échéant, l'identité du sceau ou du timbre dont cet acte est revêtu afin que celui-ci puisse faire foi partout où il sera produit» ; L'opération «désigne parfois non la formalité (la vérification), mais la déclaration écrite (l'attestation) qui en résulte » [34].

En conclusion

Une fois de plus, la société de l'information est l'occasion de relire les fondements du droit et les rappels ci-dessus nous invitent à traiter de façon rigoureuse le respect des principes posés par les textes. Ils nous invitent aussi à analyser de façon rigoureuse les textes en vigueur sans créer de confusion.

Ces lectures seront une aide précieuse pour tirer les fils des problématiques soulevées par

[30] Annexe II du présent rapport.

[31] Annexe I du présent rapport.

[32] Le terme "procédé" est entendu au sens défini plus loin (Troisième partie 2-1).

[33] Article 2, alinéa 9 de la directive : "certificat : une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne".
Article 2, alinéa 10 de la directive : "certificat qualifié : un certificat qui satisfait aux exigences visées à l'annexe I et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II".

[34] G. Cornu, *Vocabulaire juridique*, op. cit., p. 503.

les questions précises posées au groupe de travail. Elles seront abordées dans la troisième partie après une présentation des expériences de numérisation appliquées aux actes authentiques.

Deuxième partie - Les expériences factuelles de numérisation appliquées aux actes authentiques

L'acte authentique électronique n'est pas uniquement une vue de l'esprit de certains parlementaires futuristes. Il correspond d'ores et déjà à une réalité. Toutefois, cette réalité est le plus souvent limitée à une étape ou une phase de la vie de l'acte authentique. Dans le cadre de ce rapport, il était donc indispensable de faire le point sur l'état des expériences et les projets déjà très aboutis.

C'est aussi l'occasion de faire le point sur les difficultés rencontrées. Ces difficultés sont perçues le plus souvent comme une inadéquation du cadre juridique existant qui serait un frein à une informatisation menée jusqu'au bout. Elles peuvent aussi relever de pesanteurs administratives ou encore des peurs que suscite le recours aux technologies de l'informatisation.

En effet, la plupart des acteurs concernés par les actes authentiques ont depuis un certain temps engagé des expériences de numérisation des actes authentiques. Le support informatique est, aujourd'hui, utilisé très largement pour la rédaction des actes. La signature des actes reste l'un des obstacles à une chaîne ininterrompue du processus de numérisation.

L'informatisation ne s'étant pas faite avec ce souci de communiquer, les échanges se font encore trop souvent sur des sorties papier faisant l'objet d'une re-saisie.

La conservation est aussi à l'ordre du jour à travers beaucoup de projets et déjà certaines expériences. Elle pose le problème du rapport au temps des supports et procédés utilisés. Elle soulève des problèmes d'organisation qui imposent une réflexion depuis la phase d'établissement de l'acte.

Compte tenu des spécificités de ces expériences, la présentation qui suit reprendra par catégories d'actes l'état d'avancement des rapports entre électronique et chacun de ces actes authentiques. On s'appuiera pour cette présentation à la fois sur les documents préparés au sein des groupes de travail par les responsables des différentes institutions concernées et sur les comptes rendus faits à l'occasion des visites sur le terrain qui ont permis à des observateurs externes de mesurer le degré d'informatisation dans l'établissement et la conservation des actes authentiques.

A travers ce double regard - interne et externe - on tentera de poser les problèmes tels qu'ils sont vécus sur le terrain. On essayera aussi de rapporter les questionnements comme les attentes même si celles-ci dépassent, parfois, largement l'objet du décret. Certains pourraient s'étonner des longs développements consacrés à l'état civil. Ils se justifient à plusieurs titres. Tout d'abord, du fait des expériences déjà très avancées du SCEC de Nantes et de différentes municipalités. Ensuite, ces expériences sont révélatrices de questions ou de difficultés rencontrées qui peuvent être reprises et transposables à d'autres types d'actes. Enfin, la réflexion interne menée à l'occasion de ces expériences a nourri une partie du travail du groupe. Cependant, il ne faut pas en tirer une place plus importante accordée à ce type d'acte par rapport aux autres.

1 - L'état civil

Les deux expériences de terrain décrites ici sont d'une part celle de la mairie de Strasbourg et d'autre part celle de l'état civil du service central d'état civil du ministère des Affaires Etrangères à Nantes. On présentera successivement les différentes étapes de la vie d'un acte d'état civil (établissement, transcription, mise à jour, communication, conservation) en resituant, à chaque étape, le cadre juridique (principes et formalismes) dans lequel s'inscrit aujourd'hui l'informatisation de l'état civil. Cette présentation sera précédée de quelques remarques générales sur le contexte de cette informatisation, la coexistence des supports électroniques et du papier et enfin des difficultés liées à la diversité des systèmes informatiques utilisés.

1.1 - Remarques préalables

*** Le contexte de l'informatisation** [35]

Il faut replacer l'informatisation de l'état civil dans le cadre de l'action des services sur les prestations de proximité (ainsi à Strasbourg, ont été développées les « mairies de quartier » qui assurent un nombre de plus en plus important de prestations auprès des usagers).

C'est ainsi que les services de l'état civil ont aujourd'hui un triple rôle : rôle traditionnel en ce qu'ils représentent un pan de la puissance publique, rôle basé sur le territoire et enfin rôle de diffusion, de médiation, de lien social. L'INSEE a joué, aussi, un rôle déterminant dans l'informatisation des mairies en proposant des aides incitatives [36] pour l'automatisation de l'envoi des données de l'état civil nécessaires au RNIPP et à d'autres fichiers dont cet institut à la charge [37].

*** La coexistence support électronique/support papier**

Sauf à Nantes où le parti pris d' «éliminer » le papier pour l'exploitation des actes a été pris dès le départ, les autres expériences jonglent avec des transferts d'un type de support à l'autre : saisie informatique, sortie papier signée, mises à jour faites en double, numérisation des fonds anciens pour la conservation et l'exploitation (faciliter les envois de copies et d'extraits).

- Les difficultés liées à l'informatisation

En dehors du choix du logiciel et des techniques (mode image/mode texte), c'est principalement le suivi et l'évolution de l'outil technique qui n'est pas sans soulever des difficultés particulièrement quand le logiciel reste la propriété du prestataire.

Des difficultés de plusieurs ordres sont apparues : mauvaise volonté initiale de la société pour faire évoluer le produit, problèmes techniques de reprise des données au moment des migrations (d'Unix à Windows NT, par ex.). Le passage d'une version à une autre ou encore le changement de logiciel est complexe, notamment lorsque l'évolution du produit entraîne un changement dans la structure des fichiers (reprise des données, correspondances malaisées à mettre en œuvre) [38]. On insistera, aussi, sur les besoins de contrôle lors des saisies ou lors des migrations.

On notera : 1) qu'il a pu être trouvé des solutions à la plupart de ces problèmes ; 2) que ces expérimentations n'ont pas entraîné d'altérations ou de pertes des données préjudiciables. Toutefois, reste le problème de la **compatibilité** entre les différents systèmes qui permettrait aux mairies d'échanger par voie électronique. Les stockages des données [39] n'étant pas normalisés (les dessins de fichiers sont différents d'un système à un autre), le passage de l'un à l'autre ne peut se faire directement : il faut par conséquent mettre en place une « moulinette » informatique coûteuse et risquée (pertes de données).

1.2 - L'établissement des actes

S'appuyant sur l'instruction générale relative à l'état civil, M. Iffrig dans son rapport [40] décrit acte par acte - de façon détaillée - les différentes étapes d'établissement des actes de

---

[35] Voir le compte rendu de visite à la Mairie de Strasbourg (3 janvier 2001) fait par Françoise Banat-Berger in Rapports particuliers.

[36] Il s'agit principalement des 600 mairies sur le territoire desquelles se trouvent des maternités. Ces communes devaient utiliser un logiciel agréé.

[37] Voir compte rendu de F. Banat-Berger de la visite effectuée à l'INSEE le 9 janvier 2001 in Rapports particuliers.

[38] Ainsi le texte des mentions marginales constituait dans les premières versions du produit un pavé constituant un tout alors qu'aujourd'hui le texte de la mention est structuré autour de champs précis.

[39] Alors même que la présentation des actes, si elle n'est pas complètement identique d'une mairie à une autre, obéit malgré tout à l'instruction générale de l'état civil (formulaires normalisés).

[40] Rapports particuliers.

l'état civil.

Nous ne reprendrons ici que quelques-uns des points qui sont plus particulièrement utiles pour répondre aux objectifs du présent rapport.

- Pour les actes de **naissance**

La **déclaration** de la naissance - à l'officier de l'état civil de la commune sur le territoire de laquelle l'enfant est né - peut être reçue en mairie ou dans les maternités (quand l'officier de l'état civil se déplace). La déclaration peut aussi être enregistrée par la sage-femme (avec vérification de l'identité des parents). Un projet d'acte est alors établi, avec signature du déclarant, du médecin, de la sage-femme. L'acte de naissance définitif est rédigé sur la base du projet par l'officier de l'état civil. Cet acte est **signé** par le déclarant en mairie (généralement la sage-femme) et l'officier de l'état civil.

- Pour les actes de **mariage**

D'après les textes, l'acte de mariage doit être dressé sur le champ (art. 75 in fine) après la réception de la déclaration de chaque partie de se prendre pour mari et femme. L'acte doit être immédiatement signé (après lecture) par les époux, les témoins, l'officier de l'état civil.

L'officier de l'état civil aura procédé préalablement à la vérification des identités, des conditions légales de forme et de fond. En pratique, le projet est établi au vu des pièces fournies par les parties [41], enregistré puis édité [42]. Enfin, l'acte lui-même est établi la veille ou l'avant-veille du mariage. Il ne devient authentique que par la signature des parties et de l'officier public lors de la célébration du mariage à condition que soit respecté le formalisme requis.

Après signature de l'acte, des avis de mention sont envoyés dans les communes des lieux de naissance des époux ainsi que des enfants (en cas de légitimation pour des enfants nés hors mariage) [43]. En cas d'acte nul (les époux ne se présentent pas), l'acte est rayé avec la mention « nul » dans le registre papier (sans signature) tandis que l'enregistrement est supprimé de la base [44].

- Pour les actes de **décès**

Après le constat du décès, un acte de décès est établi par l'officier de l'état civil sur la déclaration d'un parent ou d'une personne possédant des informations sur l'état civil de la personne décédée.

Pour conclure ce survol rapide des différentes procédures, tout d'abord trois remarques concernant les registres. D'une part, les actes, établis aujourd'hui par un procédé informatique, sont imprimés en deux exemplaires sur papier spécial (numéroté et filigrané) qui sont pour l'instant signés d'une façon manuscrite. D'autre part, les logiciels respectent l'instruction générale de l'état civil et il est impossible d'introduire un nouveau numéro entre deux actes. Enfin, au début de chaque année, un exemplaire de chaque registre doit être transféré au greffe du tribunal de grande instance [45]. Pour l'instant seuls les registres papiers sont transférés ainsi que les pièces annexes.

On reprendra, ensuite, quelques-unes des obligations de l'officier de l'état civil qui méritent d'être soulignées. La procédure d'établissement de l'acte de l'état civil n'est pas uniquement une affaire de saisie et de traitement de données. L'officier public établit une relation avec les personnes concernées. Il « reçoit » le déclarant, il doit consigner ce qui a été déclaré, il invite les personnes concernées à justifier leur identité qu'il vérifie, il donne lecture de l'acte aux déclarants ou comparants avant que ces derniers ne signent...En ce qui concerne l'acte proprement dit, il devient un acte authentique de par la signature de l'officier de l'état civil qui engage sa responsabilité sur la vérification du respect des formes et le contenu de l'acte.

1.3 - L'expérience du service central d'état civil rattaché au ministère des Affaires

[41] Dossier qui peut être retiré dans une mairie de quartier mais qui est rapporté avec les pièces demandées à la mairie centrale avec un entretien entre les parties et un des officiers délégués du service (choix du jour…). Cet entretien permet notamment de déceler les éventuelles fraudes (mariage blanc).

[42] Parallèlement à la publication des bans.

[43] Aucune gestion des récépissés n'est effectuée (aucun enregistrement dans la base).

[44] On constatera seulement un écart dans la numérotation des actes.

[45] Art. 53 du Code civil.

étrangères [46]

De mars 1999 à juillet 2000, le SCEC a procédé à la numérisation des actes qu'il conserve dont la particularité générale est de comporter uniquement la signature de l'officier de l'état civil (transcription consulaire d'acte étranger, acte établi pour les étrangers devenus français). Cette opération a eu pour effet d'abandonner l'exploitation des actes sur registre papier. les actes informatisés ne sont pas pour autant prêts à être exploités. En effet, la numérisation n'ayant pas été effectuée par des officiers de l'état civil, elle doit être contrôlée lors de l'exploitation de chaque acte. C'est pourquoi l'officier de l'état civil est chargé de valider l'acte informatisé.

Ce qui caractérise cette expérience (décrite de façon détaillée en annexe 2), c'est tout d'abord la gestion du processus d'établissement et d'authentification de l'acte qui fait intervenir l'officier de l'état civil pour « valider » la saisie et authentifier la transcription par sa signature et l'apposition de son sceau. La signature est électronique dans la mesure où la personne habilitée va chercher l'image de sa signature dans une base de données sécurisée et qu'elle l'applique au bas de l'acte comme elle l'aurait fait avec un stylo. Toutefois, cette signature n'est pas encore apposée systématiquement. Pour l'instant, seuls les extraits et copies sont signés aussi. L'image de cette signature (et celle du sceau) apparaissent quand on visualise l'acte à l'écran ou quand on imprime celui-ci.

L'établissement des registres en double original est réglé par une sortie papier du registre informatisé mais la mise à jour des registres se fait uniquement sur la version numérisée.

1.4 - La mise à jour des registres

C'est dans le Code civil à l'article 49 et dans l'instruction générale relative à l'état civil ainsi que dans le décret du 3/8/62 que l'on trouve précisées les conditions de l'apposition de mentions marginales. On ne prendra en compte ici, que la manière dont les mentions sont apposées et non les différentes informations apposées : les mentions doivent être rédigées avec concision, d'une écriture fine et serrée de manière à laisser la place pour d'autres mentions mais pas d'abréviation, doivent être indiqués la date et le jour de l'apposition, enfin les mentions doivent être revêtues de la signature du fonctionnaire délégué qui les a apposées.

Que veut dire « en marge » ? Le terme est compris au sens large. Dans les différentes mairies (entre autres Strasbourg) la mention est portée - comme nous l'avons déjà souligné - à la fois sur le registre papier et sur le registre informatisé. Sur le registre papier, comme sur le registre informatique, la mention est portée à la suite de l'acte.

La question de la difficulté de signer les mentions informatisées a été en partie réglée en 1993. En effet, l'article 7-1 du décret du 3 août 1962 (décret n° 93-1091 du 16 sept. 1993) limite l'obligation de signature de la mention marginale aux mentions manuscrites. A Strasbourg la signature n'est apposée que sur le registre papier [47].

1.5 - La communication des actes de l'état civil : les copies et extraits

En principe les copies et extraits ne peuvent être délivrés que par les officiers d'état civil qui les détiennent [48]. La demande peut être faite en direct sur place, par courrier ou encore par voie télématique pour les services de l'état civil qui y sont raccordés. La délivrance n'est possible aujourd'hui que directement au guichet ou par courrier.

Dans la pratique actuelle (à Strasbourg), toutes les délivrances (copie intégrale, extrait,

---

[46] Quatre documents établis dans le cadre du groupe de travail présentent le SCEC du MAE :
- Note du service central de l'état civil du ministère des Affaires Etrangères du 23 juin 2000 sur l'informatisation de la tenue de l'état civil par les officiers de l'état civil du MAE et évolution des normes juridiques ;
- Note du service central de l'état civil du MAE (Nantes n° 256/dir/EC) du 26 juin 2000 ;
- M. Huber, Premières réflexions rapides sur l'acte d'état civil dressé sur support électronique eu égard aux contraintes actuelles de l'état civil, 4 juillet 2000 ;
- Compte rendu de F. Banat-Berger de la visite de l'état civil de Nantes le 30 novembre 2000.

[47] Voir infra.

[48] Art. 13 du décret du 3/8/1962, art. 193 et s. de l'instruction générale relative à l'état civil.

extrait simplifié [49]) se font sur support papier et sont signées de façon manuscrite, à partir de l'acte enregistré dans la base, d'autant que les copies sont souvent délivrées par les mairies de quartier.

En dehors de la délivrance aux particuliers, la possibilité de l'accès direct aux bases de données d'actes de l'état civil accordé à des institutions doit aussi être traitée. On citera à titre d'exemple l'arrêté du 27 juillet 1994 qui autorise la sous-direction des naturalisations à obtenir les informations contenues dans la base de données du service central de l'état civil du MAE. Si l'interconnexion du système est interdite, la cession de fichiers ne l'est pas. La CNIL l'a d'ailleurs admis en donnant un avis favorable.

Les copies et les extraits peuvent être rédigés à la main ou reproduits par tout procédé mécanique ou informatique automatisé ou optique pourvu que le document qui en résulte ne laisse ni apparaître ni deviner les indications qui ne doivent pas y figurer. On notera l'importance accordée aux mentions qui ne doivent pas figurer. Il est important de signaler que ces copies ou extraits sont signés numériquement.

1.6 - La conservation des actes de l'état civil

L'organisation de la tenue de l'état civil ne peut être conçue sans garantir la *conservation* et la *pérennité* des actes de l'état civil et, comme le soulignent Madame Guyon-Renard et Monsieur Hubert [50], le terme *"conservé"* vise non seulement les conditions de stabilité, de pérennité et de fiabilité dans l'archivage des actes dressés sur support électronique, mais aussi les conditions dans lesquelles l'officier public les exploite (délivrance de copies ou d'extraits qui ont eux-mêmes la valeur d'acte authentique et la force probante qui s'y rattache).

Dans le cadre des expériences d'informatisation, pour remplir cette même finalité d'exploitation, l'objectif a été d'opérer un traitement des registres conservés. A Strasbourg, la « re-saisie » totale de l'arriéré a été programmée. Les premières reprises ont concerné les actes qui allaient être le plus demandés dans les années à venir [51]. On a pu s'interroger sur les risques d'erreur consécutifs à cette opération. A ce jour, la sécurité de cette re-saisie repose sur le fait que les actes sont systématiquement relus à deux et que ce sont, depuis plusieurs années, les mêmes personnes provenant de cette société qui réalisent ce travail.

A Nantes au SCEC du MAE, l'opération a consisté, comme nous l'avons vu, à procéder à une scanérisation des registres en mode image. Les risques d'erreur de saisie ont été écartés mais il a fallu traiter d'autres risques de perte d'information. On notera que chaque fois qu'un acte « transcrit » électroniquement fait l'objet d'une demande d'exploitation (demande d'extrait ou de copie, notification de mention....) l'officier public procède à une sorte de validation de la transcription et authentifie l'image de l'acte.

2 - Les actes notariés

Depuis déjà longtemps, la saisie des actes notariés est faite sur des supports informatiques. Toutefois, les signatures restent pour l'instant manuscrites. Quant à la conservation des minutes, elle est encore le plus souvent assurée de façon traditionnelle. Il faut néanmoins signaler des cas où les minutes sont numérisées, principalement afin de pouvoir plus facilement en délivrer des copies, le support papier étant bien entendu conservé.

Aujourd'hui, conforté par la familiarisation des études avec l'informatique, le Conseil supérieur du notariat a ressenti le besoin d'une harmonisation des pratiques relatives à la saisie, qui est en train de se mettre en place. C'est en 1998 que le Conseil supérieur du notariat a adopté un projet d'équipement de la profession d'un réseau électronique dénommé Plan R.E.AL. Ce plan doit se dérouler sur trois grandes phases, les deux premières étant actuellement en cours de réalisation.

---

[49] Sans filiation.

[50] Voir Rapports particuliers, Notes sur l'état civil.

[51] Voir le compte rendu de F. Banat-Berger, in Rapports particuliers. La reprise est accomplie aujourd'hui pour 74 % de l'arriéré et se poursuit encore, à raison d'un marché de 300 000 Frs par an. La reprise est également effectuée en interne dès lors que les agents en ont la possibilité

La première phase du projet consiste à doter tous les membres de la profession d'une carte à puce, la carte R.E.AL., qui garantit l'identité du porteur.

La deuxième phase consiste à installer le système de sécurité sur tous les composants du réseau R.E.AL. afin de sécuriser l'ensemble des échanges entre membres de la profession en utilisant un réseau Intranet national. Au 1er janvier 2001, plus des deux tiers des études de France étaient abonnées.

Lorsque le système sera déployé dans l'ensemble des études et que le décret sur l'acte authentique électronique sera adopté, chaque notaire à titre individuel sera en mesure, en utilisant cette infrastructure de sécurité, de proposer des services électroniques à ses clients.

2.1 - L'intranet notarial

Le réseau intranet notarial, appelé **notaires.fr,** est construit à partir du service Global Intranet proposé par France Télécom.

L'ambition de ce projet est de permettre :
- le partage des données collectives de la profession, par exemple l'accès au fichier des dispositions de dernières volontés (FCDDV) ;
- l'accès sans restriction aux gisements de connaissance d'internet ;
- l'échange entre offices de documents sécurisés par les méthodes de signature électronique ;
- la communication avec les clients et au sein de la profession par les moyens des messageries internet et intranet.

Afin de garantir l'usage exclusif des services disponibles sur le réseau notaires.fr, et de sécuriser les très nombreuses communications électroniques qui leur sont associées, le Conseil supérieur du notariat a conçu avec France Télécom un réseau spécifique dont l'architecture repose sur la technologie dite de l'Intranet.

Réservé aux seuls membres de la profession notariale, il est protégé de toute tentative d'intrusion et surveillé en permanence afin d'en garantir l'inviolabilité et la performance. Il permet en revanche à ceux qui l'ont adopté d'accéder librement et en toute sécurité aux ressources mondiales d'Internet.

La technologie choisie à cette fin est basée sur l'utilisation de gardes-barrière gérés par France Télécom. Toutefois, celle-ci n'assure pas la sécurité des applications elles-mêmes et des données échangées. En particulier, les services de signature électronique et de non-répudiation nécessitent des moyens agissant à un niveau supérieur.

