Mission de recherche
Droit et Justice

DEMATERIALISATION DES ACTES AUTHENTIQUES

Rapport du groupe de travail
de la Mission de recherche Droit et Justice
à Madame Danielle Raingeard de la Blétière,
Directrice des affaires civiles et du sceau,
Ministère de la justice

12 juillet 2001

GROUPEMENT D'INTERET PUBLIC
247, rue Saint Honoré - 75042 Paris cedex 01 - Téléphone : 01 44 77 66 60 - Télécopie : 01 44 77 66 70
E-mail : mission@gip-recherche-justice.fr - Site internet : www.gip-recherche-justice.fr

Mission de recherche
Droit et Justice

Le Directeur

Paris, le 12 juillet 2001

Note à l'attention de
Madame Danielle RAINGEARD de la BLETIERE
Directrice des affaires civiles et du sceau

Objet : ***rapport du groupe de travail consacré au support électronique des actes authentiques***

La loi du 13 mars 2000 relative à la signature électronique a inclus les actes authentiques dans son champ d'application, sur proposition sénatoriale acceptée par le gouvernement. Eu égard aux difficultés soulevées par cette disposition, Madame le garde des sceaux s'était engagée, au cours des débats parlementaires, à ce que les décrets d'application soient précédés du travail préparatoire d'un groupe d'experts constitué sous l'égide de la Mission de recherche Droit et Justice. Plusieurs juristes, réunis par la Mission avaient en effet, antérieurement au projet de loi, déjà remis un rapport qui en avait fortement inspiré le contenu.

Par note du 31 mars 2000, vous avez saisi la Mission pour mettre en place ce groupe de travail, composé d'experts de différentes disciplines, afin de mener une réflexion générale sur les conditions de ce nouveau formalisme électronique et d'émettre des propositions de mesures nécessaires à la réalisation de la dématérialisation des actes authentiques, dans la perspective du ou des décret(s) d'application prévu(s) par la loi. Vous souhaitiez, enfin, conformément à l'engagement pris par Madame le garde des sceaux devant la représentation nationale, que les parlementaires soient associés, selon des modalités à définir, à différentes étapes de la réflexion.

Une démarche pluridisciplinaire

Pour entreprendre une étude approfondie de cette question, la Mission a constitué un groupe de travail réunissant des praticiens, universitaires et chercheurs d'horizons divers (juristes, économistes), des spécialistes du ministère de la Justice et du ministère de l'Industrie, des représentants des professions judiciaires concernées, avocats, notaires, huissiers, greffiers de tribunaux de commerce, en concertation avec leurs instances représentatives, ainsi que des responsables de questions relatives à l'Etat civil, à l'archivage et à la conservation des données, plusieurs d'entre eux ayant aussi le statut d'expert technique. Des représentants de votre direction ont participé aux travaux. (cf. liste jointe).

J'ai le plaisir de vous transmettre, ci-joint, les résultats de nos travaux, au premier rang desquels le rapport de synthèse établi par Mme Isabelle de LAMBERTERIE, directrice de recherche au CNRS, qui a également animé la réflexion du groupe. Sont indexés les rapports particuliers des différents sous-groupes, plusieurs études et contributions spécifiques, ainsi qu'un ensemble de fiches établissant, par pays, l'état de la législation en la matière, ce dernier travail ayant été élaboré dans le cadre d'un contrat de recherche (cf. sommaire). Mme Hélène PAULIAT, professeure de droit public à l'université de Limoges, directrice-adjointe de la Mission, a assuré avec moi la coordination des travaux.

Je dois souligner la motivation et l'implication des membres du groupe de travail, tous spécialistes du domaine, dont plusieurs sont connus pour être à l'initiative de projets et de réflexions très innovants. Malgré la diversité de leurs champs d'intervention, voire de leurs cultures professionnelles, ils ont su s'accorder sur des principes communs.

Le groupe a été soucieux d'envisager les situations concrètes telles que la gestion actuelle et future d'un service d'Etat civil à Strasbourg, d'un greffe de tribunal de grande instance à Marseille, du réseau des études de notaire ou du service central de l'Etat civil des français nés à l'étranger de Nantes.

La concertation souhaitée avec les parlementaires s'est effectuée dans les meilleures conditions. Nous avons adressé, le 30 janvier 2001, un pré-rapport sur l'état des travaux du groupe aux Présidents des commissions des Lois de l'Assemblée nationale et du Sénat ainsi qu'aux 22 autres parlementaires qui avaient manifesté un intérêt particulier à cette question. Le 6 juin 2001, M. LARCHE, Président de la commission des Lois du Sénat nous a invités à une audition (cf. compte rendu), à la suite de laquelle a été finalisée la version du rapport qui vous est remis aujourd'hui.

Sécurité juridique - sécurité technique

La comparaison internationale montre que, par delà l'harmonisation rendue nécessaire par les directives communautaires, le législateur national s'était montré particulièrement audacieux en élaborant la loi du 13 mars 2001.

Dans un domaine où se confrontent brutalement la tradition - l'authenticité fondée sur le formalisme - et la modernité - des supports dématérialisés -, les experts sont confrontés aux données actuelles et aux évolutions des techniques prévisibles aujourd'hui, donc forcément aléatoires. Ils n'ont pas voulu, pour autant, que leurs propositions soient strictement liées à ces seules évolutions technologiques. Ce rapport ne saurait, par ailleurs, être celui qu'auraient élaboré des industriels. L'analyse est d'abord celle de juristes qui s'appuient sur les principes juridiques fondant l'authenticité et le droit de la preuve.

Les réflexions du groupe ont abouti à un certain nombre de recommandations.

Les questions de terminologie sont essentielles. Ainsi le concept de « dématérialisation » doit-il être abandonné au profit de « support électronique » ou

« support informatique ». Le concept de « signature » doit être défini très précisément. L'authentification n'est pas la certification....

Le groupe de travail a opté pour la rédaction de deux types de textes réglementaires : d'une part, un décret général, ayant une fonction « pédagogique », posant les principes communs et harmonisant les approches techniques sans privilégier l'une d'entre elles, d'autre part, un décret particulier à chacune des trois principales catégories d'actes authentiques :actes de l'état civil, jugements, actes notariés.