C'est pourquoi, le Conseil supérieur du notariat a placé sa confiance dans la technologie des cartes à puces et a mis en place une infrastructure de sécurité à partir des concepts étudiés dans le cadre du projet européen OSCAR cofinancé par la Commission européenne (DG XIII – Programme ETS 97) et la Société CS - Communication et Systems.

2.2 - La carte notariale REAL

C'est une carte à microprocesseur protégée par un code confidentiel. Elle est utilisée à partir d'un lecteur raccordé au poste de travail de l'utilisateur.

2.2.1 - La carte notariale

C'est la partie la plus visible du système destiné à sécuriser des applications informatiques. Elle supporte l'algorithme RSA avec des clés dont la longueur peut atteindre 1024 bits.

Elle contient une donnée appelée *certificat* dont le rôle est de garantir le lien entre l'identité du porteur de la carte et les clés cryptographiques RSA stockées dans la mémoire de la carte.

Ce certificat est calculé par l'infrastructure de certification notariale et la création des cartes respecte une procédure de sécurité très stricte assurant le plus haut niveau de sécurité.

La carte à microprocesseur offre de multiples avantages pour le développement de nouveaux services :

- C'est un support qui permet de protéger l'identité et les privilèges de l'utilisateur ;

l'utilisateur *peut être notaire, clerc ou un autre employé de l'étude.* L'étude ne devant pas se substituer au notaire, le notaire a une clé qui lui est propre.

- C'est un coffre-fort assurant la confidentialité des clés privées et permettant ainsi la mise en œuvre de moyens de chiffrement de haut niveau de confiance.

- C'est un ordinateur capable de réaliser les calculs cryptographiques nécessaires, évitant ainsi de sortir les clés privées de la carte.

- C'est le support reconnu internationalement comme le support le plus adapté à la signature électronique en termes de sécurité, de fiabilité, de facilité d'utilisation et de coût.

* *L'animus signandi* de la personne lors de la signature est exprimé par la saisie du code confidentiel de la signature électronique du document,
* La présence de la personne est contrôlée par la présence physique de ce qu'elle possède (la carte) et la vérification de ce qu'elle sait (le code confidentiel).
* La présence de la carte peut être également contrôlée durant toute la session de travail afin de s'assurer de la présence de la personne.

- La signature électronique sécurisée d'un message ou d'un document au moyen de la carte ne peut être ni contrefaite, ni répudiée.

- C'est un support multiservices permettant à l'utilisateur d'accéder à plusieurs applications avec la même carte et le même code confidentiel.

2.2.2 - L'infrastructure de certification notariale

A chaque carte notariale sont associés un identifiant unique d'utilisateur et un jeu de clés cryptographiques.

Afin de garantir que l'utilisateur dont l'identifiant a été transmis lors de la connexion au serveur est bien un membre de la profession, il est nécessaire de créer un lien sûr entre cet identifiant et les clés cryptographiques. C'est le rôle de l'infrastructure de certification notariale. Ses fonctions sont les suivantes :

- *gestion des utilisateurs* : une fois l'utilisateur enregistré, l'autorité maintient dans une base les données de l'utilisateur (nom, droits d'accès ou privilèges, autres données associées à son certificat).

- *génération des clés :* la paire clé publique/clé privée RSA est générée pour l'utilisateur.

- *génération des certificats :* la station génère un certificat de clé publique conforme au standard X.509v3 [52].

- *personnification des cartes :* la clé privée de l'utilisateur et la clé publique de l'autorité sont chargées dans la carte ; ensuite, la clé privée ne pourra plus jamais être extraite : elle n'est plus utilisable qu'au sein de la carte et moyennant la saisie par l'utilisateur de son code confidentiel.

- *publication des certificats :* le certificat est placé dans un annuaire ; celui-ci est accessible par l'application (FCDDV) et l'infrastructure de certification notariale.

- *maintenance des listes de révocation :* l'autorité maintient une liste de certificats invalidés, par exemple suite à la perte de la carte et la publie dans l'annuaire sous la forme d'une « liste noire ».

Pour cela, l'infrastructure de certification notariale se compose des sous-ensembles suivants :

- OSCAR-CA : une des stations de certification pour les autorités de certification dont le rôle est l'enregistrement des utilisateurs des cartes et la création de leurs cartes,

- OSCAR-DIR : un annuaire qui permet à l'application de contrôler en temps réel les droits d'accès des utilisateurs, droits qui peuvent être modifiés à partir des stations de certification.

[52] ITU-T Recommandation X.509 (1997) ISO/IEC 9595-8 (to be published), Information Technology – Open Systems Interconnection – The Directory : Authentification Framework.

- OSCAR-TTS : un serveur d'horodatage qui délivre une date et heure certifiées. Ce serveur détient sa propre paire de clés RSA qui lui permet de certifier la date et l'heure associées à un message.

2.2.3 - L'architecture de sécurité

La fonction d'administration des utilisateurs est en fait organisée en deux niveaux hiérarchiques : le niveau national géré par un organisme dont l'autorité est nationale (le CSN) et un niveau régional dont la gestion est attribuée par l'autorité nationale à un organisme représentatif des instances locales (les chambres départementales de notaires).

* L'autorité de certification nationale a pour rôle de certifier les autorités de certification régionales. Sa tâche principale est l'enregistrement des informations relatives aux différentes autorités de certification et la génération des cartes Autorité. Ces cartes Autorité sont ensuite remises via un canal sûr aux autorités qui pourront les utiliser sur leurs stations de certification.
* Les autorités de certification régionale assurent l'enregistrement de chaque utilisateur relevant de leur juridiction (identifiant et droits d'accès).

2.2.4 - La carte à microprocesseur

Celle-ci rend accessible le fichier central des dernières volontés (FCDDV). De ce fait, la consultation ou le dépôt d'un document testamentaire ne sauraient en effet être autorisés via l'intranet notarial sans certification de l'identité du notaire à l'origine de l'opération grâce à sa carte à microprocesseur.

La carte pourrait permettre ensuite le développement de multiples services, tels que :

* L'accès à d'autres applications de la profession : CRIDON, bases de données immobilières, etc…
* Le paiement électronique et la banque électronique.
* La signature électronique.
* La fourniture de certificats électroniques aux clients des études notariales.
* L'authentification au sens notarial de documents déposés par les clients.

Ces projets ne remettent pas en cause la présence physique des notaires et leur rôle traditionnel en tant qu'officiers publics. Ils attestent l'identité des parties, la réalité des consentements, la véracité des mentions figurant dans l'acte. Cependant, pour mettre en conformité le droit positif avec les nouvelles conditions d'établissement et de conservation des actes notariés, il s'avère indispensable de revoir le décret du 26 novembre 1971 qui précise les formalités auxquelles l'acte notarié est soumis.

3 - Les jugements

Le rapport de P. Henry-Bonniot [53] décrit l'expérience du TGI de Marseille qui applique aux minutes civiles le système de gestion électronique de documents (GED) adopté aussi par d'autres juridictions : une fois signé, le jugement est gravé sur CD-Rom avant d'être classé. Ainsi toutes les copies, exécutoires ou non, sont délivrées à partir de l'enregistrement sur CD-Rom.

Les minutes - sur support papier - sont classées et constituent une garantie, outre une obligation légale en l'état, mais elles ne sont plus utilisées pour la délivrance des copies.

Cette situation prend en compte la dématérialisation désormais systématique de la décision judiciaire lors de sa dactylographie, du fait de son enregistrement sur un support électronique. Elle tient compte, aussi, d'un poids culturel fort en faveur du support papier qui remplit - de plus - une fonction de sauvegarde face aux possibles aléas des techniques informatiques, bien connus de l'institution judiciaire dans le passé.

Toujours dans son rapport, P. Henry-Bonniot relève quelques-unes des difficultés procédurales susceptibles de se poser dans le cadre de la numérisation des actes. Ces

[53] Voir Notes du sous-groupe "Jugements" in Rapports particuliers.

difficultés concernent, entre autres [54], les conclusions qui doivent être visées dans le jugement et parfois être jointes à la décision. Ce sont aussi les mentions en marge (rectificatives ou non, mention d'un appel en cours, mention d'une amnistie) qui posent la délicate question de la gestion en parallèle de la minute papier et des expéditions du jugement (informatisé).

4 - Les barreaux

Les expériences d'informatisation de cette profession ne concernent pas - stricto sensu - l'établissement et la conservation des actes authentiques. En effet, si les avocats sont destinataires ou transmettent des copies authentiques, ils n'ont pas qualité pour recevoir des actes authentiques puisqu'ils ne sont pas officiers publics. Toutefois des cas d'application concernant les relations entre les professionnels entre eux et avec le tribunal ont montré l'intérêt d'une gestion électronique de l'échange de pièces et de dépôt des conclusions [55]. La transmission des jugements, qui serait l'aboutissement de cette communication électronique, n'est pas encore pratiquée, même pour de simples copies.

Par ailleurs, la transmission d'actes authentiques sous signature électronique apporterait une grande commodité qu'autorisent les règles de procédure moins formalistes qu'à l'égard des parties elles-mêmes (notamment articles 671 à 674 du NCPC).

5 - Les huissiers de justice

Comme l'explique Me Voillequin, dans sa présentation [56], le taux d'équipement informatique des études d'huissier de justice est proche de 100%. Les matériels et les logiciels sont performants et récents. Les systèmes informatiques mettent à disposition des bases de données, des bibliothèques d'actes, des logiciels de conception d'actes et de suivi de procédure. La rédaction de l'acte s'opère donc sur les divers systèmes avec des logiciels différents et des formats d'encodage variant suivant les procédés utilisés.

Pour respecter les textes, aujourd'hui, l'acte une fois conçu électroniquement est édité et matérialisé en trois exemplaires papiers : un exemplaire destiné à être délivré au signifié ; la copie, un exemplaire conservé à l'étude ; la minute enfin, un exemplaire appelé double original destiné à accompagner la vie de l'affaire (il est remis au requérant, ou il est dans les pièces déposées au tribunal, il reste aussi au dossier de l'huissier de justice).

Les représentants de la profession montrent aussi l'intérêt que représenterait pour leur profession une possibilité d'organiser des échanges électroniques (avec d'autres huissiers, des avocats) [57]. Toutefois, ils insistent, aussi, sur les limites de ce type d'échanges dans leur activité première qu'est la signification. Le caractère « pédagogique » de la remise impose de sauvegarder la présence physique de l'huissier et la part accordée à l'oralité.

6 - Les greffes des tribunaux de commerce [58]

Les tribunaux de commerce ont déjà une longue expérience en matière d'échanges dématérialisés : premières expériences télématiques dès les années 1984-1986 et depuis le début des années 1990, dans le domaine des transmissions inter administrations : transmissions avec le casier judiciaire (demandes de casier pour toute personne désirant faire immatriculer son entreprise), transmissions au BODAC, à l'INSEE (numéros d'immatriculation au registre du commerce qui viennent automatiquement agrémenter les bases de données de l'INSEE), relations avec des banques et autres organismes financiers pour l'inscription d'opérations de crédit-bail [59].

---

[54] On renverra pour les autres points au rapport du groupe cité note 53.

[55] Voir Notes du sous-groupe "Jugements" in Rapports particuliers qui décrit l'expérience test de Bordeaux dès 1980 ainsi que d'autres projets (Barreaux de Versailles, Rennes)....dont Ediavocat.

[56] Contribution de la profession d'huissier de justice in Rapports particuliers.

[57] Ces éléments seront repris dans la deuxième partie.

[58] Sont repris ici les éléments du compte rendu de la visite effectuée par F. Banat-Berger, Laurent Jacques et I.de Lamberterie au Conseil national des greffiers des tribunaux de commerce le 4 janvier 2001. Le compte rendu a été rédigé par Françoise Banat-Berger, in Rapports particuliers..

[59] Cette opération est possible aujourd'hui car elle ne nécessite aucune pièce justificative : il s'agit

Actuellement, au tribunal de commerce de Bobigny, est mis en place à titre expérimental, l'établissement des assignations sur support électronique [60] : préparées par les donneurs d'ordre, elles transitent par un serveur puis sont acheminées vers les huissiers de justice (un enrôlement automatique est alors effectué). Seuls les éléments variables de l'acte sont véhiculés, l'élément standard fixe étant ensuite agrégé aux éléments variables permettant ainsi la reconstitution de l'acte proprement dit.

Des projets sont en cours notamment pour les inscriptions des privilèges de sécurité sociale [61] ou bien encore avec les centres de formalités des entreprises. En outre, un projet important (annoncé par la loi Madelin) mais jamais réalisé concerne le dépôt électronique des comptes annuels des sociétés aux greffes des tribunaux de commerce [62]. Cette question sera abordée dans la suite du rapport.

uniquement d'un simple bordereau qui est dématérialisé, puis qui fait l'objet d'une sortie papier pour archivage.

[60] Une sortie papier est tout de même encore produite, conformément à la législation.

[61] En attente de regroupement et de standardisation des centres informatiques des URSSAFF.

[62] Ce projet n'a pas encore été mené à bien en raison de la complexité de l'opération. L'idée était en effet de créer un centre commun, de passer par conséquent des conventions avec les entreprises, d'imposer un format électronique.

En conclusion : quelques réflexions transversales

Si l'usage de l'informatique est déjà depuis longtemps le lot quotidien des officiers publics, cet usage se heurte - en l'état actuel du droit - à plusieurs interrogations pour concilier les textes et les facilités qu'offre la technique. La principale de ces interrogations réside dans la signature électronique des actes authentiques dans la mesure où les officiers publics ne disposant pas encore du décret précisant les conditions d'établissement et de conservation des actes authentiques électroniques, maintiennent en parallèle des circuits papier et des circuits électroniques avec les risques d'erreur. En outre, on ne dispose pas encore (le plus souvent [63]) des réseaux sécurisés permettant un échange et un traitement de l'information. Enfin, au-delà de la rédaction des actes authentiques sur support électronique, la conservation et l'archivage sur des supports informatiques imposent une nouvelle logique. Quid de l'avenir à long terme des actes authentiques sur support informatique ?

Par ailleurs, tous s'accordent pour mettre l'accent sur le principe selon lequel l'acte authentique électronique ne doit pas remettre en cause ni modifier les missions fondamentales de l'officier public lors de l'établissement ou de la communication des actes.

[63] On notera que le notariat propose avec le réseau REAL une réponse à ce problème, voir supra.

Troisième partie - Quelles problématiques pour l'établissement et la conservation d'un acte authentique électronique ?

Le sens des termes « établissement » et « conservation » des actes authentiques électroniques

La question s'est posée de savoir s'il fallait ou non entendre *stricto sensu* les termes « établissement » et « conservation ». Il est apparu au groupe de travail qu'il fallait les entendre comme recouvrant toutes les phases de la vie de l'acte authentique : la réception des déclarations, la rédaction de l'acte, sa signature constituent les différentes phases de l'établissement initial de l'acte.

La finalité de la conservation des actes authentiques a principalement pour intérêt de **rendre possible leur délivrance** aux intéressés. En effet, ceux-ci peuvent se prévaloir de la force probante particulière de ces actes auprès de tiers ou de l'administration. L'acte authentique est généralement appelé à être communiqué et, éventuellement, mis à jour ou complété en marge. Certains peuvent aussi être complétés par des mentions. Ces deux aspects de la vie d'un acte soulèvent des problèmes de gestion. Ces derniers couvrent aussi bien les moyens mis en œuvre pour assurer l'intégrité de l'acte à court terme (tenue des registres) que ceux de sa communication. Pour prendre une certaine distance par rapport au risque de confusion relatif à l'usage d'un vocabulaire propre à certains actes [64], on intitulera "vie de l'acte" les développements relatifs à la période entre son établissement initial et sa conservation à long terme.

Enfin, on réservera, enfin, le terme « conservation » aux questions liées à sa pérennité à long terme.

Il convient avant d'aborder chacune de ces étapes de dégager quelques questions générales communes permettant ainsi de cerner la finalité du futur décret.

1 - Questions générales et finalités du ou des décrets

Comme nous venons de le voir, les professionnels et acteurs concernés n'ont pas attendu la loi du 13 mars 2000 ni le décret fixant les conditions d'établissement et de conservation des actes authentiques pour mettre en œuvre les expériences décrites ci-dessus. Pour compléter ce panorama, on donnera ici quelques témoignages qui illustrent ce qu'attendent les professionnels concernés du futur décret.

Celui-ci pourrait permettre :

* d'éliminer dans la chaîne d'établissement des actes toute rupture de charge (passage d'un support papier à un support électronique vice-versa) ;
* de réaliser des gains de productivités et des économies en mettant fin à la conservation papier des documents (greffiers des tribunaux de commerce) ;
* de simplifier des démarches administratives pour les usagers et de limiter la fraude en dématérialisant l'échange d'informations relatives à l'état civil ;
* de faciliter l'enregistrement des faits (par exemple, éviter le déplacement du préposé à l'hôpital ou du déclarant auprès de l'officier de l'état civil territorialement compétent pour créer l'acte) ;
* de faciliter et d'accélérer l'accomplissement des formalités et des échanges avec les diverses administrations ;
* il peut être, enfin, une occasion de mettre en place de nouvelles relations de confiance entre partenaires professionnels et entre les officiers publics et les « usagers » [65].

[64] Voir supra les discussions sur le thème "exploitation".

[65] Propos tenus lors de la visite au Conseil national des greffiers des tribunaux de commerce (voir Rapports particuliers).

Certaines de ces attentes visent une amélioration des conditions d'établissement et de mise à jour des actes authentiques électroniques. D'autres traitent des questions de sécurité. On ressent le besoin de créer un climat de confiance qui nécessite du temps et des explications. Enfin, certaines relèvent plus de pratiques propres à certaines catégories d'actes que de questions générales à l'ensemble des actes authentiques.

La mission confiée au groupe qui se situe principalement dans le cadre du droit de la preuve, invitait à des réflexions particulières propres à chaque catégorie d'actes. On ne pouvait donc échapper à la question de savoir s'il était souhaitable ou non de proposer un cadre commun à l'ensemble des actes authentiques électroniques complémentaire des décrets spécifiques à chaque type d'acte. Les témoignages ci-dessus invitent aussi à considérer l'acte authentique électronique non pas comme une rupture mais comme une continuité par rapport aux solutions mixtes aujourd'hui en place. Enfin, l'occasion de ce décret a incité à des réflexions qui dépassent largement le cadre de l'article 1317 du code civil. «L'acte authentique est celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises».

Faut-il ou non les traiter ? Y a-t-il des possibilités d'interaction avec d'autres textes en préparation ?

1.1 - Acte mixte/acte tout électronique

Pour le passage au tout électronique

Ce sont, principalement, les arguments économiques qui sont surtout utilisés pour justifier un système qui ferait disparaître le papier tant pour l'établissement que pour la conservation des actes authentiques. Toute rupture de charge (passage d'un support électronique à un support papier vice-versa) représente un coût induit.

Par ailleurs, les risques d'erreur de saisie et de re-saisie ne sont pas à négliger.

Enfin, les partisans du passage au tout électronique directement invoquent le fait que ce support ne présente pas plus de risque que le support papier à condition que les garanties soient apportées par la technique utilisée.

Pour des solutions mixtes

Pour la plupart des membres du groupe de travail, il s'avère essentiel de garder la possibilité de solutions mixtes associant électronique et papier dans la chaîne d'établissement, vie et conservation des actes authentiques. Plusieurs arguments ont été avancés.

Tout d'abord, les craintes liées à une technique que l'on ne semble pas maîtriser, l'inquiétude causée par les difficultés techniques liées à l'absence de compatibilité entre les différentes applications : pour passer d'une version à une autre, d'un logiciel, voire d'une application à une autre application, par les inconvénients des formats propriétaires (« soumission » à une société [66] et à ses aléas – faillite…, difficultés de récupérer les codes sources).

Ce sont aussi les craintes liées à l'avenir des supports, à l'obsolescence rapide qui sont des obstacles à une perspective de conservation pour une durée illimitée.

Certaines des craintes exprimées concernent la signature électronique qui serait très difficile à mettre en œuvre, surtout pour les parties concernées, mais aussi pour l'officier de l'état civil.

Malgré la souplesse et la facilité apparentes liées au fait qu'il n'y aurait plus de rupture de charge, il faudrait, pour ces raisons garder le maintien d'un système mixte. Il n'empêche que cette mixité n'est pas une fin en soi et ne doit être entendue que comme une phase transitoire au moins dans l'établissement et durant la vie de l'acte (communication et mise à jour des actes).

[66] Racheter un produit avec ses codes et le développer soi-même implique des moyens informatiques internes importants.

On relèvera la pertinence des arguments avancés pour un passage au tout électronique comme pour des solutions mixtes. Il est difficile de départager les uns et les autres. Toutefois plusieurs raisons militent en faveur d'une période transitoire où le passage - du support papier au support électronique - se fera par palier. En premier lieu, la confiance dans le papier n'est pas uniquement une affaire culturelle. Il faut du temps pour que les supports informatiques fassent leur preuve. Les informaticiens eux-mêmes suggèrent une coexistence dynamique des deux supports plutôt qu'un simple remplacement de l'un par l'autre [67] En second lieu, il serait regrettable de ne pas tenir compte de la diversité des situations, le pragmatisme invitant à ne pas mettre en place des réformes imposées si le besoin ne s'en fait pas sentir.

La question délicate de la conservation à long terme oblige aussi à beaucoup de prudence.

En conclusion, le groupe de travail recommande de laisser à chacun des acteurs la possibilité d'organiser à son rythme le passage au tout électronique.

1.2 - Un et/ou plusieurs décrets ?

Le Conseil supérieur du notariat est réservé sur la nécessité d'un décret général qui lui paraît peu évidente. Il n'existe pas de texte commun aux actes authentiques en général, *en dehors des articles 1317* et suivants du Code civil. On doit aussi se demander quel pourrait être le contenu d'un tel décret général, compte tenu du fait que la définition de l'authenticité résulte de la loi et que les actes authentiques sont très spécifiques. Il conviendrait donc mieux de traiter ces spécificités dans des décrets particuliers.

Toutefois, comme on a pu le voir, l'acte authentique électronique ouvre l'opportunité de rappeler les principes de l'authenticité quel que soit le type d'acte. Pour la plupart des participants au groupe de travail, le texte de l'article. 1317, comme les articles suivants, concerne tous les types d'actes authentiques. Par conséquent, il s'avère nécessaire, voire indispensable, de traiter sur les mêmes bases des points communs à tous les actes authentiques.

Certains souhaiteraient même que soit précisée la liste des actes authentiques concernés. Même si une liste exhaustive n'est pas dressée, une formulation montrant que le champ d'application du décret couvre tous les types d'actes authentiques (et non pas uniquement les actes notariés) aurait le mérite d'écarter toute ambiguïté [68].

Si un décret général semble la voie à adopter malgré les réserves de la profession notariale, il va sans dire que ce décret général devra ouvrir sur d'autres textes spécifiques à chaque type d'actes. Chaque catégorie d'acte authentique faisant l'objet de dispositions spécifiques, il faudra procéder aux adaptations nécessaires de chacun des textes les régissant respectivement.

En ce qui concerne les actes notariés, le décret du 26 novembre 1971 sur « la forme des actes notariés » traite des conditions propres au support papier. Le groupe de travail - à l'invitation du notariat - a étudié les nécessaires transpositions de ces conditions au support électronique.

Le même travail devra être fait pour l'état civil, les jugements, ou encore les textes régissant la profession d'huissiers. Le contenu des décrets spécifiques dépendra des situations particulières à chaque acte. Certaines des réflexions de ce rapport pourront servir pour leur préparation. Toutefois, il était difficile de leur consacrer une part plus importante.

En conclusion, le groupe de travail recommande à la fois la rédaction d'un décret général (en application de l'article 1317 - texte commun à l'ensemble des actes authentiques) et des décrets spécifiques à chaque type d'acte.

[67] Voir sur ce point, Ziming Liu et David G. Stork, "Is paperless really more ? Rethinking the role of paper in Redigital age", communication of the ACM, nov. 2000, vol. 43, n° 11, pp. 94-97.

[68] Voir, in Rapports particuliers, les remarques de la Direction des Archives de France.

1.3 - Les finalités du décret général

1.3.1 - Le décret peut-il aider à préciser le sens de l'art. 1317 et des différents termes ? entre autres la notion d'authenticité ?

Le Conseil supérieur du notariat attire l'attention sur le fait qu'un tel texte précisant la notion d'authenticité et les conditions générales de sa délivrance relèverait plus domaine législatif que du domaine réglementaire.

Pour les autres membres du groupe cela permettrait de lever les ambiguïtés. Il ne s'agirait pas d'autre chose que de rappeler le sens juridique différent du sens de la directive « signature électronique » qui l'utilise dans un sens technique.

1.3.2 - Le décret doit-il traiter de questions techniques ?

Dès qu'il est question de "technique" se pose la question de savoir comment les textes juridiques doivent se positionner par rapport à l'une ou l'autre technique. La lecture de la directive signature électronique et du décret de transposition sont des exemples de textes qui reconnaissent, pour un besoin déterminé (présomption de fiabilité) qu'un certain procédé présente les garanties attendues.

Faut-il pour les actes authentiques établir une "*norme*" ou recommander une *technique* ou un *procédé* dans un décret fixant les conditions d'établissement et de conservation de ces actes ?

La variété des expériences, les difficultés rencontrées pour permettre des échanges de données, les problèmes liés à la pérennisation des actes authentiques sont autant de sujets qui invitent à défendre une homogénéisation des techniques et des outils utilisés pour établir et conserver les actes authentiques électroniques. Toutefois, les avis divergent , apparemment, sur les moyens d'y parvenir.

Pour le Conseil supérieur du notariat :

* La question de la saisie des actes électroniques (« respect des rubriques ») ne doit pas être réglée dans le décret, mais dans les arrêtés d'application : il s'agit en effet d'une question purement technique.
* Les termes « sauvegarde », « sorties papier », « fixation sécurisée » sont à éviter, car ils technicisent l'œuvre de l'officier public : son rôle n'est pas de sécuriser la fixation de l'acte, mais de conférer la sécurité juridique à la transaction elle-même. Les questions techniques n'ont pas leur place dans le décret, mais dans des arrêtés d'application, ces questions étant sujettes à des évolutions constantes.

Pour les membres du sous-groupe « technique » :

Le rapport du sous-groupe de travail sur les aspects techniques de la dématérialisation des actes authentiques [69] dresse un état des solutions techniques disponibles ou susceptibles de le devenir à brève échéance. Il s'appuie entre autres sur la norme NF Z 42-013 dont la nouvelle version est proposée à l'ISO. L'ensemble des prescriptions que contient cette norme « vise à permettre que des documents électroniques soient produits, stockés et restitués de telle façon que l'on puisse être sûrs de leur intégrité et de leur fidélité par rapport aux documents d'origine ». Le sous-groupe de travail fait également référence à la réflexion menée au niveau national et international sur l'adoption du format XML en tant que standard dans les échanges dématérialisés. En conséquence :

* Il est important de mettre l'accent dans le décret général sur la qualité du support (durabilité, lisibilité) ainsi que sur l'intégrité du contenu et sa durabilité ou encore la fiabilité de la signature électronique.
* Il s'agirait, aussi, de mettre l'accent sur des normes à respecter afin d'éviter les solutions hétérogènes et fermées faisant échec à la mutualisation des données.
* Enfin recommander l'usage de formats et de supports identiques pour une catégorie d'acte donnée pouvant répondre à un besoin d'harmonisation ; le détail de ces

[69] Voir, in Rapports particuliers, F. Banat-Berger et Y. Rabineau, L'établissement et la conservation des actes authentiques dématérialisés : problématiques, Etat de la réflexion du sous-groupe "Sécurité et conservation", janvier 2001.

recommandation pouvant se trouver dans des arrêtés ministériels.

Il ne s'agit pas de vraies divergences mais deux approches du problème de la technique. A l'appui de nombreux témoignages, et comme le soulignent les notaires qui en ont fait l'expérience, la diversité des procédés comme la rapidité d'évolution des techniques invitent à rester prudent et il serait souhaitable de veiller à la neutralité technologique du décret général. Celui-ci ne devrait traiter ni des procédés ni des normes techniques.

Toutefois, le besoin de normalisation est ressenti par tous. La Direction des Archives de France insiste aussi, sur ce besoin. Il lui semble nécessaire que les solutions techniques retenues par types d'actes soient compatibles, voire uniques. Elle invoque le précédent des formulaires et modèles papiers qui sont imposés par l'administration. Il serait nécessaire de transposer à l'univers numérique l'encadrement de l'univers papier. Mais, comme cela déjà été souligné, il est indispensable que ces « modèles » soient indépendants des plates-formes matériels et logiciels [70].

Pour répondre à ce besoin, que faut-il, alors, mettre dans le décret général et réserver dans les décrets spécifiques ?

Il semble évident que le décret général doit inciter à la compatibilité, poser la recherche d'exigence de qualité des supports (durabilité et lisibilité), inviter à ménager l'avenir et prévenir les questions relatives à la portabilité etc...

Mais doit-il aller plus loin ? Recommander une norme qui peut-être demain ne sera plus le standard de fait ? Ne doit-on pas laisser aux décrets spécifiques le soin d'harmoniser l'architecture de chaque type d'acte authentique ?

En conclusion, le groupe de travail recommande que le décret général traite des critères à prendre en compte pour assurer une normalisation sans aller jusqu'à recommander ou imposer tel ou tel procédé ou technique.

2 - La répartition des compétences (fonctionnelle/territoriale)

L'informatisation de l'établissement des actes authentiques conduit à se poser la question des répartitions de compétence (territoriale et/ou fonctionnelle). L'utilisation de l'électronique doit-elle être accompagnée par une réflexion sur les répartitions possibles des rôles entre les différents officiers publics (qu'il s'agisse des officiers de l'état civil, des greffes des tribunaux ou encore des notaires, des huissiers ou de tous les organismes chargés de la conservation) ? A titre d'exemple : en matière d'acte de naissance, peut-on concevoir que l'officier de l'état civil qui reçoit la déclaration soit différent de celui qui établit l'acte ?

Faut-il profiter du décret ou des décrets pour ouvrir sur une réorganisation des procédures d'établissement et de conservation des actes authentiques ?

Cette question centrale a été principalement soulevée par le sous-groupe « état civil ». Pour ce groupe, l'intérêt majeur de la loi du 13 mars 2000 et de ses décrets d'application est d'ouvrir la réflexion sur d'autres modes de tenue de l'état civil qu'il appartient de définir en prenant en considération les demandes suivantes exprimées par les usagers et les professionnels [71].

Pourraient, ainsi, être posées les règles de ce qu'on a pu appeler le formalisme électronique et abordées les questions organisationnelles et institutionnelles.

Dans ses remarques, la Direction des Archives de France aborde, aussi, la question d'une réorganisation des structures institutionnelles et souhaite que le décret sur les actes authentiques électroniques ne reste pas au niveau des principes et tienne compte « des

[70] Voir, in Rapports particuliers, Remarques de la Direction des Archives de France : des exemples sont donnés ("définition type document" DTD ou des schémas sous le format XML).

[71] Exemple pour l'état civil : centralisation des registres, simplification du « charpentage des actes » lors de leur création, possibilités de mise en place d'une carte à mémoire « État civil » attribuée à chaque citoyen.

nouvelles réalités » pour envisager une « nouvelle répartition des charges de conservation » [72].

Tout le monde s'accorde à reconnaître que l'ensemble de ces points doivent être traités dans des textes. Mais, il est important dans ces différents points de distinguer ce qui peut relever de l'ensemble des actes ou ce qui relève de l'un ou l'autre des textes spécifiques. On peut, aussi, se poser la question de savoir si certains de ces souhaits entrent ou non dans le champ d'application de l'article 1317 qui traite de la preuve des actes authentiques et non pas des questions organisationnelles et institutionnelles.

La Direction des Archives et le sous-groupe technique ont attiré l'attention sur la complexité technique et le coût induit par la conservation à long terme des documents électroniques dans la situation actuelle. Il semble que certains des dépositaires - mairies, tribunaux, officiers ministériels - seraient dans l'incapacité de garantir l'intégrité à moyen et à long termes des documents sur support électronique. Les auteurs de ce constat insistent sur le caractère impératif d'une révision de la chaîne d'archivage à compter de la phase de production, remettant en cause les compétences fonctionnelles et territoriales actuelles.

72 Voir, in Rapports particuliers, Remarques de la Direction des Archives de France sur la dématérialisation des actes authentiques, janvier 2001 ; voir aussi, F. Banat-Berger, La signature électronique et ses conséquences sur le secteur privé, décembre 2000.

Ces remarques en appellent d'autres :

* D'une part que la loi du 13 mars 2000 n'a pas eu pour objet d'entraîner une modification d'une façon ou d'une autre de la répartition des compétences des officiers publics
* D'autre part que si la compétence territoriale des officiers publics est déterminée par la voie réglementaire [73], il ne faut pas oublier que la compétence fonctionnelle (ou d'attribution) des officiers publics et ministériels est définie par la loi [74].

En conclusion, le groupe de travail considère que les questions relatives à la compétence fonctionnelle et institutionnelle des officiers publics ne relèvent pas du champ de sa mission ni du ou des décrets concernés. Si ces points doivent être traités ce pourrait être dans le cadre d'autres textes (ex. pour la conservation la loi sur les archives).

Toutefois, le décret général pourrait faire état de la nécessité de prendre en compte dès la phase d'établissement de l'acte des questions relevant de la pérennité de cet acte (conservation à long terme).

3 - Les conditions de l'établissement des actes authentiques électroniques

Mme Guyon-Renard et M. Hubert, membres du groupe « Etat civil » proposent une interprétation du terme "établi" qui aide à la compréhension de l'article 1317.

Le terme *"établi"* se rapporte aux conditions de rédaction de l'acte et de son authenticité, c'est-à-dire celles relatives à l'intervention des différentes personnes intéressées [75] à l'acte et, plus particulièrement, l'officier public sous l'autorité et la responsabilité duquel les comparants et les témoins interviennent. Pour résumer, le mot « établi » paraît équivalent à « créé ». »

Pour les notaires, la distinction entre *« établi »* et *« dressé »* paraît sans grande portée ; les termes sont synonymes et il serait plus opératoire de les comparer au terme *« reçu »*, toujours employé par le Code civil, tant à propos des actes authentiques (art. 1317) que des actes de l'état civil (art. 34 et 35).

Quel que soit le terme (établir ou créer), la question relève des conditions posées pour l'authenticité. Comment transposer les solennités requises ? Comment traiter des différentes signatures électroniques ? Enfin, quelles sont les incidences de l'électronique sur la présentation des actes et le statut des originaux et des copies ?

3.1 - Les solennités requises pour les actes authentiques électroniques

Mme Guigou lors de la discussion parlementaire a dit expressément l'intérêt d'une réflexion sur le formalisme électronique :

« La forme électronique ne doit pas remettre en question les garanties particulières dont l'acte authentique est revêtu. Il faut trouver un formalisme électronique qui se substituera aux exigences actuelles liées au support papier et qui permettra à l'officier public de rester le témoin privilégié de l'opération constatée dans l'acte ».

Il convient donc de reconnaître que l'acte authentique électronique ne remet pas en cause le principe d'un formalisme. Pour ce formalisme « à trouver » les exigences sont-elles les mêmes que pour l'acte authentique sur support papier ?

[73] Décret n° 79-1037 du 3 décembre 1979.

[74] Pour les notaires et les huissiers, ordonnances du 2 novembre 1945. Il convient d'indiquer que pour le notariat la question de la répartition des compétences se pose plus pour la conservation des actes que pour l'établissement.

[75] Aux n°s 88 et 89 de l'instruction générale relative à l'état civil du ministère de la Justice sont définies les personnes intervenant à l'établissement des actes. Ce sont les comparants (les parties ou les déclarants), les témoins et l'officier de l'état civil.

Les propos de la Ministre semblent apporter une réponse : *le formalisme à trouver* ne doit traiter que des modalités selon lesquelles est dressé l'acte et non pas des conditions requises pour la solennité de l'opération constatée par l'acte. On traitera donc de la présence de l'officier public, de celle des parties, des signatures électroniques, enfin de questions connexes touchant à l'établissement des actes (doubles registres, copie et original...).

3.1.1 - Acte authentique électronique et présence de l'officier public

Comme nous l'avons souligné dans la première partie de ce rapport, la présence de l'officier public est une condition substantielle de l'authenticité. Sa fonction de témoin (témoin du consentement des époux, du consentement des parties, de la décision du juge, de la déclaration de naissance ou de décès, d'autres déclarations diverses) lui permet de dresser l'acte sur lequel sont constatés ces déclarations ou ces consentements.

Il est témoin privilégié car il *procède à des vérifications* et *atteste tout à la fois de l'identité* des parties, de la *réalité de leur consentement*, de la *véracité* et de l'*exactitude* de certaines mentions figurant dans l'acte.

Ce qui démarque l'acte notarié de l'acte sous seing privé, c'est la présence physique du notaire qui le reçoit (ou éventuellement de son clerc habilité). Le notaire, officier public intervient comme témoin privilégié : Il est témoin, car il rapporte dans son acte ce qu'il a vu et ce que les parties lui ont déclaré. Il en est de même de l'officier de l'état civil comme de l'huissier. On notera l'importance de la lecture faite aux déclarants.

La possibilité d'utiliser les capacités des technologies de l'information pour une déclaration ou une lecture de l'acte à distance a été évoquée. Depuis longtemps il aurait été possible avec une caméra (vidéoconférence) ou tout simplement un téléphone de procéder à ces formalités. Cependant, la quasi-unanimité s'est faite au sein du groupe de travail pour rejeter cette éventualité**.**

3.1.2 - Présence des parties ou du déclarant

Faut-il exiger aussi la présence physique des parties ou du déclarant ? Tout dépend du type d'actes dont il est question. Pour les actes de naissance ou de décès, on assiste aujourd'hui à un processus en deux temps. Le déclarant (parents...) fait sa déclaration à une personne (sage-femme, pompes funèbres...) qui à son tour joue le rôle de déclarant auprès de l'officier public. Pour un mariage, on voit mal les futurs époux représentés ou donner leur consentement à distance.

Voulant sauvegarder le principe d'un notaire instrumentaire unique qui atteste de la rencontre des consentements, le Conseil supérieur du notariat recommande expressément le recours à la technique de la procuration.

Pour les actes notariés, le consentement des parties qui ne sont pas présentes physiquement pourrait être recueilli au moyen d'une procuration authentique reçue par un autre notaire et transmise au notaire instrumentaire unique. La procuration pourrait être envoyé sous forme électronique - via un réseau sécurisé - . Elle serait ensuite annexée à la minute électronique de l'acte [76].

3.1.3 - L'identification des parties et de l'officier public

L'officier public est la personne dont « émane » l'acte authentique. Il doit être « dûment identifié » (art. 1316-1). L'acte authentique électronique - comme l'acte authentique papier - doit donc contenir les éléments permettant d'identifier celui qui remplit la fonction d'officier public.

L'identification des parties constitue aussi *une obligation pour l'officier public* dans le processus d'établissement de l'acte authentique électronique. Celui-ci engage sa responsabilité sur la vérification de l'identité des personnes parties à l'acte. Il doit aussi porter sur l'acte lui-même les identités telles qu'il les a reçues et vérifiées.

Peut-on imaginer une « identification électronique » ? Il est encore prématuré de penser à

[76] Voir, in Rapports particuliers, le rapport du Conseil supérieur du notariat.

une carte d'identité électronique mais rien ne s'y opposerait dans le principe. Toutefois, un point délicat devra être éclairci dès maintenant : un certificat à clé publique utilisable pour la signature électronique[77] peut-il être utilisé pour justifier l'identité d'une personne qui est soit déclarante soit partie ? La possession d'un certificat suffit-elle à justifier de l'identité d'une personne ? N'est-ce pas à l'officier public de vérifier cette identité et ne doit-il pas pour un acte authentique exiger la production d'autres éléments venant corroborer les indications du certificat. On mesure les risques que représenterait une présomption de fiabilité qui dégagerait l'officier public de son obligation de vérification. Dans le cadre de l'établissement de l'acte authentique, il engage sa responsabilité et la force probante de l'acte authentique (jusqu'à inscription de faux en écriture) est beaucoup plus forte que celle du certificat (présomption simple).

En conclusion, le groupe rappelle que :

A propos de la présence de l'officier public

* Quelles que soient les facilités qu'offre le support électronique pour le recueil à distance du consentement, modifier le principe actuel de présence de l'officier public serait une remise en cause de l'authenticité de l'acte auquel le législateur n'a pas souhaité apporter de modification.
* Qu'il convient d'ajouter que modifier ce principe de la présence physique pour l'adapter au support électronique, rendrait nécessaire de prévoir la même adaptation pour le support papier, afin d'éviter toute discrimination entre les supports que la nouvelle loi a bien déclarés comme étant équivalents
* Que la présence physique de l'officier public ne peut être réduite à une simple modalité d'exécution d'une obligation. Elle fait partie de l'essence même de l'acte authentique.

A propos de la présence des parties ou du déclarant

* Il ne faudrait pas que l'utilisation de l'électronique entraîne des dérives dans l'établissement des actes authentiques : la présence physique des parties (ou de ceux qui disposent de leur procuration) est indispensable au même titre que la présence de l'officier public.
* Le groupe recommande que ce principe soit rappelé dans le décret général.

A propos de l'identification des parties

* Le groupe de travail attire l'attention sur l'importance de maintenir l'obligation de l'officier public de vérifier les identités des personnes parties à l'acte, cette vérification ne pouvant être réduite à la présentation d'un certificat utilisable pour la signature électronique (voir infra).

Une fois le constat des déclarations ou du consentement effectué, les identités vérifiées et l'acte saisi sur un support électronique, reste à gérer la question de la signature des parties et de l'officier public sans lesquelles l'acte ne peut relever du statut des actes authentiques avec les conséquences que le droit y attache (force probante, date certaine et force exécutoire). Comment pourrait s'organiser la signature électronique de l'acte authentique ?

3.2 - La signature électronique

Après quelques questions générales on traitera des conditions et des modalités suivant lesquelles peut être apposée une signature électronique à un acte authentique ainsi que de la place d'une signature sécurisée dans le processus d'établissement et de conservation des actes authentiques.

3.2.1 - Questions générales

*** De l'importance de la signature**

[77] Voir décret de transposition de la directive "signature électronique".

Pourrait-on supprimer la signature de l'officier public ou des parties à l'acte établi sur support informatique ? Cette question, qui apparaît iconoclaste, mérite attention pour les raisons suivantes.

Quand on examine ce qui est envoyé aux demandeurs de copie ou d'extraits, on constate que le document qui leur est adressé ne comprend pas, toujours, la signature de l'officier qui a établi l'acte. La signature peut être uniquement celle de l'officier de l'état civil qui a fait la copie ou l'extrait et sa signature garantit la conformité de la copie à l'acte. Pourquoi exiger une signature qui ne parviendra pas à l'usager ?

Toujours à propos des actes de l'état civil, F. Banat-Berger et Y. Rabineau observent que la signature des parties pourrait ne plus être indispensable quand ces parties sont présentes lors de l'élaboration de l'acte. Dans ce cas, l'officier public atteste du consentement à l'acte et garantit les identités.

Toutefois, plaide pour le maintien d'une signature, quelle que soit sa forme (manuscrite ou électronique), la garantie qu'un officier public engage sa responsabilité pour authentifier l'acte[78].

Il semble que le caractère hautement symbolique de la signature suffit à justifier sa nécessité.

L'acte peut avoir été saisi sur support informatique par une personne qui n'est pas officier de l'état civil (secrétaire de mairie, clerc de notaire). La signature - qu'elle soit électronique ou non - manifeste l'intervention personnelle de l'officier public et engage sa responsabilité. N'en est-il pas de même des parties à l'acte ou des déclarants ?

Dans quelles conditions et suivant quelles modalités pourra être apposée la signature électronique de l'officier public et des parties sur l'acte authentique ?

3.2.2 - Conditions et modalités de la signature électronique

Dans la première partie de ce rapport le groupe de travail a proposé une lecture des différents textes. Ceux-ci distinguent de façon explicite la signature électronique de la signature électronique sécurisée.