Toutes les étapes ont été successivement étudiées, de l'établissement de l'acte authentique à sa conservation et à la délivrance de copie.

S'agissant de l'établissement des actes, le groupe insiste sur la nécessité du maintien du principe de la présence physique de l'officier public, en tant qu'essence même de l'acte authentique. C'est ainsi que l'officier public devra toujours compter, parmi ses attributions, la vérification des identités des personnes parties à l'acte, cette vérification ne pouvant être réduite à la présentation d'un certificat électronique. De même, la présence physique des parties est indispensable.

Concernant la signature électronique, cœur du processus de l'acte électronique authentique, il est apparu que les difficultés techniques liées à l'archivage de la signature électronique sécurisée au sens du décret n°2000-272 du 30 mars 2001, ne sont pas résolues aujourd'hui, dans la mesure où des migrations successives font inévitablement échouer les mécanismes de vérification de la signature. Il faut donc prévoir une signature électronique liée indissociablement aux données de l'acte, sans risque d'être ultérieurement altérée : la fonction qui assure l'intégrité de l'acte, doit être, pour les actes authentiques, dissociée de la fonction de signature proprement dite. L'accent a ainsi été mis sur un principe simple, mais essentiel : 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 abusive de signature. L'exemple du service de l'état civil de Nantes en est une bonne illustration, l'informatisation ayant été lancée sur une grande échelle, sur la base d'une notion de signature électronique très particulière : il s'agit de l'image numérisée de la signature manuscrite de l'officier d'état civil, la sécurité du système reposant sur toute une série de procédures correspondant aux attributions de l'officier public.

En outre, il convient de prendre en compte, dès l'établissement de l'acte, les besoins de conservation pouvant conditionner, limiter et guider certains choix technologiques. Le rapport propose d'ailleurs de mettre en place une instance de concertation entre les différents acteurs, qui serait amenée à jouer le rôle d'observatoire des actes authentiques électroniques, afin de décider du bien-fondé des choix techniques et de vérifier si les finalités de conservation ont bien été prises en compte. De même, il est recommandé d'accompagner l'acte authentique, dès son établissement, d'un certain nombre de données renseignant sur les conditions dans lesquelles il a été établi. Des raisons de sécurité évidentes nécessitent la tenue de doubles registres et de copies de sauvegarde.

Les notions d'original et de copie sont à reconsidérer, en partant du principe que ces qualités ne dépendent pas du support mais des conditions dans lesquelles ces originaux et copies ont été établis.

Sur le point précis de la vie de l'acte, le groupe rappelle que l'officier public garde sa compétence dans sa mission de délivrance des copies et extraits. Il insiste sur la nécessité de développer des réseaux sécurisés entre partenaires institutionnels mais reste réservé sur la délivrance directe aux particuliers, via les réseaux.

Enfin, de toutes les questions, celle qui apparaît la plus lourde et la plus coûteuse apparaît être celle relative à l'archivage des actes authentiques électroniques, qui constitue un défi technique, organisationnel et financier. La direction des Archives de France est d'ailleurs venue se joindre au groupe de travail tant il lui est apparu que la réflexion qui y était menée lui permettait de mesurer l'ampleur des problèmes posés.

Une concertation à poursuivre

A travers ce rapport, vous disposez maintenant d'un ensemble d'éléments qui, nous le pensons, vous permettront de mieux aborder, en temps voulu, le défi de l'introduction des nouvelles technologies dans le champ le plus formaliste de nos catégories juridiques d'actes.

La démarche et les principes juridiques nous paraissent clairement établis. Il reste à approfondir certains des aspects techniques et organisationnels que le groupe ne pouvait traiter. De même, il conviendrait d'engager une étude organisationnelle et financière prévisionnelle sur les modes de conservation et d'archivage des supports dématérialisés et sur les investissements humains et financiers que nécessiterait une telle évolution.

Tous les membres du groupe de travail restent à votre disposition, ainsi qu'à celle des différents interlocuteurs en charge du dossier, pour continuer à en suivre le déroulement.

Un travail de sensibilisation de l'ensemble des professionnels concernés paraît cependant nécessaire, tant les disparités de niveau d'information et d'approche sont importantes. Il me semble indispensable que, au sein du ministère, l'Inspection générale des services judiciaires, la direction des services judiciaires, la direction de l'administration générale et de l'équipement, la commission de l'informatique soient destinataires de ce rapport. Nous comptons mettre en ligne, dans un délai et selon des formes à convenir avec vous, certains éléments contenus dans le rapport et publier celui-ci, dans une version plus élaborée, dans la collection de la Mission de recherche Droit et Justice à la Documentation française Enfin, une journée de restitution des résultats pourrait se dérouler fin octobre, sous votre présidence.

Jean-Paul JEAN

SOMMAIRE

- LETTRE DE MISSION

- COMPOSITION DU GROUPE DE TRAVAIL

- RAPPORT DE SYNTHESE
(rapport rédigé par Mme Isabelle de LAMBERTERIE)

- ANNEXES

A. LES EXPERIENCES ETRANGERES : ASPECTS DE DROIT COMPARE
- Note rédigée par M. Tanguy DECAUP -

B. LES TECHNOLOGIES DE L'ECRIT ELECTRONIQUE
- Note rédigée par M. Jean-François BLANCHETTE -

- RAPPORTS PARTICULIERS

A. CONTRIBUTIONS DES PROFESSIONS JURIDIQUES

1. **La dématérialisation des actes notariés.**
   - Note remise par le Conseil supérieur du notariat -

2. **Notes sur l'état civil.**

   a) *Les actes d'état civil face à la dématérialisation des actes authentiques : état des lieux concernant les règles de l'Instruction générale relative à l'état civil et les pratiques administratives en rigueur.*
   - Note rédigée par M. Jean-Luc IFFRIG -

   b) *Note sur la finalité du décret d'application de l'article 1317 du code civil et sur les différentes phases du processus d'établissement de l'acte authentique.*
   - Note rédigée par Mme Isabelle GUYON-RENARD et M. Louis-Denis HUBERT -

   c) *Premières réflexions rapides sur l'acte d'état civil dressé sur support électronique eu égard aux contraintes actuelles de l'état civil.*
   - Note rédigée par M. Louis-Denis HUBERT -

3. **Contribution du sous-groupe « jugements ».**
   - Note rédigée par M. Patrick HENRY-BONNIOT -