* La définition de la signature électronique laisse ouverte les conditions et les modalités dans lesquelles cette signature est apposée pourvu que ces conditions et modalités correspondent à l'usage d'un procédé d'identification garantissant le lien de la signature avec l'acte auquel elle s'attache (art. 1316-4 première phrase du 2è alinéa).
* La définition de la signature sécurisée renvoie - de plus dans le décret - à d'autres exigences dont celle de rendre détectables des modifications ultérieures de l'acte signé. La finalité de la signature sécurisée est ainsi, en plus des autres finalités d'une signature (identification - authentification) de *garantir* l'intégrité du document.

Ces besoins de sécurité et de garanties s'expliquent et se justifient pleinement dans un univers numérique ouvert pour des échanges à distance entre personnes ne se connaissant pas.

Comme nous venons de le voir, l'établissement d'un acte authentique électronique se situe

---

[78] Il est pourtant des situations où cette signature électronique sera *très difficile* à apposer mais il serait souhaitable que **ces cas soient exceptionnels et strictement délimités à certaines catégories d'actes**.

M. Henry-Bonniot[78] donne comme exemple, la pratique de l'ordonnance sur requête (du TGI, du TI) qui amène les avocats à présenter un projet d'ordonnance avec leur requête. Comment signer électroniquement un document qui n'émane pas de son propre système informatique ?

D'autre part, l'ordonnance sur requête est exécutoire au seul vu de la minute, ce qui implique que cette minute est remise à l'avocat ; mais le tribunal, qui doit conserver un « double », ne peut avoir qu'un « double » authentique, c'est-à-dire une minute, puisqu'aucun greffier n'intervient dans l'élaboration de la décision.

La double signature est la réponse communément appliquée par les tribunaux judiciaires. En matière d'injonction de payer, la force exécutoire de l'ordonnance varie dans le temps. La minute, en pratique mise au bas de la requête accompagnée des pièces, est conservée au greffe et deux copies sont remises au créancier. L'une d'elles recevra la formule exécutoire si dans le délai d'un mois de sa signification il n'y a pas eu d'opposition (1410 NCPC).

dans un tout autre contexte.

*** Les conditions de l'article 1316-4 appliquées à la signature électronique de l'acte authentique**

La présence de l'officier public est une exigence, au titre des solennités requises, et la présence des parties (ou de leurs représentants) aussi.

On distinguera, donc, la signature électronique de l'officier public de celle des parties.

*** La signature électronique de l'officier public**

En ce qui concerne la signature de l'officier public, celle-ci doit attester non seulement de son identité mais aussi de son pouvoir de conférer l'authenticité à l'acte. Il faut que la signature permette cette identification et qu'elle soit apposée de façon à garantir le lien avec l'acte. Elle est un élément de l'acte et ne doit pas pouvoir être dissociée de celui-ci.

Il ne fait pas de doute qu'il est souhaitable que d'une façon ou d'une autre, l'accès aux moyens matériels et informatiques permettant l'apposition de la signature soit contrôlables et contrôlés afin qu'il n'y ait pas de risques d'utilisations abusives de la signature.

Le contrôle peut s'entendre a priori (gestion des mots de passe, autorisation d'accès, contrôle biométrique, carte à puce), ou a posteriori (dépôt de spécimen, traçabilité des opérations).

Il s'agit de la même logique que celle qui préside aux dépôts de signature des officiers publics.

*** La signature électronique des parties**

Pour les parties, quelle que soit la technique de signature, c'est l'officier public « qui garantit le lien entre la signature et l'acte auquel celle-ci s'attache ». C'est aussi lui qui identifie les parties et qui atteste de leur identité. La présence de l'officier public et l'action de vérification qu'il va mettre en œuvre pour s'assurer de l'identité de la personne qui va signer peuvent-elles être considérées comme un «procédé fiable[79]». Certains pourraient penser que par «procédé» on entend uniquement procédé technique ou industriel. Ce serait réduire les capacités de la loi à laisser ouverte les interprétations. Dans le dictionnaire Robert «procédé» signifie «méthode employée pour parvenir à un certain résultat» (sens 2). L'officier public - de par sa fonction - a reçu «l'onction de la puissance publique»[80] pour conférer à un acte authentique la force probante qui est la sienne. Sa présence physique active et l'exécution de sa mission de vérification constituent bien un procédé qui remplit les conditions de fiabilité fixées par la loi[81].

Quels que soient les moyens techniques utilisés (simple numérisation des signatures, tablette graphique, écran tactile, carte à puce…) les conditions de l'article 1316-4 sont ainsi remplies du fait même de la présence de l'officier public.

3.2.3 - La signature électronique sécurisée appliquée aux actes authentiques

Comme on a pu le souligner ci-dessus, la signature électronique sécurisée apporte des garanties sur l'intégrité du document. Il est donc tout à fait envisageable que ces garanties soient considérées comme une précaution pour prévenir des risques de modifications volontaires ou involontaires lors de la circulation ou la communication des actes authentiques. Est-ce nécessaire aussi pour les actes authentiques consignés chez l'officier public qui en assure la garde ? La réponse à cette question doit être traitée en fonction du contexte (conditions de circulation de ceux-ci) et il semble difficile de prévoir pour l'ensemble des actes authentiques une obligation générale de recourir à l'un des procédés de signature sécurisée. Ce ne peut-être, alors, qu'une question relevant des décrets particuliers au même titre que la transposition au support électronique des règles imposées pour les registres papiers.

[79] Art 1316-4 du Code civil.

[80] Voir J.- M. Olivier, op. cit., p. 14.

[81] Art. 1316-4.

Recours à une signature électronique sécurisée ne veut pas dire - obligatoirement - application du régime (mis en place par le décret du 31 mars 2001) relatif à la fourniture de services de certification électronique.

Si pour certains types d'actes authentiques la signature sécurisée est considérée comme apportant la réponse à un besoin, *on voit mal un tiers certificateur privé intervenir pour vérifier la signature d'un officier public*. Seul un opérateur public pourrait être admis à émettre le certificat qualifié d'un officier public. Les officiers publics ont pour mission de délivrer l'authenticité au nom de la République et du peuple français, sous le sceau de l'Etat et il paraît donc invraisemblable de faire certifier leur signature par un opérateur privé. La présence d'un opérateur technique ne saurait déposséder la puissance publique du contrôle exclusif sur l'acte qui lui incombe.

Pour les huissiers de justice, les notaires, ou les greffiers des tribunaux de commerce, cette fonction pourrait être confiée à la Chambre nationale des huissiers, au Conseil supérieur du notariat ou au Conseil national des greffiers[82]. Pour les juridictions et l'état civil, la Chancellerie jouerait le rôle de certificateur. Ces différentes institutions pourraient être assistées par un technicien (maison) ou prestataire externe qui délivrerait les clés sur ordre.

Enfin, la signature électronique répondant aux critères du décret de transposition de la directive [83] peut-elle être envisagée dans une perspective à long terme ? Le sous-groupe de travail sur les aspects techniques insiste sur le fait qu'aujourd'hui, tant les questions techniques (encore mal résolues) qu'organisationnelles ne permettent pas d'envisager un recours systématique aux techniques d'infrastructures à clés publiques sans hypothéquer l'avenir des signatures. Nous reviendrons sur ce point dans la suite de ce rapport relatif à la conservation des actes authentiques électroniques en en tirant les conséquences.

En conclusion

[82] On renverra sur ce point au compte rendu de la visite effectuée le 4 janvier 2001 au Conseil national des greffiers des tribunaux de commerce, compte rendu établi par F. Banat-Berger, in Rapports particuliers.

[83] Exemples étrangers :

Il est utile ici de dresser un bref panorama de la signature électronique dans les lois nationales qui ont pour but la transposition de la directive, dans l'hypothèse où la signature électronique de l'acte authentique répondra à ses critères.

Deux approches différentes étaient possibles pour chaque législateur. La première est dite technique, la seconde prône la neutralité technique et s'attache aux fonctions et aux effets de la signature.

Concernant la première approche, l'Allemagne a été l'un des premiers pays au monde à consacrer la signature digitale. Le législateur allemand considère qu'il est préférable au vu de l'expansion continue de nouvelles techniques d'opter pour un procédé connu et qui offre les meilleures garanties à l'heure actuelle de fiabilité et de sécurité. D'autres pays ont retenu les mêmes solutions (Italie, Etat d'Utah) mais seule l'Allemagne est allée jusqu'à l'ériger en norme standard, seule apte à répondre aux critères réglementaires et à produire des effets légaux. Enfin, les lois japonaise ou néerlandaise reconnaissent que la signature digitale combinée à la certification constitue actuellement le procédé pouvant inspirer et assurer confiance et sécurité dans les échanges électroniques, sans toutefois la consacrer légalement afin de ne pas restreindre le champ à cette seule technique.

A l'instar des règles uniformes de la CNUDCI, des dispositions de la directive ou de la loi de l'État de Singapour, la seconde approche consiste à osciller entre, d'une part, un plancher minimal d'exigences légales pour reconnaître à la signature électronique certains effets légaux (approche dite minimaliste) et, d'autre part, reconnaître une plénitude d'effets (c'est-à-dire équivalents à ceux de la signature manuscrite) à certains procédés fiables de signature dite avancée. A l'heure actuelle, une telle signature dite avancée renvoie à la signature digitale certifiée mais cette méthode laisse le champ ouvert au développement de tout autre technique future respectant ces conditions. Une certaine flexibilité et adaptabilité sont donc ici préservées et permettent d'appréhender l'évolution des techniques (voir par exemple la rapide évolution des techniques de paiement sur l'internet) sans recourir fréquemment à des « toilettages » des textes.

S'agissant des garanties offertes par la certification et des conditions de son exercice par les prestataires de services, la majorité des Etats membres se contente de transposer assez fidèlement la directive. Qu'ils soient publics ou privés, ces certificateurs relèvent le plus souvent, quant à leur accréditation et au contrôle de leur exercice, d'une autorité publique (soit directement le ministère compétent, soit une administration autonome indépendante). Les conditions de la certification et des prestataires participent à assurer la fiabilité des procédés de signature et l'intégrité et la confiance dans les transactions électroniques. En l'état actuel de ces législations, de nombreux enseignements peuvent être retirés pour être étendus, le cas échéant, à la signature de l'acte authentique électronique.

* Organiser le contrôle a priori ou a posteriori du pouvoir de l'officier public de signer et d'authentifier l'acte est une garantie nécessaire pour qu'il n'y ait pas de risques d'utilisation abusive de signature.
* Si pour des raisons de sécurité, il est prévu pour certaines étapes de la vie de l'acte authentique particulier l'usage d'une signature électronique sécurisée, le certificat ne pourra être donné que par un organisme public ou une chambre professionnelle ou encore l'administration.
* Si la signature électronique sécurisée répond aux besoins générés par les risques de modification, il faut aussi prendre en compte la question de la pérennisation des signatures électroniques sécurisées qui soulèvent de nombreuses interrogations et incertitudes.

3.3 - Formalisation du document électronique et statut des originaux et des copies

La rédaction des actes authentiques est soumise à des formalités qui varient d'un acte à l'autre. Celles-ci ont pour fonction d'assurer un certain nombre de garanties.

Elles devront être aménagées et adaptées dans les décrets particuliers relatifs à chaque type d'acte. Néanmoins, certaines questions communes méritent une réflexion transversale sur laquelle le groupe de travail souhaite attirer l'attention.

Il s'agit, en premier lieu, de la présentation spatiale (à l'écran ou sur un support) des informations contenues dans un acte authentique électronique ; en second lieu, du statut des originaux et copies des actes authentiques électroniques.

Ces réflexions ouvriront sur la nécessité d'intégrer à l'acte certaines données et informations qui renseignent sur les conditions d'établissement de cet acte. Enfin, les risques induits par les supports informatiques invitent à prendre en considération des précautions spécifiques (sauvegarde).

3.3.1 - La formalisation spatiale des actes authentiques

On peut se demander si ce qui importe c'est uniquement le contenu des informations de l'acte authentique ou si il faut aussi attacher une importance à la façon dont ces informations sont présentées. Cette question est, bien entendu, fondamentale quand les contraintes de présentation relèvent du formalisme imposé par les textes.

A titre d'exemple, dans le formalisme imposé aux actes notariés (art. 9 du décret de 1971), les actes doivent être écrits en un seul et même contexte dans sans blanc. De même, l'indication selon laquelle la signature du notaire sur les grosses et exécutions doit être apposée à la dernière page (art. 15, al. 4). On mesure combien la question est cruciale quand certains éléments essentiels de l'acte authentique électronique - comme la signature - sont difficilement appréhendables quand ils sont apposés par un code. Ne faut-il, comme sur un support traditionnel, retrouver un signe ou une marque qui indique que la signature a bien été apposée et où elle a été apposée ?

Le fait même de poser la question pourrait être considéré par certains comme une confusion entre l'acte électronique et sa représentation papier. Cette question a soulevé de nombreux débats dont on peut tirer les conclusions suivantes.

Il est vrai que la garantie que l'identité du signataire comme le lien entre la signature et le contrat sont assurés par la présence de l'officier public. Il est vrai aussi que le formalisme dans la rédaction des actes authentiques est un moyen de s'assurer que ces actes n'ont pas été modifiés. La signature électronique sécurisée peut apporter cette même garantie. Toutefois, garantir la "lisibilité" externe de la signature électronique comme aménager l'organisation spatiale de l'acte sont non seulement des moyens de rassurer mais aussi des moyens de faciliter la lecture de l'acte en aidant le lecteur à trouver ses repères.

La "lisibilité" de la signature peut être nécessaire pour distinguer le simple acte préparatoire numérisé et non encore signé et l'acte authentifié par la signature de l'officier public. On peut alors envisager - comme l'a suggéré le Conseil supérieur du notariat en France, d'assortir l'acte signé de marques distinctives pour faciliter la reconnaissance des actes authentiques. Ce pourrait être, suivant les cas, une image numérisée ou scannée de la

signature manuscrite ou un signe correspondant au sceau de l'Etat.

La formalisation spatiale de l'acte authentique électronique contribue, ainsi, à répondre à une demande de sécurité juridique légitime.

3.3.2 - Originaux et copies des actes authentiques électroniques

Comment déterminer quel est l'original d'un acte authentique électronique ? Quel est le statut des différentes copies ?

Si on se réfère aux catégories des actes authentiques sur support papier, à l'examen des conditions d'élaboration et d'opposabilité des différents types d'actes, on constate que les règles varient selon les actes. Toutefois, il apparaît qu'une même approche pourrait être recommandée pour l'ensemble des actes authentiques.

En premier lieu, l'esprit de la loi du 13 mars 2000 invite à prendre une certaine distance par rapport au support papier ou électronique. **La qualité d'original ou de copie ne doit pas dépendre de la nature du support.**

En second lieu, l'original comme la copie seront les documents désignés comme tels par l'officier public qui a la charge de l'établissement et de la conservation de l'acte. L'original restera sous le contrôle de l'officier public. Les copies authentiques et exécutoires seront celles reconnues comme telles pour remplir leurs fonctions.

L'article 1335 du Code civil pourra s'appliquer et en cas de disparition de l'original, *la valeur probatoire de la copie dépendra des conditions dans lesquelles elle aura été établie* (tirée de l'autorité du magistrat, établie par l'officier public qui est dépositaire de l'original...)

Cette solution permet de tenir compte des situations très diverses et de la mixité des supports.

C'est l'officier public qui est garant de la conservation des registres ou des minutes. On pourra alors avoir un original électronique :

- que l'acte original ait été établi initialement sur un support électronique ;
- que l'original soit le résultat d'une numérisation postérieure avec validation par l'officier public de cette numérisation ;
- que l'original soit le résultat d'une migration validée par l'officier public qui vérifie la fidélité de celle-ci.

On mesure, une fois de plus l'importance des informations relatives aux conditions d'établissement de l'acte

3.3.3 - Les informations sur les conditions d'établissement de l'acte

Que ce soit pour apprécier la véracité de l'acte ou pour déterminer le statut du document, les informations sur les conditions d'établissement sont indispensables. Elles doivent accompagner l'acte durant sa vie, être éventuellement intégrées à celui-ci, être conservées avec lui.

Ces informations doivent porter sur la nature de l'acte, l'identification de l'officier public, sa sphère de compétence, la date d'apposition des signatures et les conditions dans lesquelles celles-ci ont été apposées. Doit aussi être mentionné le statut du document (original, copies authentiques, titre exécutoire, extraits....).

3.3.4 - La nécessité des copies de sauvegarde

Cette dernière question sera reprise dans la partie consacré à la conservation. Toutefois, il convient de rappeler d'ors et déjà le rôle de sauvegarde que jouaient les doubles registres pour les actes de l'état civil.

Ne faudrait-il pas généraliser l'obligation de sauvegarde régulière y compris éventuellement sur des supports autres qu'électroniques ?

En conclusion, le groupe ouvre des pistes qui pourront être approfondies :

* Sur la présentation de l'acte ainsi que la lisibilité des signatures (de l'officier public comme des parties, manifestée par un signe ou un sceau) qui doivent être prises en considération.

* Sur la qualité d'original ou de copie qui ne dépend pas du support mais des conditions dans lesquelles ces originaux ou copies ont été établis.
* Sur le fait que l'acte authentique électronique devrait être accompagné d'un certain nombre de données renseignant sur les conditions dans lesquelles il a été établi.
* Sur l'établissement de double registre et de copies de sauvegarde (dès l'établissement de l'acte authentique électronique) qui répond plus que jamais à une nécessité.

4 - "La vie" des actes authentiques électroniques

Seront traités successivement la communication des actes authentiques électroniques et l'apposition de mentions.

4.1 - La communication des actes authentiques électroniques

4.1.1 - La délivrance des copies authentiques et des extraits des actes authentiques

Qui délivre ?

En principe, la délivrance des copies ou d'extraits relève de la compétence de l'officier public qui conserve l'acte d'origine [84]. Faut-il maintenir ce principe pour les actes authentiques électroniques ?

L'informatisation de l'état civil et le souci de faciliter le service aux citoyens ont d'ores et déjà incité plusieurs collectivités locales à organiser une base de données centrale et des accès déconcentrés dans des mairies annexes. Toutefois, on se trouve toujours dans ces cas dans la même entité territoriale.

Selon l'avis du Notariat, la nouvelle loi ne change rien à la règle et ce qui est valable pour des actes sur support papier doit être étendu aux actes sur support électronique [85].

L'acte authentique électronique pourrait-il être une occasion de revoir le principe de la compétence territoriale, du moins pour la délivrance des copies ? La réponse à une telle question dépasse le cadre de la mission qui a été confiée au groupe de travail (cf. supra). Toutefois, il convient de rappeler que la délivrance de copies et d'extraits relèvent des prérogatives de l'officier public qui les a conservés. Si le cas échéant une réorganisation de la conservation des actes est mise en place (sous forme d'une base de données centralisée), il serait souhaitable que l'officier public puisse avoir accès à la base de données et "puiser" dans cette base l'extrait ou la copie authentique qui lui est demandé. Il pourrait ainsi délivrer en son nom cet extrait ou cette copie.

*** Les relations inter-administration et/ou interprofessionnelles : de l'importance des réseaux sécurisés**

En ce qui concerne les actes de l'état civil, on constate que de très nombreuses demandes sont liées à la demande d'une administration ou d'une organisation professionnelle. Ne pourrait-on pas développer au maximum les relations administration à administration (par réseau sécurisé) pour l'échange des actes [86] ? Toutefois, il faudrait veiller à ce que les droits des particuliers soient respectés : *droit d'accès à l'information les concernant, droit de vérifier si les informations fournies sont exactes, que ces informations doivent bien être communiquées, qu'elles sont nécessaires pour le destinataire final* .

Selon les huissiers, on a déjà souligné l'intérêt de l'acte authentique électronique qui permettra des relations plus rapides avec d'autres huissiers de justice ou des demandeurs (avocats ou autres) notamment dans des procédures aux délais courts [87].

---

[84] Ce principe s'applique aux greffes, aux notaires comme à l'état civil.

[85] Ce principe s'applique en vertu de l'article 17 du décret n° 71-941 du 26 novembre 1971.

[86] Ce qui repose le problème de la compatibilité des produits ! Voir particulièrement les développements du rapport du sous-groupe "Sécurité et conservation",in Rapports particuliers.

[87] Saisie attribution et dénonce, saisie conservatoire et dénonce, saisie des coffres - délai de 1 jour - notamment.

Selon les notaires, la copie authentique [88] de l'acte authentique électronique devrait pouvoir être envoyée uniquement par intranet, et aux seuls professionnels directement concernés (registre du commerce et des sociétés, conservation des hypothèques). Ces modalités s'imposent pour garantir la confidentialité du document et la sécurité de l'échange.

Enfin les décisions de justice pourraient être délivrées par le biais de réseaux sécurisés aux destinataires (avocats, huissiers..).

*** Peut-on envisager une délivrance par les réseaux aux particuliers ?**

Une telle perspective pourrait présenter des avantages : coût réduit, meilleur service à l'usager (service à domicile). Toutefois, en principe, la communication des copies ou extraits d'actes authentiques ne doit se faire qu'après un contrôle de la qualité du demandeur et des raisons de sa demande par l'officier public, ceci afin de limiter la fraude.

Pour les membres du groupe de travail, autant les échanges inter-institutions semblent opportuns, autant il semble prématuré d'envisager d'autres solutions que celles qui sont pratiquées aujourd'hui.

Toutefois, pour faciliter les services de proximité, la copie (ou l'extrait) des actes d'état civil, pourrait être envoyée à la mairie du domicile du demandeur par un réseau intranet, ou la copie authentique de l'acte notarié au notaire le plus proche du domicile du demandeur.

Enfin, les exemples étrangers [89] invitent à réfléchir sur les possibilités de la mise en place d'une carte à mémoire état civil (type "carte Vitale" ou en liaison avec la "carte vitale") attribuée à chaque citoyen lui permettant de suivre l'évolution de son registre de l'état civil et de s'auto-délivrer des copies ou extraits. Si aujourd'hui, la suppression des fiches d'état civil procède d'une même logique de simplification pour les usagers, reste le problème du contrôle de la finalité de la sortie de ces extraits et surtout de la fiabilité de la mise à jour de la carte ?

[88] La minute de l'acte notarié n'est pas appelée à circuler sauf le cas très rare des actes dits en brevet. Ces brevets peuvent être remplacés par une copie authentique.

[89] L'expérience espagnole démontre que son administration générale dispose de l'infrastructure juridique et technique nécessaire à l'utilisation de moyens électroniques dans les relations entre ses différents organismes et entre ces services et les administrations des provinces autonomes.

Le même schéma existe dans les relations entre administrations et administrés. Ainsi la résolution du Ministre du Trésor du 13 avril 1999 a mis en place les conditions et la procédure de déclaration de l'impôt sur le revenu pour l'année 1998 par voie électronique sécurisée au moyen de la signature électronique reposant sur une infrastructure à clés publiques. Ce processus existait déjà pour la déclaration par les entreprises.

En conclusion

* Ces questions dépassent la mission du groupe de travail, toutefois celui-ci souligne l'intérêt de mener une réflexion acte par acte sur les modes de communication et de circulation.
* Le groupe souhaite par ailleurs rappeler l'importance du développement de réseaux sécurisés entre institutionnels. Il reste réservé sur la délivrance directe aux particuliers via les réseaux. Toutefois, les institutionnels (notaire, mairie) proches du domicile du particulier pourraient servir d'interface pour la délivrance des actes.

4.1.2 - La gestion des flux d'actes authentiques mixtes (papier/électronique)

Dans la mesure où il s'avère indispensable de laisser la possibilité de maintien d'actes authentiques sur différents types de support, on doit pouvoir résoudre la question d'une circulation de ces documents, c'est-à-dire une chaîne de transmission qui passerait de l'électronique au papier vice-versa.

Directement confrontée au problème (avec l'envoi de jugement ou de pièces qui seraient sur support papier), la Chambre nationale des huissiers [90] suggère le recours à la scanérisation qui permettrait de joindre l'image du document papier à l'acte authentique électronique. Dans ce cas, l'authentification par l'officier public apporterait les garanties requises. Toutefois la circulation de ce type de document ne pourrait se faire que dans des réseaux fermés et sécurisés.

Un aménagement des flux d'actes authentiques ou des modes de circulation relève des règles propres à chaque type d'acte. Ces questions pourraient être reprises dans les décrets particuliers, le décret général ayant rappelé les principes de la délivrance et de la conservation.

4.2 - L'apposition des mentions

Comment bénéficier des facilités offertes par l'électronique pour améliorer la gestion des mentions marginales ? Cette question se pose, de façon cruciale, particulièrement pour les actes de l'état civil. Elle existe aussi pour d'autres types d'actes authentiques.

On distinguera l'envoi des mentions (1) et l'apposition de celles-ci (2).

4.2.1 - L'envoi des avis de mentions

Si un réseau intranet sécurisé peut être mis en place, l'envoi des avis de mentions marginales pourrait se faire via ce réseau de même que l'accusé de réception d'apposition des mentions. Il faudra aussi accompagner cette mise en place d'une normalisation des présentations afin que l'économie réalisée permette aussi d'éviter une re-saisie.

4.2.2 - L'apposition des mentions

Pour l'état civil, la coexistence des deux supports (papier et électronique), sur lesquels sont enregistrés les mentions, est ressentie durement en termes de charge de travail et de lourdeur de la procédure. Il serait souhaitable, si les systèmes mis en place offrent les garanties, que - comme cela a été mis en place au SCEC du MAE à Nantes - les mentions soient uniquement apposées sur la base de données numérisées. Il faudra ensuite régler la question des sauvegardes (voir infra).

Selon les huissiers, le visa des mentions de signification (faites par le clerc assermenté) se fait au retour de l'acte signifié par l'huissier lui-même en son office. Quant aux mentions de délivrance de l'acte, elles sont intégrées à l'acte, et font partie intégrante de celui-ci.

Selon les notaires, les mentions marginales - plus rares [91] - doivent évidemment être apposées sur la minute de l'acte et c'est un des rôles de l'officier public. Pour l'instant rien n'a

[90] Voir, in Rapports particuliers, Contribution de la profession d'huissier de justice.

[91] Par exemple : mentions sur la minute des actes de la création de copies exécutoires, mention d'un changement de régime matrimonial sur la minute du contrat de mariage.

été précisé sur les modalités de cette apposition sur une minute électronique dans le cadre du projet REAL.

En conclusion

* La circulation et le traitement des mentions devraient pouvoir être réglés par les décrets particuliers à condition que des garanties appropriées soient apportées sur les réseaux sur lesquels celles-ci seront appelées à circuler.

5 - La conservation des actes authentiques électroniques [92]

La question de la conservation peut apparaître comme un problème "classique" qu'il faut régler, principalement, en tenant compte de sa finalité. Ne rencontre-t-on pas des problèmes techniques pour la conservation des registres papiers ?

Le Conseil supérieur du notariat rappelle à juste titre que la notion de conservation est la même quel que soit le support, et que le souci de la pérennité de l'acte et de son intangibilité (ou intégrité) se trouvent déjà dans les décrets actuels [93].

Pourtant, la logique de l'usage de l'électronique invite, aussi, à penser autrement la conservation sans transposer, obligatoirement, à ce nouveau support les catégories du papier.

Pour la Direction des Archives de France, le passage à l'acte authentique électronique ne remet-il pas en cause profondément la structure institutionnelle de la politique de l'archivage (y compris en termes techniques et financiers) [94] ? Comment traiter les problèmes d'archivage et de conservation des actes électroniques avec les mêmes répartitions de compétence et les mêmes règles qu'aujourd'hui ? En effet, l'officier public est tenu, de par la loi, d'assurer la conservation des actes pendant 100 ans pour les notaires, 30 ans pour les minutes des jugements, 150 ans pour les registres d'état civil dans les mairies. Au-delà des durées mentionnées ci-dessus, la responsabilité définitive de l'archivage relève de la compétence des Archives de France, chargées de la conservation des actes authentiques pour une durée illimitée. Avant que cette responsabilité définitive revienne aux Archives, l'officier public est-il à même d'assurer la pérennité des systèmes permettant les mises à jour, la communication et la conservation ? Avec quels moyens ?

Ces questions, si elles ont un lien avec l'établissement et la conservation des actes

---

[92] Exemple étranger sur les archives électroniques du notariat autrichien

Un parallèle avec l'initiative du notariat autrichien, seule expérience étrangère véritablement aboutie en la matière, est intéressant (sachant qu'il n'y a qu'environ 200 notaires en Autriche).

Le 1er janvier 2000 est entré en vigueur en Autriche un dispositif réglementaire original pour la mise en place d'archives électroniques pour les actes authentiques. Ces archives sont conçues et organisées par la Chambre du Notariat autrichien en collaboration avec une entreprise privée de matériels de télécommunications.

La finalité de ces archives est l'enregistrement et la conservation électroniques des actes authentiques notariés, des autres actes authentiques publics et des actes privés écrits ou portant des signatures électroniques sécurisées. Ce système privilégie la centralisation et la coexistence transitoire du papier et de l'électronique.

Sa mise en œuvre se décompose en trois temps.

Tout d'abord, pour tout nouvel acte reçu (c'est-à-dire les actes notariés reçus à partir du 1er janvier 2000), coexisteront l'archive papier avec son double scanné puis archivé électroniquement.

Ensuite, l'archivage des actes sera centralisé. Pour ce faire, les notaires utiliseront le procédé des signatures électroniques sécurisées au moyen duquel ils certifieront la conformité des données de l'acte électronique avec l'original (par carte à puces ou code secret). De plus, afin de garantir la confidentialité et la sécurité des données, le cryptage de l'acte s'effectuera directement sur l'ordinateur de l'étude. Le document électronique sera alors envoyé directement aux archives centrales et conservé électroniquement.

Enfin, l'objectif est de ne conserver les archives notariales que sous la forme électronique exclusivement.

S'agissant de la consultation, celle-ci pourra se faire directement par la voie électronique. Mais la question se pose de savoir si la délivrance d'extraits ou de minutes se fera en toute sécurité par cette même voie électronique ou nécessitera un envoi par courrier.

De nombreux commentateurs de lois nationales regrettent que la question de la conservation ne soit pas envisagée au même titre que l'établissement ou la circulation des actes sur support électronique et considèrent qu'il s'agit d'un enjeu incontournable à l'avenir.

[93] Voir par exemple l'article 7 du décret de 1971 relatif aux actes établis par les notaires.

[94] Voir, in Rapports particuliers, Remarques de la Direction des Archives de France..

authentiques, ne peuvent, pour autant, être traitées que de façon incidente dans un décret général relatif à la preuve des actes authentiques électroniques. Elles entrent dans le cadre d'une réorganisation de la politique de conservation et d'archivage dans la société de l'information. Néanmoins ces différents textes, tout en gardant leur logique propre doivent être fondés sur une approche commune à celle du droit de la preuve, afin que les solutions proposées trouvent de part et d'autre leur cohérence. C'est la raison pour laquelle ce rapport consacrera de longs développements à cette question. Ces développements aideront à appréhender le besoin de ne pas hypothéquer l'avenir des actes authentiques. Les impératifs de la conservation à long terme peuvent-ils, ainsi, orienter les modalités d'établissement de l'acte authentique ? Comment ? Quelles conséquences doit-on en tirer dans le décret général ?

On examinera donc les modalités relatives à l'établissement des actes authentiques qui pourraient soulever des difficultés de conservation. C'est la pérennité d'une signature électronique sécurisée utilisant le procédé de cryptographie à clés publiques qui retiendra, particulièrement notre attention compte tenu des conséquences à tirer si ce mode de signature pose des problèmes de conservation.

La réorganisation institutionnelle des fonctions de stockage et d'archivage mérite aussi d'être traitée dans la mesure où elle relève des problèmes spécifiques à chaque type d'actes.

5.1 - Les interactions entre l'établissement et la conservation des actes authentiques électroniques

Pour la phase de conservation à long terme, la difficulté réside dans l'inconnu que présente aujourd'hui l'avenir des supports électroniques. Il faut en assurer une *lisibilité* pérenne à l'acte authentique électronique alors que les instruments informatiques utilisés pour le créer, et le décoder ont disparus.

Les réflexions qui suivent, déjà en germe dans les premières versions du rapport, ont été nourries par des travaux postérieurs [95] qui s'appuient à la fois sur des considérations pragmatiques et sur les incitations à la prudence qui se multiplient dans les milieux scientifiques concernés pour relativiser l'impact de certaines techniques, comme celle utilisée pour la signature cryptographique à clés publiques. Si elles apportent des garanties pour répondre aux risques induits par ceux qui voudraient modifier de façon malveillante des documents, elles ne permettent pas de répondre aux contraintes induites par l'archivage à long terme.

Si dans l'état actuel de la technique, la pérennité du document peut être assurée par une migration des formats d'encodage liée à un saut technologique, cette pérennité est plus problématique si le document a été "signé" avec un mécanisme de signature électronique sécurisée de type cryptographique. Dans ce cas, il faut assurer non seulement la lisibilité du document mais de plus assurer la pérennité du dispositif de vérification de signature.

Sans entrer dans des considérations techniques, la difficulté réside dans le fait que le processus de migration invalide nécessairement la signature cryptographique qui y est associée. En effet le système de vérification de signature ne peut faire de distinction entre une modification malhonnête et une modification résultant du processus de migration. Face à cette difficulté on se trouve devant le dilemme suivant :

* soit on veut assurer la conservation d'un document lisible, il faut alors détruire la signature qui y est attachée ;
* soit on veut assurer la conservation de la signature et le document archivé sera inintelligible pour les générations futures.

Plusieurs types de solutions ont été proposées pour résoudre ce dilemme. Mais aucune ne permet d'assurer une garantie de pérennisation de la signature de celui qui a authentifié l'acte en le signant.

Certains proposent des "resignatures" ou "sursignatures" mais ce ne sont pas celles de l'origine et même si un nouvel officier public authentifie l'intégrité et la fidélité du document

[95] Voir les développements de J.-F. Blanchette (annexe II). Les remarques sur les aspects techniques sont directement tirées de ses réflexions au sein d'un petit groupe de travail interne au CECOJI.

sur son nouveau support, on ne dispose plus de la signature d'origine. D'autres suggèrent la mise en place de systèmes d'archivage centralisés qui apporteront des garanties quant à la fidélité des migrations mais ne résoudront pas la difficulté de conservation de la signature initiale.

Enfin, la solution des formats "canoniques" correspond à des normes qui permettraient grâce à un *pré-traitement* de rendre moins vulnérables les documents aux transformations du format d'encodage. Malheureusement ces solutions n'offrent qu'une solution à court terme au problème de la pérennité des signatures cryptographiques.

Il semble donc essentiel, dans le cadre d'une politique d'archivage responsable de tenir compte de ces aléas. Ces incertitudes peuvent aussi avoir des incidences sur les propositions relatives aux conditions d'établissement de l'acte authentique électronique.

En conclusion :

* Il faudrait reconnaître que la fonction qui assure l'intégrité de l'acte doit être, pour les actes authentiques, dissociée de la fonction de signature proprement dite.
* En conséquence, le décret fixant les conditions d'établissement et de conservation de l'acte authentique doit pouvoir rendre indépendante la signature électronique de l'usage de tout procédé de sécurité dont la conservation à long terme est hypothétique.
* L'acte authentique électronique pourrait, alors, être conservé pour les générations futures avec une signature électronique qui est celle de l'origine et qui constitue l'un des éléments substantiels de cet acte.
* Enfin, il faudrait recommander l'usage de la signature cryptographique pour ce pour quoi elle a été conçue, principalement, apporter des garanties que le document n'a pas été modifié. La signature cryptographique viendrait alors se surajouter à la signature électronique.

5.2 - La réorganisation institutionnelle des fonctions de stockage et d'archivage

5.2.1 - La réorganisation institutionnelle

*** Pour une centralisation dès la phase d'établissement des actes authentiques électroniques**

Pourquoi pas un service central de l'état civil sur le modèle du service central état civil du MAE à Nantes ? Cette possibilité qui a été proposé par certains membres du groupe de travail doit être examinée dans la mesure où elle peut avoir des incidences sur la conservation des actes authentiques électroniques. Les possibilités d'une centralisation de l'état civil faciliteraient l'accès à toute instance publique autorisée. De plus l'usager n'aurait à s'adresser qu'à un seul service chargé de l'état civil en France.

Pour le Conseil supérieur du notariat, il sera aussi souhaitable de mettre en commun, à l'échelon régional, voire même national, les moyens et les systèmes de stockage et de reproduction des actes notariés. Des raisons financières plaident aussi en faveur d'une solution collective, la maintenance technologique pouvant représenter un coût important.

La Direction des Archives de France pose, aussi, la question du moment où doivent être transférés les registres dématérialisés. Faut-il transposer les délais prévus pour le papier qui se justifiaient à une époque où l'on voulait éviter des allers et retours entre le « producteur » et le service central des archives ? Les délais d'utilité administrative ont-ils encore leur raison d'être ?

Poursuivant son raisonnement, la Direction des Archives de France suggère que l'acte authentique dématérialisé soit transféré et « archivé » dès sa « validation », à savoir son authentification, par l'officier public. Ce transfert permettrait de reporter sur un seul service, ou un nombre limité de services, les problèmes de *compatibilité* [96] entre les différents systèmes (logiciels à faire agréer par ce service, qui imposerait un certain nombre de recommandations

[96] Voir infra les recommandations sur l'établissement des actes authentiques.

quant à l'architecture des systèmes et le format des actes).

Cette position, séduisante pour gérer correctement l'archivage, ne tient pas compte de la vie de nombreux actes ou des missions propres aux officiers publics. On ne voit pas à quel titre ce serait le service d'archive qui traiterait des mentions à apposer aux actes d'état civil. Cela remet en cause le monopole de l'officier de l'état civil qui a établi l'acte. Pour pallier ces difficultés, la suggestion faite plus haut d'envoyer à intervalles réguliers au service en charge de l'archivage des versions consolidées du registre numérisé serait une possibilité de concilier les différentes missions (celle de la commune qui ne serait pas « dépossédée » de sa mission de tenir à jour l'état civil, d'effectuer les mises à jour et de délivrer des copies et celle de l'institution en charge de garantir la pérennité des actes authentiques). Une autre solution suggérée serait de donner accès à l'officier de l'état civil de la commune pour mettre à jour le registre national (ou régional, ...) ou délivrer des extraits ou des copies. Le sous-groupe de travail « Sécurité et conservation » analyse cette voie médiane en étudiant les possibilités d'un service centralisé à l'échelon régional [97] qui « externaliserait » la fonction de stockage tout en permettant à l'officier public un accès permanent aux données conservées à distance.

Le Conseil supérieur du notariat attire l'attention sur l'importance du maintien du système actuel qui confie aux notaires la responsabilité de la garde de leurs actes dans le moyen terme. Ce système permet en effet de concilier les exigences de la sécurité juridique et celles du respect de la vie privée.

La conservation des minutes par les notaires répond à une obligation juridique, celle d'apporter la preuve des actes et des engagements juridiques souscrits. Elle est un élément de la sécurité juridique que les notaires doivent à leurs clients puisqu'elle garantit l'existence des actes qu'ils ont signés ainsi que le contenu des contrats qu'ils ont fait constater ou des faits qu'ils ont révélés.

Cette sécurité à un corollaire s'agissant d'actes conclu entre particuliers et intéressant leur vie privée, leur famille et leur patrimoine : la confidentialité et l'obligation de secret. Interdiction est faite aux notaires de donner communication de leurs actes à d'autres qu'aux parties elles-mêmes ou à leurs héritiers ou ayants droit. S'agissant des actes notariés, il ne serait donc conforme ni à la tradition ni à la loi de confier à d'autres personnes qu'aux notaires le soin d'en conserver le dépôt pendant cent ans.

*** La conservation à long terme des actes authentiques électroniques : faut-il centraliser ?**

L'analyse qui suit part du présupposé qu'il n'y a pas eu de centralisation pour la conservation à long terme au moment de l'établissement de l'acte.

La structure actuelle est communale ou départementale afin de faciliter l'accès pour les citoyens. On pourrait envisager une aide et une assistance spécifiques à ces collectivités locales, sans centralisation pour assurer une conservation appropriée des actes authentiques électroniques. Toutefois, cette hypothèse ne semble pas facile à mettre en œuvre tant pour des raisons économiques que techniques.

*** Vers un archivage national ?**

La Direction générale des Archives estime qu'il serait logique et plus fiable d'établir pour le long terme un système d'archivage national disposant des moyens correspondants. Selon elle, il pourrait s'agir d'un établissement spécifique sous la tutelle des Archives de France. Les notaires estiment que, pour des raisons financières et technologiques, il serait opportun de constituer pour les premiers cent ans pendant lesquels ils sont directement en charge de la conservation des actes (c'est-à-dire pour le moyen terme) un minutier électronique centralisé sous leur responsabilité qui assurerait la maintenance technologique de la conservation des actes électroniques (cf. supra). Ce minutier pourrait être ouvert aux autres actes authentiques. Il sera toutefois utile que les procédés technologiques et les procédures qui seront adoptés pour l'archivage des actes notariés électroniques soient établis en concertation avec la Direction des

[97] Voir, in Rapports particuliers, Note relative à l'établissement et à la conservation des actes authentiques dématérialisés, la présentation détaillée de ce que pourrait être un schéma de ce type.

Archives de France, puisque ces actes seront transférés dans les services départementaux ou nationaux des archives au bout de cent ans. Enfin, pendant plusieurs années, afin de faciliter la transition, il est proposé qu'une copie papier continue à être établie en sus de la minute électronique de l'acte.

*** Comment concilier une centralisation qui pourrait s'avérer nécessaire et le service de proximité aux usagers ?**

Une centralisation avec accès direct des officiers publics territoriaux pourrait être alors envisagée pour le moyen terme.

Pour le long terme, il faudrait continuer à rendre possible le rôle de médiation que jouent pour les administrés et les citoyens les services d'archives communales et départementales. Ne pourraient-ils pas servir d'interface entre les demandeurs et le service central [98] ?

[98] Voir sur ce point les propositions de la Direction Nationale des Archives, in Rapports particuliers..

5.2.2 - Les incidences sur les modalités d'établissement des actes

En dehors de la question de la signature qui a été longuement étudiée ci-dessus, les conditions d'établissement des actes authentiques peuvent être amenées à évoluer en fonction de l'organisation institutionnelle de la conservation des actes authentiques.

Même si il y a eu centralisation dans la première phase de vie de l'acte, la conservation à long terme exige que des *précautions particulières* soient prises dès l'établissement de l'acte : copies de sauvegarde utilisant différents types de supports, par exemple : des disques non réinscriptibles (WORM), ou la technologie dite COM (computer output microfilm) qui permet de réaliser une image du document électronique et de la stocker sur un film.

La Direction des Archives de France attire aussi l'attention sur l'intérêt de définir, au plan national, les conditions d'élaboration de chaque type documentaire. Cela doit-il aller jusqu'à rechercher une *simplification du « charpentage »* des actes authentiques lors de leur création ?

En conclusion

* Il convient de rappeler la nécessité de tenir compte de la conservation dès l'établissement de l'acte, les besoins de la conservation pouvant conditionner, limiter et guider certains choix technologiques.
* Sans être rétrograde, la prudence invite à garder la possibilité de solutions mixtes de conservation et d'archivage associant papier et électronique.
* Toutefois les questions institutionnelles et organisationnelles ne peuvent relever du décret général et doivent être reprises soit dans des décrets spécifiques à certaines catégories d'actes authentiques soit dans des textes propres à la politique en matière d'archivage.

*** * * * ***

Comme ce rapport le montre, l'acte authentique électronique concerne de multiples acteurs : depuis les parties concernées, les officiers publics, les institutions en charge de la conservation à long terme, les informaticiens et autres professionnels des technologies de l'information.

La diversité de ces acteurs et le caractère général d'un certain nombre des questions soulevées incitent à poursuivre cette réflexion transversale. Dans quel cadre ? Une instance de concertation entre les différents acteurs serait nécessaire pour décider du bien-fondé des choix techniques et vérifier qu'ont été prises en compte tant les finalités d'établissement que de conservation. Cette instance pourrait aussi jouer le rôle d'observatoire des actes authentiques électroniques.

Quatrième partie - Quelques propositions pour le futur décret

Outre des réflexions particulières propres à chaque catégorie d'actes, c'est autour de quatre questions principales que le groupe de travail est invité à remplir une double mission de réflexion et de proposition.