4. **La réflexion préparatoire au décret d'application de la loi du 13 mars 2000 et à l'acte authentique électronique.**
   - Contribution de la profession d'huissier de justice -

5. **Dispositions applicables aux modalités de collecte et de diffusion pour les actes électroniques des tribunaux de commerce.**
   - Contribution du Conseil national des greffiers des tribunaux de commerce -

B. CONTRIBUTIONS RELATIVES A L'ARCHIVAGE ET A LA CONSERVATION DES ACTES AUTHENTIQUES ELECTRONIQUES

1. **Remarques de la Direction des archives de France sur la dématérialisation des actes authentiques.**

2. **L'établissement et la conservation des actes authentiques dématérialisés : problématiques.**
   - Note rédigée par Mme Françoise BANAT-BERGER et M. Yves RABINEAU -

C. COMPTES RENDUS DE VISITES

1. **L'informatisation du service de l'état civil de Nantes (Ministère des affaires étrangères).**
   (compte rendu de visite)
   Note sur l'informatisation du service central d'état civil. (SCEC)
   (note de synthèse n° 256/DIR/EC)

2. **L'informatisation de l'état civil de Strasbourg.**
   (compte rendu de visite)

3. **L'INSEE**
   (compte rendu de visite)

4. **Conseil national des greffiers des tribunaux de commerce**
   (compte rendu de visite)

5. **Le service de transfert et d'archivage des fichiers (Centre national d'études spatiales)**
   (compte rendu de visite)

6. **Audition par la commission des Lois du Sénat**
   (compte rendu d'audition)

LETTRE DE MISSION

R É P U B L I Q U E F R A N Ç A I S E

MINISTÈRE DE LA JUSTICE

Paris, le 31 mars 2000

DIRECTION
DES AFFAIRES CIVILES ET DU SCEAU

Bureau du droit civil général

références :
134-10/C/LJ
C:\LAURENT\NOTECONT\PREUVE\PROJET.LOI\GIP-SAIS.NO3
Affaire suivie par :
Laurent JACQUES

NOTE
POUR
MONSIEUR JEAN-PAUL JEAN
DIRECTEUR DU GIP DROIT ET JUSTICE

Objet : Constitution d'un groupe de travail sur la dématérialisation des actes authentiques.

Lors de la discussion en première lecture au Sénat du projet de loi portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique, le garde des sceaux s'est déclaré favorable à l'inscription dans la loi du principe de l'accès de l'acte authentique au mode électronique, tout en annonçant, compte tenu des difficultés de mise en oeuvre d'une telle dématérialisation, **la constitution d'un groupe de travail** réunissant des juristes spécialisés et des experts en matière de technologies nouvelles, chargé d'étudier les mesures à prendre par voie réglementaire.

La qualité du travail réalisé par le premier groupe d'experts constitué dans le cadre du GIP, unanimement saluée, conduit la Chancellerie à faire à nouveau appel à la structure que vous dirigez pour accomplir cette nouvelle mission.

La direction des affaires civiles et du sceau est tout naturellement disposée à vous apporter son concours.

Vous trouverez ci-joint ses suggestions quant à **la composition** du groupe de travail, **aux objectifs** qui pourraient lui être assignés et **au calendrier** dans lequel il serait souhaitable qu'il accomplisse sa mission.

I - COMPOSITION

Le souci d'assurer une parfaite cohérence entre la réforme législative et les décrets d'application me conduit à vous proposer d'intégrer dans le nouveau groupe les juristes experts qui participaient aux travaux précédents d'adaptation du droit de la preuve, auxquels pourrait s'ajouter un juriste spécialiste de procédure civile.

La dématérialisation des actes authentiques impliquant une réflexion d'ordre non seulement juridique, mais aussi technique, notamment sur le niveau de sécurité à prévoir ou sur les modes de conservation des actes, il me semble que sa composition devait être élargie **à des experts en matière de certification, d'horodatage et d'archivage des documents**.

Des magistrats des ordres judiciaire et administratif pourraient également prêter leur concours aux travaux ainsi qu'un officier de l'état-civil.

La participation d'un représentant de la profession notariale et d'un huissier de justice me paraît aussi souhaitable.

Enfin, le magistrat en charge de ces questions dans ma direction pourrait suivre les travaux de ce groupe.

Il me paraîtrait opportun que le groupe puisse **recourir à des auditions** pour entendre des personnes qualifiées. Pourraient par exemple être auditionnés des experts techniques (notamment ceux qui travaillent déjà sur la certification dans le cadre d'un groupe de travail constitué au sein du secrétariat à l'industrie) et des praticiens du droit, avocats ou magistrats.

Enfin, conformément aux engagements pris par Madame le garde des sceaux, il conviendrait d'associer les parlementaires aux différentes étapes de la réflexion selon des modalités à définir.

II - OBJET

Le groupe de travail pourrait, me semble-t-il, être investi **d'une double mission de réflexion et de propositions.**

- Il pourrait avoir pour mission de **rechercher les conditions d'un nouveau formalisme électronique venant se substituer aux actuelles exigences liées au support-papier.**

Outre les réflexions particulières qui devraient être menées pour chaque catégorie d'actes (jugements, actes de l'état civil, actes notariés), le groupe pourrait mener une réflexion générale visant à répondre notamment aux questions suivantes :

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

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 ?

- Après avoir mené ces réflexions, il pourrait **émettre des propositions de mesures, nécessaires à la réalisation de la dématérialisation des actes authentiques, et ce dans la perspective de l'élaboration du ou des décrets d'application prévus par la loi.**

III - CALENDRIER

La dématérialisation des actes authentiques suppose, compte tenu du nombre de questions qui se posent, des réflexions longues et très approfondies. Il faut néanmoins tenir compte des demandes des professionnels du droit, qui sont pour certains déjà engagés dans la voie de la certification électronique.

Compte tenu des attentes nombreuses qu'a suscité l'annonce de la reconnaissance du principe de l'acte authentique électronique, **il m'apparaît qu'un délai relativement court (de l'ordre de six mois)** pourrait être fixé au groupe d'experts pour la réalisation d'un premier rapport d'étape.

Mes services restent à votre disposition pour vous apporter toutes les informations complémentaires que vous pourriez souhaiter.

La directrice des affaires civiles et du sceau

Danielle RAINGEARD DE LA BLETIERE

COMPOSITION DU GROUPE DE TRAVAIL

Liste des membres du groupe de travail
sur la dématérialisation des actes authentiques

Mme BANAT-BERGER Françoise	Chef du service des archives du ministère de la justice
M. BERBINAU Jean	Délégué de la Commission de l'informatique, des réseaux et de la communication électronique (COMIRCE), ministère de la justice
M. BLANCHETTE Jean-François	CNRS, Centre d'études sur la coopération juridique internationale (CECOJI)
M. BLOCH Jean-Claude	Directeur du service des formalités administratives, mairie de Besançon
M. BLUTEAU Jacques	Informaticien conseiller, ministère des affaires étrangères
M. BORON François	Greffier, représentant du Conseil national des greffiers
M. BORTOLUZZI Stéphane	Conseil national des barreaux
M. BOUCHON Daniel	Directeur de l'Association pour le développement du service notarial (ADSN), Conseil supérieur du notariat
M. BRUNTZ Jean-Michel	Avocat général près la cour d'appel de Paris
M. CALARD Jean-Michel	Greffier en chef, tribunal de grande instance de Marseille
M. CATALA Pierre	Professeur de droit, université de Paris II
Mme CHADELAT Catherine	Sous-directrice, direction des affaires civiles et du sceau, ministère de la justice
M. DARDAYROL Jean-Pierre	Chef de service à la Mission interministérielle de soutien technologique pour le développement des techniques de l'information et de la communication dans l'administration (MTIC), Premier Ministre

M. DECAUP Tanguy	CNRS- Centre d'études sur la coopération juridique internationale (CECOJI)
M. DELPEUCH Jean-Pierre	Directeur des affaires juridiques, Conseil supérieur du notariat
Mme DHÉRENT Catherine	Direction des Archives de France
M. FABRE Philippe	Consultant, Conseil national des greffes
M. FAYOL François-Xavier	Avocat, représentant du Conseil national des barreaux
M. GARIOUD Georges	Directeur adjoint, Mission de recherche Droit et Justice
M. GRELLEY Pierre	Mission de recherche Droit et Justice
Mme GUYON-RENARD Isabelle	Conseiller juridique, service central d'état civil, ministère des affaires étrangères
M. HENRY-BONNIOT Patrick	Président du tribunal de grande instance de Reims
M. HUBERT Louis-Denis	Procureur adjoint près le tribunal de grande instance de Nantes
M. HUET Jérôme	Professeur de droit, université de Paris II
M. IFFRIG Jean-Luc	Directeur du service population, mairie de Strasbourg
M. JACQUES Laurent	Bureau du droit civil général, direction des affaires civiles et du sceau, ministère de la justice
M. JEAN Jean-Paul	Directeur de la Mission de recherche Droit et Justice
M. LAMBERT Alain	Président honoraire, Conseil supérieur du notariat
Mme de LAMBERTERIE Isabelle	**Directrice de recherche, CNRS-Centre d'études sur la coopération juridique internationale (CECOJI)** **Rédactrice du rapport de synthèse du groupe de travail**
M. LE MOGNE Claude	Chef du service informatique, Conseil supérieur du notariat
M. LUCAS de LAYSSAC Claude	Professeur de droit, université de Paris I

M. MATHIAS Jean-Dominique	Administrateur, Conseil supérieur du notariat
M. MENUT Bernard	Président, Chambre nationale des huissiers de justice
Mme MERTENS Christine	Association pour le développement du service notarial (ADSN), Conseil supérieur du notariat
M. MOTEL Jacques	Premier vice-président, Conseil supérieur du notariat
Mme PAULIAT Hélène	Professeur de droit, université de Limoges, Directrice adjointe, Mission de recherche Droit et Justice
M. PERDIOLAT Laurent	Service des technologies et de la société de l'information, ministère de l'industrie
Mme POURCEL Solange	Conseil supérieur du notariat
M. POUSSIN Jean-Pierre	Délégué de la Commission de l'informatique, des réseaux et de la communication électronique (COMIRCE), ministère de la justice
M. RABINEAU Yves	Inspection générale des services judiciaires, ministère de la justice
Mme RAINGEARD de LA BLÉTIERE Danielle	Directrice des affaires civiles et du sceau, ministère de la justice
Mme SCHMIDT-PARISET Florence	Conseillère technique, Cabinet du Premier Ministre
M. TEIL Jean-Pierre	Ministère de la culture
M. TONNET Georges	Avocat, Conseil national des barreaux
Mme TROCHAIN Catherine	Présidente de la Commission de l'informatique, des réseaux et de la communication électronique (COMIRCE), ministère de la justice Première présidente de la cour d'appel de Bourges
M. VIVANT Michel	Professeur de droit, université de Montpellier
M. VOILLEQUIN André	Chambre nationale des huissiers de justice

RAPPORT DE SYNTHESE

- Rapport rédigé par Mme Isabelle de LAMBERTERIE -

"Réflexions sur l'établissement et la conservation des actes authentiques"

Rapport de synthèse
rédigé par Isabelle de Lamberterie
Directeur de recherche au CNRS – CECOJI
(Centre d'études sur la coopération juridique internationale)
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 ?

---

[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.

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.

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 [1]. De ce fait, le travail effectué fait œuvre de

[1] 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

précurseur avec les limites de l'exercice.

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

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.

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 "[2]. 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* [3] 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 [4].

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" [5]

---

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

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

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

[5] 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.

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. 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 » [6].

« 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 » [7].

« 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 » [8].

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[9].

« 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) » [10].

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) [11] que pour les actes d'état civil (délégations aux agents communaux) [12].

---

[6] Idem, p. 89.

[7] Idem, p. 89.

[8] Idem, p. 312.

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

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

[11] 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.

[12] 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 [13]

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 »

---

[13] 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).

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

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 [14] 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 [15] les résultats d'un travail sur les questions fondamentales relatives à l'acquisition de l'authenticité pour les différents actes authentiques [16]. 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 [17] 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 [18].

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,

---

[14] " .....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".

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

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

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

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

principalement, des actes notariés [19]. Ce peut être aussi un acte de l'état civil [20].

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 » [21] 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 » [22].