1- Comment préserver les garanties de fond offertes par l'authenticité (contrôle de la réalité du consentement, information des parties...) dans le cadre d'un acte dématérialisé[99] ?

2 - Dans quelles conditions et suivant quelles modalités pourra être apposée la signature électronique de l'officier public et des parties sur l'acte authentique ?

3 - Comment assurer l'archivage et la conservation pour une durée illimitée de l'acte authentique dématérialisé ?

4 - Dans quelles conditions pourront être délivrées des copies des actes authentiques dématérialisés ? Quelle sera, alors, la force probante de ces copies ?

A travers ces questions très précises, il convient de dégager, en les transposant au droit de la preuve, quelques-unes des problématiques de fond de la régulation de la société de l'information.

Comment respecter les grands principes sur lesquels est fondé le droit de la preuve des actes authentiques ? Comment répondre aux besoins de sécurité technique et juridique ? Comment établir un cadre juridique qui réponde au besoin de sécurité technique pour lutter contre les risques engendrés par la circulation de ces actes dans l'univers numérique et qui n'hypothèque pas l'avenir en ménageant la pérennisation des actes authentiques électroniques dans un futur lointain inconnu ? Ce sont ces problématiques qui ont servi de trame à l'organisation du travail du groupe.

Une fois de plus, la société de l'information est l'occasion de relire les fondements du droit et les rappels ci-dessus nous invitent à traiter de façon rigoureuse le respect des principes posés par les textes. Ils nous invitent aussi à analyser les textes en vigueur sans créer de confusion.

Ont été analysés les points essentiels qui sont communs à tous les actes authentiques et qui en constituent les éléments substantiels :
- d'une part la présence de l'officier public sans lequel il ne peut y avoir authenticité,
- d'autre part la signature de l'acte qui est - plus qu'une solennité requise - l'une des composantes de cet acte.

Les autres solennités requises sont spécifiques à chaque catégorie d'actes authentiques. Du fait de ces spécificités, la question se pose de savoir si ces formalités spécifiques relèvent ou non du cadre du décret prévu à l'article 1317 ou dans le cadre d'une révision des décrets propres à chaque type d'acte authentique.

La présentation des expériences factuelles de numérisation appliquées aux actes authentiques nous a invité à tirer quelques réflexions transversales.

Si l'usage de l'informatique est déjà depuis longtemps le lot quotidien des officiers publics, cet usage se heurte - en l'état actuel du droit - à plusieurs interrogations pour concilier les textes et les facilités qu'offre la technique. La principale de ces interrogations réside dans la signature électronique des actes authentiques dans la mesure où les officiers publics, ne disposant pas encore du décret précisant les conditions d'établissement et de conservation des

[99] Un point de vocabulaire : Dans la logique de la loi du 13 mars 2000 qui reconnaît la valeur d'un écrit, quel que soit son support, il nous a semblé plus opportun – dans la suite du rapport et dans la mesure du possible - de parler de support informatique ou électronique pour l'acte authentique plutôt que de « dématérialisation », bien que ce terme soit culturellement associé au support informatique.

actes authentiques électroniques, maintiennent en parallèle des circuits papier et des circuits électroniques avec les risques d'erreur. En outre, on ne dispose pas encore (bien souvent [100] des réseaux sécurisés permettant un échange et un traitement de l'information. Enfin, au-delà de la saisie des registres papiers pour faciliter la vie de l'acte, la conservation et l'archivage sur des supports informatiques imposent une nouvelle logique. Quid de l'avenir à long terme des actes authentiques sur support informatique ?

Par ailleurs, tous s'accordent pour mettre l'accent sur le principe selon lequel l'acte authentique électronique ne doit pas remettre en cause ni modifier les missions fondamentales de l'officier public lors de l'établissement ou de la communication des actes.

Ces lectures, ainsi que ces expériences, sont une aide précieuse pour tirer les fils des problématiques soulevées par les questions précises posées au groupe de travail et permettent aujourd'hui de faire les propositions suivantes.

A - Questions générales

1 - Un et/ou plusieurs décrets ?

Le groupe de travail recommande à la fois la rédaction d'un décret général (en application de l'article 1317 - texte commun à l'ensemble des actes authentiques) et des décrets spécifiques à chaque type d'acte.

2 - Les finalités du décret général

Le groupe de travail recommande que :

- Le décret général puisse avoir une **fonction pédagogique** et expliciter certains principes fondamentaux de l'authenticité comme la présence de l'officier public et son rôle, dans la mesure où ces questions ne relèvent pas du domaine législatif.

- Le décret général n'ait à traiter que des **questions générales communes** (voir infra) à l'ensemble des actes authentiques entrant dans le champ de l'article 1317 laissant à des textes spécifiques les questions relevant de certains actes particuliers ou le traitement des problèmes institutionnels ou organisationnels.

- Le décret général traite des critères à prendre en compte pour assurer une normalisation et une harmonisation entre les systèmes sans aller jusqu'à recommander ou imposer **telle ou telle solution technique**.

- Le décret général devrait laisser à chacun des acteurs la possibilité d'organiser à son rythme le passage au tout électronique

- Le décret général devrait faire état de la nécessité de prendre en compte dès la phase d'établissement de l'acte des questions relevant de la pérennité de cet acte (conservation à long terme).

B - Les conditions de l'établissement des actes authentiques électroniques

1- Les solennités requises pour les actes authentiques électroniques

A propos de la présence de l'officier public

Le groupe considère que :

- Quelles que soient les facilités qu'offre le support électronique pour le recueil à distance du consentement, modifier le principe actuel de présence de l'officier public serait une remise en cause de l'authenticité de l'acte auquel le législateur n'a pas souhaité apporter de modification.

[100] Le système REAL du notariat répond à cette exigence.

- Que la présence physique de l'officier public ne peut être réduite à une simple modalité d'exécution d'une obligation. Elle fait partie de l'essence même de l'acte authentique.

- Qu'il convient d'ajouter que modifier ce principe de la présence physique pour l'adapter au support électronique, rendrait nécessaire de prévoir la même adaptation pour le support papier, afin d'éviter toute discrimination entre les supports que la nouvelle loi a bien déclarés comme étant équivalents.

A propos de la présence des parties ou du déclarant

- Il ne faudrait pas que l'utilisation de l'électronique entraîne des dérives dans l'établissement des actes authentiques : quand la loi le prévoit, la présence physique des parties (ou de ceux qui disposent de leur procuration) est indispensable au même titre que la présence de l'officier public.

- Le groupe recommande que ce principe soit rappelé dans le décret général.

A propos de l'identification des parties

- Le groupe de travail a souligné l'importance de maintenir l'obligation de l'officier public de vérifier les identités des personnes parties à l'acte, cette vérification ne pouvant être réduite à la présentation d'un certificat utilisable pour la signature électronique.

2 - La signature électronique

A travers le titre de la loi du 13 mars 2000 (portant adaptation du droit de la preuve aux technologies de l'information et **relative à la signature électronique**), on mesure l'importance attachée au concept de signature. Elle est donc au cœur du processus de l'acte authentique électronique et le groupe de travail a été invité à apporter des éléments de réponse à la question suivante :

Dans quelles conditions et suivant quelles modalités pourra être apposée la signature électronique de l'officier public et des parties sur l'acte authentique ?

Pour le groupe de travail :

- Organiser le contrôle, a priori ou a posteriori du pouvoir de l'officier public de signer et d'authentifier l'acte, est une garantie nécessaire pour qu'il n'y ait pas de risque d'utilisation abuse de signature.

- Si, pour des raisons de sécurité, il est prévu à certaines étapes de la vie d'un acte authentique particulier l'usage d'une signature électronique sécurisée, le certificat ne pourra être donné que par un organisme public ou une chambre professionnelle ou encore l'administration.

- Si la signature électronique sécurisée répond aux besoins générés par les risques de modification, il faut aussi prendre en compte la question de la pérennisation des signatures électroniques sécurisées qui soulèvent de nombreuses interrogations et incertitudes.

3 - Formalisation du document électronique et statut des originaux et des copies

Le groupe ouvre des pistes qui pourront être approfondies.

- Sur la présentation de l'acte ainsi que la lisibilité des signatures (de l'officier public comme des parties, manifestée par un signe ou un sceau) qui doivent être prises en considération.

- Sur la qualité d'original ou de copie qui ne dépend pas du support mais des conditions dans lesquelles ces originaux ou copies ont été établis.

- Sur le fait que l'acte authentique électronique devrait être accompagné d'un certain nombre de données renseignant sur les conditions dans lesquelles il a été établi.

- Sur l'établissement de double registre et de copies de sauvegarde (dès l'établissement de l'acte authentique électronique) qui répond plus que jamais à une nécessité

4 - La répartition des compétences (fonctionnelle/territoriale)

Le groupe de travail considère que les questions relatives à la compétence fonctionnelle et institutionnelle des officiers publics ne relèvent pas du champ de sa mission ni du ou des décrets concernés. Si ces points doivent être traités ce pourrait être dans le cadre d'autres textes comme par exemple, en matière de conservation à long terme (voir infra) la loi sur les archives.

C - La vie de l'acte

A propos de la communication des actes

Le groupe suggère que dans le cadre de ce décret :

- L'acte authentique électronique ne remette pas en cause la compétence de l'officier public dans sa mission de délivrance des extraits et copies des actes qu'il a établis

- Un aménagement des flux d'actes authentiques ou des modes de circulation relève des règles propres à chaque type d'acte. Ces questions pourraient être reprises dans les décrets particuliers, le décret général ayant rappelé les principes de la délivrance et de la conservation.

- Par ailleurs, il souhaite rappeler l'importance du développement de réseaux sécurisés entre institutionnels. Il reste réservé sur la délivrance directe aux particuliers via les réseaux. Toutefois, les institutionnels (notaire, mairie) proches du domicile du particulier pourraient servir d'interface pour la délivrance des actes.

A propos des mentions

- La circulation et le traitement des mentions devraient pouvoir être réglés par les décrets particuliers à condition que des garanties appropriées soient apportées sur les réseaux sur lesquels celles-ci seront appelées à circuler.

D - La conservation des actes authentiques électroniques

- La question de la conservation peut apparaître comme un problème "classique" qu'il faut régler, principalement, en tenant compte de sa finalité. Ne rencontre-t-on pas des problèmes techniques pour la conservation des registres papiers ?

- Pourtant, la logique de l'usage de l'électronique invite, aussi, à penser autrement la conservation sans transposer, obligatoirement, à ce nouveau support les catégories du papier.

- Il convient de rappeler la nécessité de tenir compte de la conservation dès l'établissement de l'acte, les besoins de la conservation pouvant conditionner, limiter et guider certains choix technologiques.

A propos des supports de conservation

- Il conviendrait d'analyser les besoins effectifs propres à chaque situation et de faire des choix qui prennent en compte les risques objectifs liés aux solutions techniques. La possibilité de solutions mixtes de conservation et d'archivage associant papier et électronique devrait être envisagée.

A propos de la conservation de la signature électronique

- Il faudrait reconnaître que la fonction qui assure l'intégrité de l'acte, doit être, pour les actes authentiques, dissociée de la fonction de signature proprement dite.

- En conséquence, le décret fixant les conditions d'établissement et de conservation de l'acte authentique doit pouvoir rendre indépendante la signature électronique de l'usage de tout procédé de sécurité dont la conservation à long terme est hypothétique.

- Enfin, l'usage de la signature cryptographique pourrait être recommandé pour ce pour quoi elle a été conçue, à savoir, principalement, apporter des garanties que le document n'a pas

été modifié. La signature cryptographique viendrait alors se surajouter à la signature électronique.

A propos des questions institutionnelles et organisationnelles

- Les questions institutionnelles et organisationnelles ne peuvent relever du décret général et doivent être reprises soit dans des décrets spécifiques à certaines catégories d'actes authentiques, soit dans des textes propres à la politique en matière d'archivage.

- Toutefois, une instance de concertation entre les différents acteurs serait nécessaire pour décider du bien-fondé des choix techniques et vérifier qu'ont été prises en compte tant les finalités d'établissement que de conservation. Cette instance pourrait aussi jouer le rôle d'observatoire des actes authentiques électroniques.

ANNEXES

Introduction
Aspects de droit comparé

L'objet

L'objet de cette étude a été de constituer des fiches par pays relatant l'état de leur législation en matière de signature électronique et d'acte authentique électronique.

Les pays retenus

Sur le choix des pays retenus, l'objectif était de réunir un large éventail tant des principaux acteurs de l'internet et des échanges électroniques ou économiques au sens large, que de certains pays émergents ou s'étant dotés très tôt de telles législations.

C'est pourquoi à côté des principaux Etats membres de l'Union européenne (Allemagne, Autriche, Belgique, Espagne, Italie, Luxembourg, Royaume-Uni, Suède), le choix s'est porté sur les Etats-Unis (et certains de ses Etats), le Japon et le Canada, mais aussi sur Singapour, la République tchèque et la Tunisie. Soit au total, 14 pays.

La méthode

Cette étude comparatiste s'est déroulée en trois temps.

Il s'est d'abord agi de rechercher la législation de chacun de ces pays. Pour ce faire, l'internet a été l'outil de travail principal à travers la consultation de sites généraux et des sites des ministères des pays.

Le second temps a été consacré à l'étude détaillée de ces textes.

Enfin, il a fallu mettre en perspective les différents contenus sous la forme de fiches en retenant plusieurs idées directrices :

d'une part, retracer la **procédure législative** en cours ou ayant abouti à la reconnaissance de la signature électronique (textes, intitulés, dates, références),

d'autre part, rendre compte du cadre réglementaire mis en place sur la **signature électronique proprement dite** (définitions, niveaux de reconnaissance, catégories, fonctions, effets juridiques),

enfin, rendre compte des dispositions relatives à la **mise en œuvre** de la signature électronique (techniques de signature éventuellement consacrées, procédure de certification, prestataires de services de certification, exigences et critères techniques de sécurité, droits et obligations des utilisateurs, reconnaissance des certificats étrangers).

Les sources

Le point de départ de cette étude a été les travaux de la CNUDCI (Commission des Nations Unies pour le Droit Commercial International) et de la Commission européenne.

Sur le plan international, l'impulsion pour l'intégration et l'harmonisation législatives en matière de signature électronique est donnée par la CNUDCI. Les documents de la CNUDCI étudiés ont été le rapport du groupe de travail sur le commerce électronique (CNUDCI, 35ème session, Vienne, 6-17 septembre 1999) et les règles uniformes sur les signatures électroniques et le guide pour leur incorporation dans le droit interne (CNUDCI, 37ème session, Vienne, 18-29 septembre 2000) [101].

Sur le plan communautaire, au départ la principale source de travail a été les travaux de la commission qui ont abouti à l'élaboration du projet de directive puis à l'adoption de la directive du 13 décembre 1999 relative à un cadre communautaire pour les signatures électroniques

[101] La 38ème session se tiendra du 12 au 23 mars 2001 à New York.

ainsi que l'accord politique en vue de la position commune relative au commerce électronique obtenu le 7 décembre 1999 au Conseil « marché intérieur ».

Sur le plan national, les sources ont été constituées par les textes de lois eux-mêmes (ou le cas échéant par les projets de lois) ainsi que par les décrets ou ordonnances pris pour leur application.

D'autre part, la consultation de certaines études ont fourni des éléments d'analyse et de mise en perspective importants :

« Digital Signature Blindness : Analysis of legislative approaches toward electronic authentication », Babette Aalberts et Simone van der Hof, Tilburg, novembre 1999.

« *Authenticity in a Digital Environment* », Charles T. Cullen, Peter B. Hirtle, Clifford A. Lynch et Jeff Rothenberg, Council on Library and Information Resources, Washington D.C., mai 2000.

Pour les aspects techniques : « Matérialité de l'acte authentique électronique : encodage, signature, archivage », Jean-François Blanchette, décembre 2000.

« Europe 2002, une société de l'information pour tous : plan d'action », Conseil et Commission européenne, juin 2000.

Recommandation relative à l'informatisation de l'état civil, Commission internationale de l'état civil, Assemblée générale de Strasbourg, 21 mars 1991.

Enfin, il importe de donner les principales adresses des sites qui ont été consultés et grâce auxquels la majorité des textes ont pu être trouvés :

- http://rechten.kub.nl/simone/ds-lawsu.htm
- http://www.law.kuleuven.ac.be/icri/projects/tables.htm
- http://www.uncitral.org/
- http://www.europa.eu.int/index-fr.htm
- http://www.droit-technologie.org/

PAYS	DATE (loi votée)	DATE (entrée en vigueur)	NOM	DECRET D'APPLICATION
Allemagne	13 juin 1997	1er août 1997	Digital Signature Law	1er novembre 1997 amendé le 1er juillet 2000
Italie	15 mars 1997	15 mars 1997		10 novembre 1997 8 février 1999
Singapour	3 juillet 1998	10 juillet 1998	Electronic Transactions Act	
Autriche	19 août 1999	1er janvier 2000	SigG	2 février 2000
Espagne	17 septembre 1999	1er septembre 1999	Loi sur les signatures électroniques	21 février 2000
Royaume-Uni	29 novembre 1999	25 mai 2000	Electronic Communications Bill	
France	**13 mars 2000**	**15 mars 2000**	**Portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique**	
République tchèque	29 juin 2000	1er juillet 2000	Electronic Signature Act	
Etats-Unis (loi fédérale)	30 juin 2000		Electronic Signatures in Global and National Commerce Act	
Tunisie	9 août 2000			
Luxembourg	14 août 2000	8 septembre 2000		
Belgique	20 octobre 2000	22 décembre 2000	Introduisant l'utilisation de moyens de télécoms et de la signature électronique dans la procédure judiciaire et extra-judiciaire	
Suède	1er novembre 2000	1er janvier 2001	Act on qualified electronic signatures	
Japon	19 novembre 1999	Rapport public sur la signature électronique et la certification dans le but de promouvoir le com-merce électronique pour 2001		

ALLEMAGNE

En Allemagne, le mouvement législatif tendant à la reconnaissance et l'utilisation de la signature électronique se fit en deux temps. D'abord en 1997, le droit allemand a encadré l'utilisation des signatures digitales [102]. Puis aujourd'hui, le législateur allemand arrive au terme du processus de reconnaissance de la signature électronique [103].

S'agissant de la 1ère étape, le Bundestag a approuvé le 13 juin 1997 la « **Digital Signature Law** » (incluse à l'article 3 de la « Multimédia Law »). Elle est entrée en vigueur le 1er août 1997.

La « Digital Signature Law » est une loi technique car elle ne traite pas de la validité juridique des signatures digitales. Son but est de donner les conditions de mise en place d'une infrastructure sécurisée pour l'utilisation de signatures digitales en Allemagne.

L'intention du gouvernement allemand est de créer à terme un standard pour l'utilisation de ces signatures. Ainsi le Federal Office for Informations Security (BSI), une agence gouvernementale, s'est vu confier la mise en place de tels standards sous le contrôle du législateur.

Cette loi conduit donc à l'édification d'un système sécurisé, compétitif et destiné au marché pour l'utilisation de signatures digitales en Allemagne.

La mise en œuvre pratique et technique de cette infrastructure a été organisée par un **décret d'application** le « **Digital Signature Ordinance** », applicable depuis le 1er novembre 1997. Ce texte envisage notamment le rôle et la responsabilité des autorités de certification ainsi que les critères et techniques nécessaires à la création de ces signatures. Ce décret a été amendé le 1er juillet 2000 en vue de l'adoption de critères communs de création et d'utilisation.

Concernant la 2ème étape, le ministère de l'Economie et des Technologies publia en avril 2000 un texte [104] déterminant les choix et les axes à suivre pour transposer la directive relative à un cadre commun sur les signatures électroniques.

Cette révision de la législation allemande se compose de deux séries de mesures.

La première concerne la réforme proprement dite de la « Digital Signature Law » du 13 juin 1997. La seconde consiste à introduire de nouvelles dispositions dans le Code civil et de Procédure civile allemand pour donner à la signature électronique un statut légal.

Sur la réforme [105] de la « Digital Signature Law » en tant que telle, un projet fut déposé et approuvé par le gouvernement le 16 août 2000. Il est aujourd'hui en discussion devant le Bundestag dans le but d'entrer en vigueur le 1er janvier prochain.

Quant à son contenu, il constitue une modification substantielle de la loi du 13 juin 1997.

D'une part, il transpose assez fidèlement les dispositions de la directive communautaire relatives la signature électronique du 13 décembre 1999.

D'autre part, il modifie la structure et la terminologie employée par la loi. Il établit par exemple un système d'accréditation libre et volontaire des prestataires de service de certification. Dans le même temps, des incitations sont données aux prestataires de service de

[102] Par signature digitale (ou également appelée signature numérique), on entend signature fondée sur la cryptographie asymétrique, dite "à clé publique".

[103] On peut remarquer "l'originalité" du mouvement législatif allemand qui, contrairement aux autres pays, a inversé le processus. Ils ont effet d'abord réglementé l'utilisation des signatures digitales, ce qui en 1997, était assez avant-gardiste, pour ensuite s'intéresser, du fait de la directive, au concept juridique de la signature et de ses fonctions pour en confronter et reconnaître différents modes.

[104] "Act establishing a framework for electronic signatures (Signature Act)".

[105] "Draft Law concerning the Conditions for Electronic Signatures and for the Amendment of Further Provisions".

certification pour qu'ils requièrent une accréditation administrative. Une condition d'équivalence et de réciprocité reconnaît aux certificats étrangers la même valeur et le même effet que les certificats qualifiés allemands s'il est démontré qu'ils offrent un degré de sécurité équivalent.

Enfin, le projet retient le concept fondamental de la « Digital Signature Law » en maintenant une infrastructure libre et sécurisée pour les signatures électroniques reposant sur la technologie PKI, l'ensemble étant supervisé par une agence gouvernementale.

Sur la seconde série de mesures qui complètent les dispositions de droit civil et de procédure civile, un projet a été adopté par le gouvernement le 6 septembre dernier et a été transmis dans le même temps au Parlement avec le projet de réforme de la « Digital Signature Law ». Ces dispositions visent à introduire notamment les clauses d'assimilation et de non-discrimination de l'article 5 de la directive.