- 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 [23] - la présence d'un seul officier public est

---

[19] L'article 1 de l'ordonnance du 2 novembre 1945 accorde un monopole aux notaires pour recevoir tous les actes et contrats auxquels les parties doivent ou veulent assurer le caractère d'authenticité attaché aux actes de l'autorité publique.

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

[21] 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.

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

[23] Remarques préliminaires sur le projet de décret aux regard des textes législatifs et réglementaires en

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 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 » [24]. 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....» [25].

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» [26].

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.

---

vigueur - mai 2000

[24] 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.

[25] 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.

[26] Idem.

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 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 [27]. Par ailleurs les fiches comparatives sur les autres législations en vigueur montrent l'état de réflexion sur ce sujet dans les pays concernés [28].

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 [29] 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 » [30] 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. » [31].

---

[27] Annexe II du présent rapport.

[28] Annexe I du présent rapport.

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

[30] 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".

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

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 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 [32]

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 [33] 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 [34].

* 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) [35]. 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 [36] 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).

---

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

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

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

[35] 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.

[36] 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).

1.2 - L'établissement des actes

S'appuyant sur l'instruction générale relative à l'état civil, M. Iffrig dans son rapport [37] décrit acte par acte - de façon détaillée - les différentes étapes d'établissement des actes de l'état civil.

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

[37] Rapports particuliers.

- 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 [38], enregistré puis édité [39]. 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) [40]. 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 [41].

- 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 [42]. 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.

---

[38] 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).

[39] Parallèlement à la publication des bans.

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

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

[42] Art. 53 du Code civil.

1.3 - L'expérience du service central d'état civil rattaché au ministère des Affaires étrangères [43]

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 [44].

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 [45]. 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

---

[43] 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. Hubert, 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.

[44] Voir infra.

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

possible aujourd'hui que directement au guichet ou par courrier.

Dans la pratique actuelle (à Strasbourg), toutes les délivrances (copie intégrale, extrait, extrait simplifié [46]) 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 [47], 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 [48]. 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

---

[46] Sans filiation.

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

[48] 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

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.

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 œ 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 [49].

- *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 ».

---

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

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.

- 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 [50] 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.

---

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

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 difficultés concernent, entre autres [51], 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 [52]. 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 [53], 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) [54]. 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.

---

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

[52] 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.

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

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

6 - Les greffes des tribunaux de commerce [55]

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 [56].

Actuellement, au tribunal de commerce de Bobigny, est mis en place à titre expérimental, l'établissement des assignations sur support électronique [57] : 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 [58] 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 [59]. Cette question sera abordée dans la suite du rapport.

---

[55] 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..

[56] Cette opération est possible aujourd'hui car elle ne nécessite aucune pièce justificative : il s'agit uniquement d'un simple bordereau qui est dématérialisé, puis qui fait l'objet d'une sortie papier pour archivage.

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

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

[59] 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 [60]) 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.

[60] 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[61], 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

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

entre partenaires professionnels et entre les officiers publics et les « usagers » [62].

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 [63] 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.

---

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

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

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).

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 [64] 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 [65].

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

---

[64] 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.

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

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.

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 [66] 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

[66] 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.

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 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 [67].

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

[67] 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).

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 [68].

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 nouvelles réalités » pour envisager une « nouvelle répartition des charges de conservation » [69].

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.

---

[68] 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 « Etat civil » attribuée à chaque citoyen.

69 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 [70], il ne faut pas oublier que la compétence fonctionnelle (ou d'attribution) des officiers publics et ministériels est définie par la loi [71].

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 [72] 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

---

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

[71] 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.

[72] 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.

principe d'un formalisme. Pour ce formalisme « à trouver » les exigences sont-elles les mêmes que pour l'acte authentique sur support papier ?

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 [73].

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.

---

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

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 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[74] 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

---

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

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**

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[75].

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).

---

[75] 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[75] 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).

* 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 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[76]». 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»[77] 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[78].

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.

---

[76] Art 1316-4 du Code civil.
[77] Voir J.- M. Olivier, op. cit., p. 14.
[78] Art. 1316-4.

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.

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[79]. 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 [80] peut-elle être envisagée dans une perspective à long terme ? Le sous-groupe de

---

[79] 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.

[80] 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

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

* 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

---

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.

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 [81]. 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 [82].

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

---

81 Ce principe s'applique aux greffes, aux notaires comme à l'état civil.

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

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 [83] ? 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 [84].

Selon les notaires, la copie authentique [85] 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 [86] 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 ?

---

[83] 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.

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

[85] 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.

[86] 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 [87] 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 [88] - doivent évidemment être

---

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

[88] Par exemple : mentions sur la minute des actes de la création de copies exécutoires, mention d'un

apposées sur la minute de l'acte et c'est un des rôles de l'officier public. Pour l'instant rien n'a été précisé sur les modalités de cette apposition sur une minute électronique dans le cadre du projet REAL.

changement de régime matrimonial sur la minute du contrat de mariage.

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 [89]

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 [90].

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) [91] ? 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 ?

---

[89] 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.

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

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

Ces questions, si elles ont un lien avec l'établissement et la conservation des actes 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 [92] 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

---

92 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.

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 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* [93] entre les différents systèmes (logiciels à faire agréer par ce service, qui imposerait un certain nombre de recommandations 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 [94] 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

---

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

[94] 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.

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 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 [95] ?

[95] 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[96] ?

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

---

[96] 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.

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 (bien souvent [97] 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 :

---

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

- 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.

- 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

A. LES EXPERIENCES ETRANGERES :

ASPECTS DE DROIT COMPARE

-Note rédigée par M. Tanguy DECAUP-

Aspects de droit comparé

M. Tanguy DECAUP,
doctorant au Centre d'études
sur la coopération juridique internationale
CNRS

- sous la direction de Mme Isabelle de LAMBERTERIE -

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) [1].

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 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.

---

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

« 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 nov. 1997 amendé le 1er juillet 2000
Italie	15 mars 1997	15 mars 1997		10 nov. 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'infor-mation 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 commerce 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 [2]. Puis aujourd'hui, le législateur allemand arrive au terme du processus de reconnaissance de la signature électronique [3].

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 [4] 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 [5] 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 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.

---

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

[3] 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.

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

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

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 [6] 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 » [7].

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[8].