AUTRICHE

L'Autriche a été le premier Etat membre de l'Union européenne à transposer **complètement** la directive 99/93 du 13 décembre 1999 relative aux signatures électroniques en loi nationale.

La loi autrichienne du 19 août 1999 sur les signatures (SigG), adoptée dès juillet 1999 par le Parlement, est entrée en vigueur le 1er janvier 2000. Elle a été complétée par une ordonnance sur les signatures (SigV) adoptée le 2 février 2000.

Ces textes exposent le dispositif légal de création et d'utilisation des signatures électroniques ainsi que les conditions requises pour les services de certification.

Plan : Section 1 : Objet et définitions (articles 1 et 2)
Section 2 : Effets juridiques des signatures électroniques (articles 3 à 5)
Section 3 : Prestataires de services de certification (articles 6 à 12)
Section 4 : Surveillance (articles 13 à 17)
Section 5 : Exigences techniques de sécurité (articles 18 et 19)
Section 6 : Droits et obligation des utilisateurs (articles 20 à 23)
Section 7 : Reconnaissance des certificats étrangers (article 24)
Section 8 : Dispositions finales (articles 25 à 28)

Sur les effets juridiques principaux de la loi

Les procédés de signature utilisés dans les échanges juridiques et commerciaux peuvent varier quant à leur niveau de sécurité et leur classe de certification.

L'effet juridique d'une signature électronique et sa valeur probatoire ne peuvent pas être refusés pour la seule raison que la signature électronique n'existe qu'en la forme électronique, ou qu'elle ne repose pas sur un certificat qualifié, délivré ou non par un prestataire accrédité de services de certification, ou encore, parce qu'elle n'aurait pas été établie en utilisant les composants techniques et les procédés définis par la loi (article 4).

Sur les effets juridiques spécifiques de la loi

L'article 4 (1) SigG dispose que la signature électronique sécurisée (dite « signature avancée » à l'article 5 de la directive) remplit les mêmes exigences et a les mêmes effets juridiques que la signature manuscrite prévue à l'article 886 du ABGB, le Code civil autrichien, sauf disposition légale ou accord des parties.

Les dispositions du Code de procédure civile autrichien (article 294) relatives à la présomption de véracité d'un acte sous seing privé s'appliquent aux documents électroniques comportant une signature électronique sécurisée (article 4 (3) SigG).

L'ensemble de ces effets juridiques ne se produisent plus dès lors qu'il est prouvé que les conditions de sécurité prévues par la loi et l'ordonnance ne sont pas respectées ou que les précautions prises en vue du respect de ces exigences se trouvent compromises.

L'article 4 (1) SigG *in fine* prévoit une **exception** concernant :
les actes juridiques relevant du droit de la famille et du droit successoral et soumis à la forme écrite ou à une forme plus solennelle,
les autres déclarations de volonté ou actes juridiques qui nécessitent pour leur validité une certification des signatures, une authentification judiciaire ou notariale ou un acte notarié,
les jugements,
les déclarations de volonté, actes juridiques ou données qui nécessitent pour leur inscription aux registres foncier ou des sociétés, ou à tout autre registre public, une certification publique des signatures, une authentification judiciaire ou notariale ou un acte notarié.

Pour tous ces actes juridiques, la signature électronique sécurisée n'a pas la même valeur et ne produit pas les mêmes effets juridiques que la signature manuscrite (article 4 (2) SigG).

LES ARCHIVES ELECTRONIQUES DU NOTARIAT AUTRICHIEN

Le 1er janvier 2000 est entré en vigueur en Autriche un dispositif réglementaire original pour la mise en place d'archives électroniques pour les actes authentiques, appelées CyberDOC.

Ces archives sont conçues et organisées par la Chambre du Notariat autrichien en collaboration avec une entreprise privée de matériels de télécommunications.

La finalité de ces archives est l'enregistrement et la conservation électroniques des actes authentiques notariés, des autres authentiques publics et des actes privés écrits ou portant des signatures électroniques sécurisées.

Sa mise en œuvre se décompose en trois temps.

Tout d'abord, pour tout nouvel acte reçu (c'est-à-dire les actes notariés reçus à partir du 1er janvier 2000), coexisteront l'archive papier avec son double archivé électroniquement.

Comment se déroule l'enregistrement électronique des archives ? Une fois équipées du matériel nécessaire, les études pourront scanner et enregistrer directement les actes reçus sur le disque dur de leur ordinateur grâce à un logiciel spécifique.

Ensuite, l'archivage des actes sera centralisé. Pour ce faire, les notaires utiliseront le procédé des signatures électroniques sécurisées au moyen duquel ils certifieront la conformité des données de l'acte électronique avec l'original (par carte à puces ou code secret).

De plus, afin de garantir la confidentialité et la sécurité des données, le cryptage de l'acte s'effectuera directement sur l'ordinateur de l'étude. Le document électronique sera alors envoyé directement aux archives centrales et conservé électroniquement.

Enfin, l'objectif est de ne conserver les archives notariales que sous la forme électronique exclusivement.

Tant l'inscription aux archives (enregistrement et dépôt d'un acte) que leur consultation (recherche et accès pour lecture) sont payantes.

S'agissant de la consultation, celle-ci pourra se faire directement par la voie électronique. Mais la question se pose de savoir si la délivrance d'extraits ou de minutes se fera en toute sécurité par cette même voie électronique ou nécessitera un envoi par courrier ?

Cette réforme doit être intégrée dans un vaste ensemble d'adaptations technologiques initiées par le notariat autrichien : registre électronique des testaments, consultation électronique du registre foncier et du registre des sociétés par les notaires.

BELGIQUE

La genèse de la réforme « ou un accouchement difficile » :

La transposition de la directive européenne sur un cadre communautaire sur les signatures électroniques en droit interne belge a été envisagée sous deux angles d'approche qui seront ici résumés.

Il a d'abord été conduit une modification de l'article 1322 du Code civil relatif à la preuve des obligations, puis un texte spécifique sur les prestataires de services de certification.

Sur la réforme du Code civil, un premier projet de loi [106] visait à ouvrir les concepts traditionnels aux nouvelles techniques de signature et à introduire la clause d'assimilation de l'article 5.1 de la directive. Mais ce projet, rendu caduc par le changement de législature, ne fut pas relevé de caducité.

Il fallut attendre le 17 mars 2000 (adoption par le Conseil des ministres) puis le 6 juillet 2000 (adoption en séance plénière par la Chambre des représentants de Belgique) pour que le **processus d'introduction de la signature électronique dans le Code civil soit définitivement réengagé**. La **loi datée du 20 octobre 2000** a été publiée au Moniteur belge le 22 décembre 2000 (p. 42698)

Il n'en reste pas moins que ce qui surprend, est que ce projet « visant à modifier certaines dispositions du Code civil relatives à la preuve des obligations » n'a pas été déposé en tant que projet de loi à part entière, **mais sous la forme d'un amendement** à la proposition de loi du 4 août 1999 « introduisant de nouveaux moyens de télécommunication dans la procédure judiciaire et extrajudiciaire » [107].

Aujourd'hui, l'article 2 de la loi « introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire » dispose que :

« L'article 1322 du Code civil est complété par l'alinéa suivant :

Peut satisfaire à l'exigence d'une signature, pour l'application du présent article, un ensemble de données électroniques pouvant être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu de l'acte ».

Par ce texte, une définition fonctionnelle est introduite dans le Code civil. Il en ressort désormais que tout acte sous seing privé signé électroniquement est recevable pour le juge. Il devra néanmoins vérifier que les fonctions d'imputabilité (c'est-à-dire l'identification du signataire et son adhésion au contenu de l'acte) et de maintien de l'intégrité de l'acte sont bien assurées.

La recevabilité comme preuve en justice d'une signature électronique ne peut être contestée au seul motif qu'elle se présente sous la forme électronique. (et ce, en vertu du principe de non-discrimination énoncé à l'article 5.2 de la directive). Partant, il appartiendra ensuite au juge de se prononcer sur la valeur probante des documents signés électroniquement qui lui sont soumis[108].

Pourtant, certains auteurs ont émis de nombreuses critiques.

---

[106] Projet 2141 déposé lors de la précédente législature.

[107] Amendement n° 12 dudit projet de loi déposé le 13 juin 2000 à la Chambre des représentants de Belgique devenu l'article 2 de ce projet dont il a été ajouté dans la dénomination "et de la signature".

[108] Rappel sur la distinction recevabilité / force probante : une preuve recevable n'emporte pas nécessairement la conviction du juge. Cette question de la conviction du juge est celle de la valeur probante. Pour accorder à un élément probatoire une valeur probante, le juge doit considérer que cet élément peut aider à résoudre le problème qui se pose à lui, qu'il constitue une manifestation fiable de la réalité (ce qui n'est pas toujours le cas même si ces éléments étaient recevables).

Un projet lacunaire

Ces auteurs regrettent que le projet n'exige pas de transformation, quelle qu'elle soit, de l'écrit afin d'établir un lien indissociable entre l'écrit et la signature et s'assurer que l'écrit émane bien du prétendu signataire.

Un projet dépendant

De même, une législation spécifique à une catégorie d'actes sous seing privé peut faire obstacle par ses dispositions particulières à l'utilisation de la signature électronique. Et tant que les législations spécifiques n'auront pas été adaptées, le nouveau dispositif ne saurait être applicable.

Un projet frileux

Enfin, cette réforme ne concerne **que les actes sous seing privé**. Ce texte manque donc d'ambition pour ces auteurs pour **ne pas s'être aligné sur la loi française qui envisage l'acte authentique électronique**. Une telle évolution ne pourra être indéfiniment ignorée.

Sur le second point, cette réforme de l'article 1322 du Code civil ne peut être envisagée sans la combiner avec le projet de loi « relatif à l'activité des prestataires de service de certification en vue de l'utilisation de signatures électroniques » déposé le 16 décembre 1999 à la Chambre des représentants.

Ainsi son article 4, § 4 dispose que :

« Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique avancée réalisée sur la base d'un certificat qualifié et créée par un dispositif sécurisé de création de signature est assimilée à une signature au sens de l'article 1322 du Code civil, que celle-ci soit réalisée par une personne physique ou morale ».

On retrouve ici transposé le principe d'assimilation. Autrement dit**, une signature électronique, quelle qu'elle soit, est reconnue juridiquement**. Il s'agit dès lors de distinguer trois catégories de signature : les premières dites avancées si elles respectent pour leur création et leur utilisation toutes les conditions légales ; les secondes également avancées qui ne respecteraient pas toutes ces conditions (par exemple quant à l'accréditation du prestataire ou quant aux qualités du certificat émis ; et enfin, les troisièmes, non avancées, qui doivent être obligatoirement reçues par le juge, mais dont la valeur juridique dépendra de l'appréciation du juge.

Quant à la **signature électronique avancée**, c'est-à-dire créée par un dispositif sécurisé de création de signature combinée à un certificat qualifié (ayant certaines mentions et émis par un prestataire de service de certification accrédité suivant le processus mis en place par le projet belge), elle a **la même force probante et produit les mêmes effets juridiques que ceux reconnus à la signature manuscrite**.

Il est intéressant de souligner que dans l'exposé des motifs du projet de loi, même si la **neutralité technologique** est adoptée par l'utilisation de définitions larges, celle-ci n'est que potentielle. Le rapporteur estime en effet que seule, **à l'heure actuelle**, **la technique de signature digitale (ou numérique) fondée sur la cryptographie asymétrique, dite « à clé publique », répond à la définition de la signature électronique avancée au sens de la directive**.

En outre, le système d'accréditation est libre même si chaque prestataire pourra, s'il le demande, obtenir une accréditation administrative s'il répond aux conditions stipulées dans la loi.

ESPAGNE

La législation relative à l'Internet en Espagne a été envisagée globalement et comprenait à l'origine trois textes : **le décret-loi 14/1999 du 17 septembre 1999 sur les signatures électroniques**, l'ordonnance du Ministre du Développement du 21 mars 2000 qui régule le système d'attribution des noms de domaine (.es) et le décret-loi 7/2000 du 23 juin 2000 relatif aux mesures urgentes dans le secteur des télécommunications et notamment concernant l'utilisation de l'Internet par les entreprises et les citoyens. Aujourd'hui les dernières dispositions concernent la protection des données personnelles et l'aspect pénal de la régulation.

Le contexte de cette soudaine régulation s'explique par la forte expansion de l'Internet, la conscience de ses énormes débouchés pour l'économie et l'emploi mais aussi de ses importants risques techniques et nombreuses conséquences juridiques. C'est pourquoi, les premières normes promulguées font référence à l'utilisation des **techniques de cryptographie** et sont relatives à la **signature électronique**.

La loi espagnole du 17 septembre 1999 sur la signature électronique

Il est intéressant de rappeler qu'il existe depuis 1997 des dispositions sur l'utilisation de la signature électronique par les administrations publiques espagnoles.

La loi du 17 septembre 1999 s'inspire très largement des travaux et du projet de directive du 13 décembre 1999 fixant un cadre commun sur les signatures électroniques.

Son objectif est d'assurer et de garantir la sécurité des communications et des transactions en raisonnant d'un point de vue juridique et non sous l'angle exclusif de la technique. Le texte établit qu'une signature électronique complétant un document électronique respectait les avait les mêmes caractéristiques qu'une signature manuscrite, c'est-à-dire l'imputation du document à son auteur et la garantie de son intégrité.

Les principales dispositions de la loi sont les suivantes :

- **elle fait produire des effets juridiques à la signature électronique et à la signature électronique avancée (article3),**
- **elle encadre le rôle et la compétence des prestataires de services de certification (titre 2, chapitres 1 et 3),**

  - elle exige la tenue d'un registre des prestataires de services de certification (article 7) [109],

  - elle prévoit un contrôle administratif des prestataires de services de certification (titre 2, chapitre 4),

- **elle prévoit les conditions d'attribution et de perte de validité des certificats (titre 2, chapitre 2),**
- **elle encadre les systèmes de signatures électroniques et l'évaluation de leur adéquation aux dispositions légales.**

Le décret d'application du 21 février 2000

Suite à ce texte et en vue de sa mise en œuvre concernant les aspects techniques, un **décret d'application** fut adopté le 21 février 2000 par le Ministre du Développement. Ce décret organise d'une part, l'accréditation des prestataires de services de certification et d'autre part, la certification de certains produits de la signature électronique.

[109] Il est à noter que le décret organisant la liste des fournisseurs de services de certification n'a pas encore été promulgué. Il est pour l'instant seulement prévu par la loi qu'il sera tenu au Ministère de la Justice. Ce décret est pourtant indispensable à la mise en œuvre complète d'un système global de signatures électroniques. La signature électronique n'acquerra des effets équivalents à la signature manuscrite qu'à la condition de respecter les prescriptions légales de garantie d'imputabilité et d'intégrité et les exigences relatives à la certification, au premier rang desquelles figure l'inscription à ce registre des fournisseurs de services de certification..

Ce texte porte davantage sur les procédures à respecter pour la certification que sur les prestataires capables de mettre en œuvre cette certification au moyen de la signature électronique (voir remarque note 1). Il permet néanmoins de rappeler ce que l'acte doit contenir pour avoir un effet légal reconnu.

L'instruction du 31 décembre 1999 de la Direction générale des Registres et des Notaires indique comment établir et conserver au registre du commerce des actes par la voie télématique et en ayant éventuellement recours à un procédé fiable de signature électronique.

La résolution du 26 avril 2000 de la Direction générale des Registres et des Notaires envisage l'applicabilité de la loi du 17 septembre 1999 à des domaines spécifiques. Elle précise l'utilisation de la signature électronique pour les actes notariés, les actes d'Etat civil et les actes accomplis par les institutions administratives et judiciaires.

Ces spécifications sont en rapport direct et conformes à celles données par l'instruction du 31 décembre 1999 relatives au registre foncier et au registre du commerce.

ETATS-UNIS

Au niveau fédéral, le Président Clinton a signé le 30 juin 2000 la loi octroyant aux signatures électroniques la même valeur juridique qu'aux signatures manuscrites. Ce texte, l' »Electronic Signatures in Global and National Commerce Act » fait directement écho à la directive européenne sur les signatures électroniques adoptée le 13 décembre 1999.

A l'origine, cette loi est issue d'un large consensus né au milieu des années 90 sur les perspectives que le commerce électronique allait engendrer.

Si ses dispositions se veulent être neutres d'un point de vue technologique, reprenant ainsi l'approche de la directive européenne, il apparaît très clairement que la seule technique envisagée dans l'esprit des rédacteurs qui répond aux exigences requises est la signature digitale.

La loi établit un principe général selon lequel on ne peut dorénavant dénier une valeur probante et des effets légaux à une signature électroniques pour le seul fait qu'elle est sous la forme électronique et non pas sous une forme manuscrite. De la même manière, un acte ne peut se voir dénier une valeur ou des effets légaux pour le seul fait qu'il a été rédigé sous une forme électronique ou signé électroniquement. Il s'agit donc de donner au document ou à la signature électroniques les mêmes effets que ceux relatifs au document papier ou à la signature manuscrite, à la condition de respecter les conditions et exigences légales.

L'objet des développements qui suivent est de montrer les liens et les compétences respectives de la loi fédérale et des lois de chaque Etat américain sur la preuve électronique.

En effet, de nombreux Etats avaient déjà avant l'adoption de la loi fédérale eux-mêmes adoptés un cadre réglementaire relatif au document et à la signature électroniques.

Bien entendu à partir de sa date d'entrée en vigueur, la loi fédérale américaine a invalidé toute disposition d'une loi d'un Etat américain qui lui était contraire. D'un autre côté, certaines dispositions fédérales coexistent sur de nombreux points avec les législations étatiques.

La coexistence entre la loi fédérale et les lois des Etats américains s'articule selon d'une part, l'énoncé par le texte fédéral de règles impératives (section 101 de la loi), et d'autre part, l'autorisation pour chaque Etat fédéré de modifier ou remplacer les effets de la loi fédérale en prévoyant un certain nombre d'exceptions (section 102).

Pour mieux appréhender le champ de « préemption » de la loi fédérale sur les législations des Etats fédérés, il convient d'examiner successivement les différents dispositifs que peuvent avoir prévu ces Etats.

1ère hypothèse : Si un Etat n'exige aucun écrit pour former un contrat ou constituer un acte déterminé, la loi fédérale est inapplicable.

2ème hypothèse : Si un Etat prévoit que la signature électronique ou un acte authentique électronique sont valables au même titre que la signature manuscrite ou l'acte authentique papier, la loi fédérale ne s'applique pas non plus car la loi de l'Etat ne dénie aucune valeur probante à une telle signature ou à un tel acte du seul fait qu'ils sont sous une forme électronique. Ainsi l'objet principal de la loi fédérale est-il bien respecté.

3ème hypothèse : La loi de l'Etat prévoit qu'une signature électronique ou un document électronique signé ne sont valables et produisent des effets que si la technique utilisée est bien celle prévue par le texte. Dans ce cas, les règles impératives de la section 101 de la loi fédérale sont pleinement applicables et censurent un tel choix de ne consacrer qu'une seule technique (qui le plus souvent sera une infrastructure cryptographique à clé publique). Ce texte contredit en effet le principe général édicté par la loi fédérale puisque cela revient à dénier toute force probante ou tout effet légal à un acte électronique ou à une signature électronique, créés par une autre technique, pour le seul fait qu'ils sont sous une forme électronique. Il s'agit donc

d'une réelle discrimination.

4ème hypothèse : Enfin, une loi d'un Etat qui prônerait l'utilisation d'une seule technique qui permettrait de satisfaire aux conditions relatives à la signature et à l'écrit, et permettrait de s'assurer de l'identité des parties et de l'intégrité du message serait bien appliquée. Dans ce cas, la loi fédérale ne censurerait pas ces dispositions car ce qui est prévu est un dispositif sécurisé de signature et moins une discrimination technique. Le texte fédéral s'attachant seulement ici à pouvoir laisser une porte ouverte à l'utilisation d'autres techniques qui satisferaient à ses exigences. C'est d'ailleurs le dispositif le plus souvent retenu par les différents Etats américains avec le choix de consacrer la signature digitale sans exclure l'utilisation d'autres techniques sécurisées et fiables.

En résumé, on peut donc dire que la loi fédérale américaine s'attache à faire respecter deux grands principes : d'une part, le principe de la reconnaissance et de l'équivalence entre la forme électronique et la forme papier ou manuscrite, et d'autre part, le principe de neutralité technique. Pour d'autres questions comme les droits et obligations des utilisateurs, ou les conditions requises pour valoir comme un écrit papier ou une signature manuscrite il est renvoyé aux textes des Etats (renvoi opéré par la section 102 de la loi fédérale).

La totalité des Etats américains se sont dotés d'une législation spécifique en matière de document et signature électronique. Les premières dispositions en la matière datent de 1993 en Californie.

La très grande majorité de ces Etats ont prôné la neutralité technique. Seuls trois d'entre eux (Arizona, Floride, et Wyoming) ont retenu expressément la technique PKI [110]. Pour toute forme de communication, à l'exception des actes notariés, et encourent donc la censure par la loi fédérale.

Enfin, l'utilisation de la signature électronique varie selon les Etats : elle peut être applicable pour toutes sortes de communications, limitée aux échanges avec les administrations ou avec les banques, limitée aux actes de plaidoirie et à l'établissement des jugements, ou limitée aux actes d'état civil.

[110] Public Key Infrastructure.

ITALIE

La législation italienne sur la signature digitale se compose de trois séries de dispositions.

La première est contenue à l'article 15.2 de la loi du 15 mars 1997 qui consacre en tant que principe légal la validité des documents électroniques.

Il dispose en effet que les instruments et documents constitués par les services publics et les personnes privées utilisant des moyens informatiques ou télématiques, ou les contrats conclus sous cette forme, leur archivage ou leur transmission par des moyens informatiques sont valables et peuvent constituer des preuves légales.

Les critères et les méthodes d'application de ces dispositions seront établis pour les services publics et les personnes privées par des décrets spécifiques.

Le décret présidentiel du 10 novembre 1997 reprend les principes généraux cités ci-dessus et leurs spécifications. De plus, il affirme qu'une signature digitale est équivalente à une signature manuscrite tout en prévoyant différents niveaux d'équivalence.