Pourtant, certains auteurs ont émis de nombreuses critiques.

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.

---

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

[7] 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".

[8] 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 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) [9],
  - 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.

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.

---

[9] 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..

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 [10]. 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.

[10] 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 [11] (c'est-à-dire une sorte de 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

[11] 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 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).

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.

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 [12] et d'autre part, les expériences étrangères principalement française et belge [13].

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[14].

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 [15].

De la même manière, une nouvelle conception de l'originalité est proposée sous l'angle fonctionnel[16]. 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.

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

---

[12] 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".

[13] 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.

[14] 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.

[15] 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".

[16] 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."

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[17].

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.

---

[17] 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[18].

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) [19], laquelle implique l'émission d'un certificat électronique par un tiers de confiance. Ce certificat contient certaines informations qui confirment l'identité du signataire [20].

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 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.

---

[18] 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.

[19] 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.

[20] 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.

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 [21].

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 1[er] 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 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.

---

[21] 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.

B. LES TECHNOLOGIES DE L'ECRIT ELECTRONIQUE

-Note rédigée par M. Jean-François BLANCHETTE-

Les technologies de l'écrit électronique : synthèse et évaluation critique*

Jean-François BLANCHETTE

Centre d'études sur la coopération juridique internationale
Centre national de la recherche scientifique

18 janvier 2001

* La rédaction de ce rapport a profité des apports de nombreuses personnes : Mme Isabelle de Lamberterie, CECOJI, Centre national de la recherche scientifique ; Nick Mettyear, société PenOp ; Johan Rommelaere, société LCI SmartPen ; Graham Shaw, société Signum Technologies ; Isabelle Guyon-Renard, François Frankel et Jacques Bluteau, Service central de l'état civil, Ministère des affaires étrangères ; Me Menut et Me Bobant, Chambre nationale des huissiers de justice ; M. Jean Berbineau, COMI, Ministère de la justice ; Me Motel, Me Mathias, Me Delpeuch, Me Gard, M. de Martel, Mme Moreau-Bosc, Conseil supérieur du notariat ; Me Lambert, M. Bouchon, M. Lemogne, Association pour le développement du service notarial ; M. Gentilini, M. Henry-Bonniot, Tribunal de grande instance de Reims ; Daniel Poulin, Pierre Trudel, Centre de recherche en droit public, Université de Montréal ; Béatrice Fraenkel, Centre d'étude de l'écriture, Centre national de la recherche scientifique ; Françoise Banat-Berger, Service des archives, Ministère de la justice. Toute erreur et/ou opinion n'engage évidemment que la seule responsabilité de l'auteur. Ce rapport a été rendu possible par une bourse doctorale du Conseil de la recherche en sciences humaines du Canada et par une bourse de coopération France-Québec du Ministère des affaires internationales du Gouvernement du Québec.

A un homme muni d'un marteau, tout ressemble à un clou.
— Proverbe américain.

Table des matières

Chapitre 1

Introduction

À la mi-temps des travaux du groupe de travail sur l'acte authentique électronique, il apparaît utile de faire le point sur cet objet mystérieux. En effet, malgré les nombreuses et riches discussions, certains aspects de la problématique ont été peu abordés ; en particulier, on peut se demander à quoi ressemble *concrètement* cet acte authentique électronique : de quelle matière informatique est-il fait précisément? Quelles sont les possibilités offertes et les contraintes imposées par les différentes technologies qui réalisent, dans le concret, l'acte authentique électronique? Si on a remarqué à plusieurs reprises que le groupe de travail sur la dématérialisation des actes authentiques a du travailler à partir d'un texte de loi initialement conçu pour le commerce électronique, on a moins observé que nous avons également hérité des *technologies* issues du commerce électronique.

Le but de ce document est de donc présenter un survol des problématiques techniques particulières que pose l'acte authentique électronique, et d'offrir un survol aussi étendu que possible des technologies actuellement disponibles qui tentent d'y répondre. Un tel document permettra, il est espéré, de fonder les discussions juridiques sur une assise plus plus tangible, moins exclusivement théorique, [1] et de confronter directement les technologies impliquées dans la construction de l'acte authentique électronique : qu'accomplissent exactement ces technologies? Quelles sont leur modalités de fonctionnement, d'utilisation, leur a-priori analytiques? Que peut-on dire de leur déploiement à grande échelle et sur le long terme?

Cette étude préliminaire ne prétend pas aucunement à l'exhaustif : l'ampleur du champ, la somme des informations techniques à synthétiser, et les moyens à ma disposition ne permettent tout simplement pas de produire un rapport qui tiendrait compte de l'ensemble des facteurs en jeu. L'objectif beaucoup plus modeste de ce rapport est plutôt d'ouvrir le champ de la discussion avant que celle-ci ne s'enferme dans des solutions technologiques trop précises. La question de la sécurisation des échanges électroniques est, à mon avis, à peine entamée, tant du point de vue technique que réglementaire, sans même parler de l'adoption de ces nouvelles façons de faire par les utilisateurs. Pourtant, selon certains, les solutions technologiques permettant d'assurer la sécurisation pérenne des documents existent déjà, ne resterait qu'à en assurer le déploiement... Comme nous pourrons le constater, la situation est, en réalité, beaucoup plus complexe et beaucoup moins reluisante que les brochures commerciales satinées ne le laissent croire...

Le premier travail conceptuel important est de distinguer les différents étapes de la vie de l'acte

1. Un tel exercice a été brillamment réussi par M. Dominique PONSOT, dans son rapport *Valeur juridique des documents conservés sur support photographique ou numérique*, Observatoire juridique des technologies de l'information, 1995 — un rapport qui démontre la possibilité d'un langage qui soit tout à la fois intelligible au juriste et scientifiquement précis.

authentique, et d'examiner les questions technologiques qui se posent à chacune de ces étapes. Nous distinguerons les étapes suivantes dans la vie de l'acte, avec les questions afférentes:

1° **sa rédaction**: logiciel de rédaction ; format d'encodage de l'acte ;
2° **sa signature**: type de technologie ; outil de signature ; présence des parties à la signature ; signification de la signature de chacun des parties ; formalisme de la signature ; mécanismes d'intégrité additionnels ;
3° **la transmission du document**: stockage initial ; mécanisme de transmission ; nature de l'émetteur et du destinataire ;
4° **la réception du document**: notification du destinataire ; délais de transmission ; intelligibilité du document ; vérification des signatures ;
5° **le stockage à long terme**: format d'encodage ; support ; mécanismes institutionnels ; production des copies conformes ; vérification de la signature ; valeur probante.