Le décret impose qu'une signature digitale soit certifiée par une autorité de certification accréditée. A défaut elle pourra quand même valoir à titre de preuve, mais d'une force probante inférieure à celle de la signature manuscrite, ou de commencement de preuve.

Les garanties de l'autorité de certification sont similaires à celles prévues par le projet de directive européenne en son annexe II sur les signatures électroniques.

Enfin, le décret du Premier Ministre du 8 février 1999 définit les règles et prescriptions techniques. Ainsi en est-il des algorithmes utilisés pour signer, des fonctions de hachage du document utilisées, des trois types de clés possibles et de la fonction unique qu'elles remplissent, de la longueur minimum d'une clé (1024 bits), des obligations respectives des parties et de l'autorité de certification, des informations contenues dans le certificat, de son format, de la procédure d'enregistrement devant l'autorité de certification, de la révocation des certificats et de la suspension des procédures, des garanties offertes par l'autorité de certification ou bien encore de l'archivage.

JAPON

Le 19 novembre 1999, les ministres des Postes et Télécommunications, du Commerce international et de l'Industrie (MITI) et de la Justice ont rendu public un rapport sur la signature électronique et la certification dans le but de promouvoir le commerce électronique et poser les fondations des activités économiques et sociales relatives aux réseaux dont l'Internet.

Après avoir présenté les objectifs de cette réforme qui devrait être applicable en 2001, les auteurs envisagent les points essentiels à considérer et prônent certaines orientations majeures pour la future loi.

1/ Sur les objectifs de la réforme

En premier lieu, il est rappelé l'ampleur actuelle et surtout à venir du phénomène de l'Internet qui fera « partie intégrante de la vie de toute la société » et se « retrouvera dans tous ses secteurs importants tels que le commerce, la finance, l'éducation, la protection médicale et sociale, l'administration ». L'Internet dépasse les modes traditionnels de communication et les liens privés. Chaque utilisateur se retrouve donc confronté à de nouvelles problématiques relatives à avoir des garanties suffisantes sur l'identité de l'expéditeur d'informations et sur l'intégrité elle-même de ces informations. La signature électronique et la certification électronique doivent ainsi être amenées en ces domaines à jouer un rôle prépondérant, comparable à celui de la signature manuscrite dans les communications, échanges et transmissions de données et d'informations traditionnels. Il n'existe à l'heure actuelle aucun texte au Japon régissant ces nouveaux instruments et utilisations.

Il apparaît donc essentiel que le Japon se dote d'un dispositif réglementaire destiné à assurer la sécurité des transactions et à prévenir tout différend tel qu'il existe dans le système légal de la preuve. Tout le commerce électronique mais aussi bientôt l'ensemble des activités économiques et sociales dépendront de la création d'un environnement dans lequel chaque personne aura et se sentira en confiance pour participer à ces échanges. Enfin, cette réforme devra être suffisamment large pour intégrer et s'adapter à toutes les nouvelles techniques qui seraient relatives à l'image, au texte, au son ou à toute autre forme.

En second lieu, une telle démarche pour le Japon se doit de prendre en considération les expériences étrangères. En effet il apparaît essentiel pour sa viabilité que les dispositions de cette réforme intègrent le caractère transfrontalier de toutes ces activités et soient compatibles et reconnues réciproquement à l'étranger. Pour cette raison, ont été prises en compte les orientations de la loi fédérale américaine et des lois de certains Etats américains (Utah, Illinois), de la directive communautaire du 13 décembre 1999 et des lois de certains Etats membres (Allemagne, France, Grande-Bretagne, Irlande et Italie), des lois de certains pays asiatiques (Malaisie, Singapour et Corée du Sud) et des travaux de la CNUDCI (Commission des Nations Unies pour le Droit commercial international).

2/ Sur les 5 orientations prônées par le projet de réforme :

a) Assurer la sécurité des réseaux pour le commerce électronique et les autres activités économiques et sociales

Pour y satisfaire, il s'agit de reconnaître à la signature électronique les mêmes fonctions et valeur probatoire que la signature manuscrite. Ainsi une signature électronique permet d'identifier l'expéditeur ou l'utilisateur et de garantir l'intégrité du contenu des données transmises.

Il est aujourd'hui indiscutable que la signature digitale [111] (c'est-à-dire une sorte de

[111] La signature digitale repose sur un schéma de cryptographie à clé publique.
L'utilisateur crée une paire de clés codées : une clé privée gardée secrète par l'utilisateur et une clé publique distribuée librement. L'utilisateur crypte les données de son message au moyen de sa clé privée avant de l'envoyer (auquel il faut ajouter en pratique l'étape dite du hachage). Le destinataire utilise alors la clé publique pour décrypter le message. Il n'existe qu'une seule clé publique correspondant à la

signature électronique reposant sur une infrastructure à clé publique) est très largement utilisée. Pourtant une telle signature deviendra vite inutilisable ou perdra ses fonctionnalités dès lors qu'un prestataire de services de certification utilisera un certificat défectueux ou lorsque le destinataire et seul utilisateur de la clé privée en fera un mauvais emploi. Ces hypothèses doivent être prises en compte au moment de désigner la (ou les) infrastructure(s) adéquates.

Il peut être en outre conseillé de choisir un large éventail de fonctionnalités de méthodes de vérification d'identité pour s'adapter à toutes les activités de l'Internet, du commerce électronique ou du multimédia.

Enfin, les techniques en ces matières étant très évolutives, il importe de clarifier non seulement le statut et la valeur de la signature électronique mais aussi, ce qui est considéré par la loi comme un procédé permettant de signer électroniquement, en élaborant par exemple une classification facilement compréhensible par tout utilisateur.

b) Garantir la neutralité technologique pour les signatures électroniques et la liberté pour les activités de certification.

Aujourd'hui, s'il ne s'agit pas de donner un statut légal à la technique dite PKI, c'est-à-dire fondée sur une infrastructure à clé publique, la signature électronique ainsi créée est appréhendée comme étant la plus appropriée et offrant le plus de garanties par rapport aux autres techniques actuelles qu'elles soient fondées ou non sur des techniques plus avancées. **Il n'en demeure pas moins que la loi doit rester totalement neutre sur le plan technologique et permettre la création et l'utilisation de signatures fondées sur de nouvelles méthodes ou techniques.** Pour ce faire**, la loi doit s'attacher non pas à consacrer un type de signature** (qui pourrait être choisie selon l'importance de son utilisation à une période donnée comme la signature digitale aujourd'hui**), mais aux fonctions que doit remplir une signature**. A cet effet, il s'agit de prévoir l'étendue et la nature des données que la signature électronique peut identifier et garantir (texte, son, image…).

De plus, il semble indispensable d'instaurer un système totalement libre pour les activités de certification. Si la loi pose certaines exigences de sécurité et de garantie c'est uniquement dans le but d'offrir à la signature électronique ainsi créée les mêmes effets que la signature manuscrite dans le système légal de preuve. Il faut donc éviter de prévoir un ensemble de conditions trop restrictives dès lors qu'il ne s'agit plus de la valeur juridique proprement dite de la signature, mais par exemple d'activités de certification afin de ne pas freiner le développement du commerce.

c) Assurer la liberté de choix pour chaque utilisateur d'un prestataire de services de certification.

Il est instauré un système d'accréditation volontaire géré par le gouvernement. Certaines conditions standards sont fixées pour obtenir cette accréditation et déterminent les obligations du prestataire de services de certification accrédité (relatives au niveau de sécurité offert, à l'étendue des opérations offertes, aux méthodes d'identification et de vérification, à la situation fiscale, …).

d) Assurer la protection de la part des prestataires de services de certification des données individuelles des particuliers et des sociétés et du secret de l'existence de communications entre un utilisateur et un prestataire de services de certification.

e) Maintenir une compatibilité internationale des systèmes de signature électronique et d'authentification avec les systèmes étrangers.

clé privée de l'expéditeur, le destinataire peut donc avoir l'assurance que le message a bien été signé par la clé privée correspondante (et donc en principe par son propriétaire).

LUXEMBOURG

La loi luxembourgeoise sur les signatures électroniques a été adoptée par le Parlement le 12 juillet 2000, signée par le Grand-Duc le 14 août 2000 et enfin publiée le 8 septembre dernier au Journal officiel.

Elle se compose de deux parties : l'une concerne le commerce électronique en général, l'autre la preuve et la signature électroniques en particulier.

Même si cette réforme s'inspire au niveau international des travaux de la CNUDCI, ses principales références sont d'une part, les différents textes communautaires [112] et d'autre part, les expériences étrangères principalement française et belge [113].

Une première série d'adaptation aux règles générales de la preuve littérale vise à reconnaître à l'acte sous seing privé électronique une valeur équivalente à celui revêtu d'une signature manuscrite. Dans un second temps, le texte encadre l'activité des prestataires de service dits de certification sollicités pour l'usage de la signature électronique sur un réseau ouvert.

Concernant le champ d'application (titre 1, article 2, § 2)

Il est intéressant de souligner parmi les exclusions du champ d'application de la loi celle relative aux activités de notaires ou de professions équivalentes dans la mesure où ils supposent un lien direct et spécifique avec l'exercice d'une autorité publique. Sont visés les actes authentiques établis par le notaire en tant qu'officier public.

Concernant l'usage de la cryptographie (article 3) :

Le **principe de liberté** de l'usage de techniques de cryptographie est institué.

Concernant l'activité de prestataires de services :

L'accès à cette activité ne fait l'objet d'aucune autorisation préalable spécifique[114].

Sur la preuve littérale

Reprenant le schéma de la loi française, la loi luxembourgeoise donne une définition fonctionnelle de la signature sans s'attacher ni au mode d'expression de la signature ni à son support [115].

De la même manière, une nouvelle conception de l'originalité est proposée sous l'angle fonctionnel[116]. C'est-à-dire que l'originalité ne se ramène pas, comme par le passé, à la nature et à l'absence de modification du support, mais cette originalité découle de ce que l'intégrité d'une information puisse être établie de son origine à nos jours.

---

[112] La directive du 13 décembre 1999 relative à un cadre communautaire pour les signatures électroniques et l'accord politique en vue de la position commune relative au commerce électronique obtenu le 7 décembre 1999 au Conseil "marché intérieur".

[113] En effet, le droit luxembourgeois de la preuve est directement inspiré du Code Napoléon. Mais ce texte tient aussi compte des lois allemande, italienne et de certains états des Etats-Unis.

[114] Il s'agit de poser le principe général suivant lequel la mise sur site d'activités commerciales ne fait l'objet d'autres réglementations que celles déjà existantes et non spécifiques à la société de l'information.

[115] L'article 1322-1 du Code civil luxembourgeois dispose :
"La signature nécessaire à la perfection d'un acte sous seing privé identifie celui qui l'appose et manifeste son adhésion au contenu de l'acte.
Elle peut être manuscrite ou électronique.
La signature électronique consiste en un ensemble de données, liées de façon indissociable à l'acte, qui en garantit l'intégrité et satisfait aux conditions posées à l'alinéa premier du présent article".

[116] L'article 1322-2 dispose :
"L'acte sous seing privé électronique vaut comme original lorsqu'il présente des garanties fiables quant au maintien de son intégrité à compter du moment où il a été créé pour la première fois sous sa forme définitive."

Il est mis fin pour les actes sous seing privé revêtus d'une signature électronique à la formalité du double original.

Le problème de l'archivage de documents électroniques comportant une signature électronique n'est pas envisagé par la loi. Pourtant certains commentateurs luxembourgeois relèvent que cette question devra être abordée par la suite. Dans la technique du cryptage qui a été retenue, la paire de clés utilisée pour signer le document et le certificat émis par un prestataire n'ont qu'une durée d'utilisation limitée car, après une certaine période, la paire de clés n'a plus un niveau de sécurité suffisant. Il faudra donc en recréer et s'assurer que le message à nouveau signé garde la même valeur juridique que le message initialement signé.

Sur la signature électronique et les prestataires de services de certification

Le recours à la certification (et subséquemment au certificat qualifié ou non) est donc consacré par la loi. L'article 17 de la loi renvoie toutefois à des décrets d'application la fixation des exigences et des garanties que devront satisfaire les dispositif sécurisés ou non de création de signature, les certificats qualifiés et les dispositifs de vérification de signature, afin d'assurer la neutralité technique du texte de la loi.

L'accréditation des prestataires de services de certification par une autorité nationale d'accréditation et de surveillance est possible mais constitue une condition indifférente quant à la valeur juridique d'une signature électronique dotée d'un certificat qualifié quel qu'il soit.

L'article 18 de la loi établit un lien direct entre l'introduction de la définition ouverte et fonctionnelle du concept de signature et les principes relatifs à la certification pour les échanges dématérialisés[117].

Enfin l'on peut noter le procédé du recommandé électronique qui offre à l'instar de celui déposé matériellement la possibilité pour l'expéditeur d'un message signé digitalement de se constituer une preuve de l'envoi, de la date et, le cas échéant, de la réception de ce message.

[117] Article 18 de la loi : "Des effets juridiques de la signature électronique"
Selon le § 1, la combinaison d'une signature créée par un dispositif sécurisé, que le signataire peut garder sous son contrôle exclusif, et d'un certificat qualifié donne une force probante équivalente à une signature manuscrite au sens de l'article 1322-1 du Code civil.
§ 1 : "Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique créée par un dispositif sécurisé de création de signature que le signataire puisse garder sous son contrôle exclusif et qui repose sur un certificat qualifié, constitue une signature au sens de l'article 1322-1 du Code civil."
En revanche, lorsque la signature électronique ne satisfait pas aux exigences du § 1 de l'article 18, la loi reprend le principe de non-discrimination énoncé par la directive (article 5 § 2).
§ 2 : "Une signature électronique ne peut être rejetée par le juge au seul motif qu'elle se présente sous forme électronique, qu'elle ne repose pas sur un certificat qualifié, qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de certification, ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature".
Il appartiendra donc à la personne qui s'en prévaut d'apporter la preuve de la fiabilité de la technique utilisée afin d'établir que la signature répond aux critères posés par l'article 1322-1 du Code civil. Ainsi l'acte auquel elle est attachée servira de commencement de preuve par écrit.
§ 3 : "Nul ne peut être contraint de signer électroniquement".

SUEDE

Le gouvernement suédois a présenté le 18 mai 2000 au Parlement un projet de loi sur les signatures électroniques qualifiées « Act on Qualified Electronic Signatures ». Le Parlement suédois l'a approuvé en novembre 2000 et il entrera en vigueur le 1er janvier 2001. Ce texte constitue l'une des mesures du programme du gouvernement pour « la Société de l'Information pour Tous ». Cette réforme se propose de transposer les dispositions de la directive communautaire du 13 décembre 1999 sur un cadre commun pour les signatures électroniques.

Même si la signature électronique est, dans de nombreux cas particuliers, reconnue légalement et est déjà utilisée en Suède (par exemple par les banques), le projet doit servir à donner confiance au public sur la signature électronique et encourager son utilisation pour toutes les formes de communications dans la société. Par ce biais, le gouvernement souhaite stimuler le commerce électronique afin qu'il occupe une place prépondérante dans l'économie. En outre, les administrations publiques sont encouragées à utiliser plus souvent au quotidien de telles procédures et à en augmenter l'accessibilité.

Le texte consacre d'emblée une signature électronique particulière : **la signature électronique qualifiée** basée sur un certificat qualifié, émis par un prestataire de services de certification qui devra se déclarer auprès d'une autorité de régulation et de supervision avant toute émission de certificats. Il est proposé que l'Agence nationale des Postes et Télécommunications suédoise soit désignée comme cette autorité[118].

La nouvelle législation reconnaît donc une signature électronique particulière qui remplit les exigences de sécurité. Pour être considéré comme qualifiée, une signature devra être issue d'un procédé sécurisé de création de signature et basée sur un certificat qualifié.

Le choix d'utiliser un tel procédé sécurisé de création est de garantir que la signature n'a pas été contrefaite, qu'elle est bien uniquement liée au signataire et qu'elle ne peut être utilisée par des personnes autres que les parties. Le certificat qualifié devra contenir certaines informations à titre de validité telles que la personne physique ou morale ayant délivré le certificat, l'identité du signataire ou encore la période de sa validité.

La signature électronique sert à prouver que le contenu du message transféré électroniquement n'a pas été altéré, que l'origine du message provient bien du véritable émetteur ou que ce dernier ne puisse dénier par la suite avoir envoyé le message.

Dans l'exposé des motifs, il est précisé qu'il est important**, pour utiliser la signature électronique dans un système ouvert**, que les parties aient accès aux informations sur le signataire. A cet effet, il est indiqué qu'un système de signatures électroniques connu et déjà développé était le système reposant sur une infrastructure à clés publiques (PKI) [119], laquelle implique l'émission d'un certificat électronique par un tiers de confiance. Ce certificat contient certaines informations qui confirment l'identité du signataire [120].

Le projet de loi consacre plusieurs principes issus de la directive européenne.

En Suède, selon le droit commun, un acte est valable qu'il ait été conclu verbalement, sous la forme d'un écrit papier ou par voie électronique. Des exceptions existent pour lesquelles un

[118] Cette autorité, auprès de laquelle tout prestataire de services de certification aura dû se déclarer, publiera la liste de tous les prestataires autorisés à émettre des certificats. Elle pourra également poser toute question, ordonner toute inspection ou prescrire toute mesure à l'encontre d'un prestataire qui ne respecterait pas ou plus les exigences légales.

[119] L'infrastructure à clés publiques utilise la technique de la cryptologie asymétrique au moyen d'une paire de clés. La personne qui signe le message utilise sa clé privée tandis que celle qui le reçoit peut vérifier l'identité du signataire, et s'assurer que le contenu du message n'a pas été altéré, en utilisant la clé publique du signataire.

[120] On peut donc dire que si le législateur suédois n'a pas consacré de solution technique particulière (en vertu du principe de neutralité), il avait très fortement à l'esprit, qu'en l'état actuel de la technique, l'utilisation de la signature électronique doit reposer sur la technique PKI pour correspondre aux exigences légales de la signature électronique qualifiée.

écrit papier est exigé à titre de validité notamment dans le secteur public ou pour les contrats de vente immobilière. Dorénavant, pour faire la preuve d'un acte juridique, un écrit électronique aura la même force qu'un écrit papier s'il répond aux exigences légales et s'il est signé par une signature électronique qualifiée.

La signature électronique est par cette réforme considérée comme ayant la même force probante qu'une signature manuscrite (clause d'assimilation). En outre, dans tous les cas où l'emploi d'une signature électronique est autorisé, une signature électronique qualifiée sera toujours acceptée.

La Suède souhaite faire de son service public un pionnier dans l'utilisation des technologies de l'information. L'objectif est de rendre le service public plus accessible et efficace tant dans ses communications internes entre les différentes administrations publiques, que dans ses communications externes avec les entreprises et les citoyens. Il convient donc d'adopter pour le législateur suédois des règles de sécurité communes et des solutions standards.

TUNISIE

La Tunisie s'est dotée d'un dispositif légal qui **intègre la signature électronique par la loi du 9 août 2000** relative aux échanges et au commerce électronique [121].

Cette loi fixe les règles générales régissant les échanges et le commerce électroniques en consacrant le document et la signature électroniques.

Plan de la loi : Chapitre 1 : Dispositions générales / Définitions
Chapitre 2 : Du document électronique et de la signature électronique
Chapitre 3 : De l'agence nationale de certification électronique
Chapitre 4 : Des services de certification électronique
Chapitre 5 : Des transactions commerciales électroniques
Chapitre 6 : De la protection des données personnelles
Chapitre 7 : Des infractions et sanctions

Le 1er chapitre donne les **définitions**, et par là même indique certaines orientations majeures, notamment techniques, prises par la loi, des termes suivants : échanges électroniques, commerce électronique, certificat électronique, fournisseur de services de certification électronique, **cryptage** (pour lequel il est renvoyé à l'arrêté du ministre des communications du 9 septembre 1997, fixant les conditions d'utilisation du cryptage dans l'exploitation des services à valeur ajoutée des télécommunications), dispositif de création et de vérification de signature.

Le second chapitre traite de la conservation du document électronique qui fait foi au même titre que celle du document écrit.

Le texte énumère les garanties que doit offrir le support de conservation. Ce support doit ainsi permettre la consultation de son contenu, sa conservation dans sa forme définitive de manière à assurer l'intégrité de son contenu et la conservation des informations relatives à son origine, sa destination, ses dates et lieux d'émission et de réception.

Il renvoie ensuite à un arrêté du ministre chargé des télécommunications pour définir les caractéristiques techniques d'un dispositif fiable de création des signatures électroniques.

Le chapitre 3 crée l'agence nationale de certification électronique et définit sa mission et ses obligations. Elle octroie, notamment, les autorisations d'exercice de l'activité de fournisseur de services de certification électronique et fixe les caractéristiques du dispositif de création et de vérification de signature.

Le chapitre 4 définit d'abord les conditions requises pour les personnes souhaitant obtenir l'autorisation préalable d'exercice de l'activité de fournisseur de services de certification.

Ensuite, la loi envisage le rôle et les obligations de ces fournisseurs. Ils sont chargés de l'émission, de la délivrance et de la conservation de certificats en utilisant des moyens fiables, capables de protéger contre la contrefaçon et la falsification de certificats, conformément aux prescriptions d'un cahier des charges définies par le texte.

Toutes les informations collectées par les fournisseurs de services de certification électronique dans le cadre de l'exercice de leurs activités ne peuvent être publiées ou communiquées, ou utilisées en dehors du cadre des activités de certification**, sans l'autorisation écrite ou électronique de la personne concernée**.

Enfin, après la création, la vérification et les effets de la signature électronique, la loi prévoit les **cas de suspension définitive ou temporaire ou d'annulation de ces**

[121] Cette loi n° 2000-83 fut discutée et adoptée par la Chambre des députés tunisienne le 27 juillet 2000 et publiée au Journal Officiel le 11 août 2000.

certificats. Elle précise alors que dans de telles hypothèses, le titulaire du certificat suspendu ou annulé **ne plus utilisé les éléments de cryptage personnel de la signature, objet du certificat**, et il ne peut faire certifier ces éléments de nouveau par un autre fournisseur de services de certification électronique.

Cette loi très technique ne s'attache donc pas à la validité ou aux fonctions de la signature mais n'envisage que le certificat électronique reposant sur la cryptographie et ses différents acteurs.