Il est difficile de traiter de ces rubriques indépendamment les unes des autres et, idéalement, ce rapport les traiterait toutes, mais, faute de moyens et de temps, nous découperons la vie de l'acte en trois parties : l'encodage, (chapitre deux), la signature (chapitre trois), et l'archivage (chapitre quatre), pour conclure (chapitre cinq) par quelques observations générales sur l'acte authentique électronique et sa sécurisation.

Chapitre 2

Encodage

Au sein d'un système informatique, toute information est nécessairement représentée sous forme d'un encodage. Les publicités expriment souvent cette réalité en saupoudrant les images de 0 et de 1, mais en fait, l'encodage binaire n'est utilisé que dans les couches matérielles basses de l'ordinateur. Les applications informatiques définissent plutôt des encodages de haut niveau, encodages permettant d'entreposer de l'information dans un fichier de façon à pouvoir, d'une part, la conserver, d'autre part, la transmettre et l'échanger. Ainsi, tout traitement de texte offre une fonction de sauvegarde d'un document de travail sous forme d'un fichier, de façon à pouvoir travailler sur un même document en plusieurs étapes, et d'autre part, de façon à pouvoir échanger le fichier avec d'autres utilisateurs. [1] L'encodage est la manière dont cette information est structurée au sein du fichier — nous verrons plus loin des exemples qui permettront de rendre cette notion plus concrète.

Si le besoin initial pour un format d'encodage — entreposer, transmette, échanger — est relativement évident, il est beaucoup plus subtil de comprendre pourquoi différents types d'encodages sont apparu, se sont imposé ou, le plus souvent, disparu sans laisser de trace. Pour ce faire, il faut explorer les logiques techniques, économiques et historiques sous-tendant ces formats.

Nous nous intéressons ici uniquement à l'encodage de documents. Évidemment, l'objet « document » peut être compris de différentes façons : contenu sémantique, apparence visuelle, série de caractères alphanumériques, collection d'informations, etc. Les normes d'encodage des documents privilégient en général un seul de ces aspects, et intègrent les autres de façon secondaire. Nous verrons que les questions relatives à l'encodage se posent à chacune des étapes de la manipulation de l'acte authentique électronique : à l'établissement évidemment, mais aussi à la signature (problème du *what you see is what you sign*) et à l'archivage (problème de la migration des fichiers).

Il existe à peu près autant d'encodages que d'applications. [2] Certains sont totalement inconnus du grand public, alors même qu'ils dominent au sein de communautés d'utilisateurs. [3] L'encodage peut varier selon le type d'application l'utilisant (traitement de texte, traitement d'image, base de

1. La gestion — l'accès, destruction, etc. — des fichiers est réalisée au niveau du système d'exploitation, mais l'encodage du fichier est fonction de l'application informatique.

2. La bible des formats d'encodage graphique : James D. Murray et William van Rypper, *Encyclopedia of Graphics File Formats, 2nd Edition*, O'Reilly, 1996.

3. Par exemple, les mathématiciens utilisent le langage TEX pour produire des documents en format DVI, offrant un typographie de qualité supérieure, tout en étant relativement indépendant de la plate-forme informatique. La difficulté d'apprentissage de l'encodage TEX en fait un candidat peu probable comme format universel, mais pour les mathématiciens, c'est un outil indispensable et très désirable, qui a connu un succès fulgurant en moins d'une dizaine d'années. Voir à ce sujet Donald KNUTH, *Digital Typography*, CSLI Publications, 2000.

données), la communauté d'utilisateurs visée, etc. L'encodage peut faire l'objet d'une norme ou non — nous traiterons de la question de la normalisation des encodages à la fin de cette section.

En considérant la notion juridique de « lisibilité » dans le contexte des documents électroniques, il faut garder à l'esprit que tout encodage est inclus dans un chaîne d'autres encodages. Le simple affichage d'une lettre à l'écran est le fruit d'une interaction touffue de ces encodages : encodage des caractères (ASCII, Unicode), polices de caractères (PostScript, TrueType), structuration de l'information sous forme d'un document (Word, Wordperfect), structuration de l'information (XML, etc), couleur (ColorSync, etc), modèle d'imagerie (GDI, Quickdraw, etc). Chacun de ces encodages évolue selon une dynamique qui lui est propre et qui varie selon des facteurs économiques, problématiques techniques, influences historiques. De plus, un format d'encodage ne peut être compris que comme un élément donné dans la chaîne totale des équipements qui le rend intelligible : un fichier Word ou HTML est toujours conçu pour être jumelé au logiciel Word ou à un fureteur Web, lui-même conçu pour un certain modèle d'ordinateur et un certain système d'exploitation. Du point de vue du groupe de travail, ceci souligne que la notion de *lisibilité d'un document électronique ne peut être comprise en dehors de l'interaction de l'ensemble de ces encodages avec le logiciel et le matériel informatique conçu pour les interpréter.*

2.1 Grille d'évaluation des formats d'encodage

Dans le contexte de la sélection d'un encodage approprié à l'acte authentique électronique, il faut considérer un ensemble de questions :

1° **Composition** : Peut-on composer le document à partir de bases de données existantes? Comment peut-on créer le document à partir d'archives papier? Peut-on le créer à partir d'un document à la volée?

2° **Extraction** : Comment peut-on extraire de l'information structurée du document?

3° **Forme et fond** : L'encodage donne-t-il une forme fixe au document (ou, préservation des qualités visuelles du document?) L'encodage respecte-t-il la forme du document? La présentation du document varie-t-elle selon les équipements?

4° **Signature** : Quel type de signature l'encodage permet-il ? (cryptographique, biométrique, stéganographique, image?)

5° **Modifications** : L'encodage permet-il de faire des ajouts, modifications, annotations? Comment ces annotations sont-elles archivées?

6° **Normalisation** : Cet encodage est-il normalisé? Quelle est la nature de cette norme? Quelles sont les institutions qui ont créées cette norme? Quelles sont les perspectives de pérennité de cette norme?

7° **Lisibilité** : Comment l'encodage est-il couplé à un outil de lecture?

8° **Traductibilité** : L'encodage est-il susceptible d'être traduit en un autre encodage?

Encore une fois, le manque de temps et de moyens ne me permettront pas de traiter systématiquement de chacun de ces points individuellement. Dans le cadre qui nous concerne, on peut considérer les encodages suivants : 1°) texte « brut » ; 2°) Word et RTF ; 3°) HTML ; 4°) XML ; 5°) PostScript et PDF ; 6°) JPEG et TIFF. Chacun de ces formats est représentatif d'une façon particulière de concevoir la notion de document, le plus souvent à l'exclusion des autres notions. Pour chacun des exemples, j'ai tenté de fournir une représentation de l'encodage, quand c'était possible (ce n'est pas le cas pour

un fichier TIFF), de façon à rendre la notion d'encodage moins abstraite. Une telle « cuisine » informatique n'est pas sans utilité pour mieux comprendre les défis que représente concrètement l'authenticité électronique. [4]

2.2 Le format texte

C'est le niveau zéro de l'encodage d'un document, puisque tous les éditeurs de texte permettent d'afficher, lire, et imprimer des documents en format « texte ». Ce qui ne signifie par pour autant que ce soit un format universel, puisque chacun des trois systèmes d'exploitation dominants — Windows, Macintosh et Unix — codifient le format texte différemment, en utilisant des marqueurs de fin de ligne différents. En format texte, peu d'informations sont gérées : le format se contente de gérer les caractères alphanumériques, ainsi qu'un certain nombre de caractères « blancs » — retour de chariot, fin de ligne, espace blanc, espace de tabulation, fin de fichier, etc. Le plus souvent, ces caractères sont codés en ASCII, mais ce codage ne spécifiant pas la représentation des caractères accentués, il sera graduellement remplacé par le standard UNICODE. [5]

Au sein de la communauté informatique, le format texte jouit d'une grande popularité pour la création de documents. Le plus souvent, les programmes informatiques sont écrits à l'aide d'éditeurs de texte programmables extrêmement sophistiqués (Emacs, Alpha, etc). Si le format ne permet pas de jouir d'aides visuelles comme le changements de polices ou de style au sein d'un document, ces éditeurs étagent les lignes et colorent les mots-clés d'un programme, de façon à le rendre plus facilement intelligible. Dans ce cas particulièrement, le texte devient véritablement fonction de l'interaction dynamique entre logiciel de lecture et fichier.

2.2.1 Exemple d'un fichier texte

```
Longue vie à l'acte authentique électronique!
```

On voit qu'aucune information particulière n'est conservé quant à l'apparence du document — pas d'informations sur la police de caractère, la taille, l'italique ou le gras, etc. On gère les espaces blancs et les caractères, c'est tout. C'est cette simplicité qui lui permet cependant une grande universalité, mais comme pour tout les formats d'encodage, c'est l'interaction entre du matériel, du logiciel, et un document qui permet d'afficher et d'imprimer cette phrase.

2.3 Les formats Word et RTF

L'encodage des fichiers crées par les différentes versions des logiciels de traitement de texte Word est le meilleur exemple d'une norme qui s'est imposée *de facto*. Bien que cet encodage aie été entièrement conçu par Microsoft, il s'est imposé du seul fait que le logiciel lui-même s'est imposé. Ainsi, il est courant d'échanger des documents en format Word, car la plupart des utilisateurs assument que tous et chacun disposent du logiciel pour les lire. Il existe aussi des logiciels qui permettent uniquement de lire des fichiers Word, sans pouvoir les modifier. [6]

4. Pas nécessaire d'être diplomé en chimie pour réussir une génoise mais encore faut-il en connaître un peu sur l' interaction entre les œufs, la farine, l'air et la chaleur.

5. Ce standard vise à pouvoir encoder l'ensemble des alphabets, permettant d'encoder plus de 65 ■■■ caractères différents, incluant l'ensemble des idéogrammes chinois, japonais, et coréens — voir `http://www.unicode.org`.

6. Voir Icword pour le Macintosh (`http://www.icword.com`), Microsoft Reader pour Windows (`http://www.microsoft.com/reader/`), pour Windows, et Ted (format RTF) pour Unix (`http://www.nllgg.nl/Ted/`).

Le format Word est avant tout conçu pour répondre à des besoins d'éditions modestes et variés, allant de la rédaction d'un thèse à la celle de lettres. Le logiciel est conçu dans une optique où le document est tout simplement imprimé sur papier, et son paradigme dominant est ainsi le fameux WYSIWYG, *What You See Is What You Get*, c'est-à-dire que le logiciel donne au texte la même apparence à l'écran que celle qu'il aura sur papier.

Word permet également de structurer l'information de façon assez sophistiquée. Cela a commencé avec la fonction de gestion des envois postaux de masse, mais ces fonctions sont exploitées par les logiciels de rédactions d'actes notariés, par exemple, pour échanger de l'information entre le logiciel et l'acte en cours de rédaction. Cette structuration de l'information ne fait l'objet d'aucune norme, elle est simplement interne à Word.

Il existe un format créé pour faciliter l'échange entre les différentes logiciels de traitement de texte (Word, WordPerfect, etc), le format RTF *(Rich Text Format)*, comme son nom l'indique, est un format texte mais qui spécifie des paramètres quant à la police, etc. Ce format a été élaboré par Microsoft pour permettre l'échange de fichiers entre les différents traitements de texte. Ce format n'est jamais rédigé directement, mais plutôt produit par les logiciels de traitement de texte, et tous les logiciels commerciaux le lisent, si ce n'est pour assurer un minimum d'interopérabilité avec le joueur dominant du marché — Microsoft Word.

2.3.1 Exemple d'un fichier RTF

```
{\rtf1\mac\deff2
{\fonttbl{\f2\froman New York;}
{\f20\froman Times;}
{\f22\fmodern Courier;}
{\stylesheet{\f16 \sbasedon222\snext0Normal;}}
{\info}\paperw11900\paperh16840\margl1701\margr1701\margt1417\margb1417
\deftab709\widowctrl\ftnbj\sectd \sbknone\linemod0\linex0\headery1077
\footery1077\cols1\colsx709\endnhere\pard\plain \qc \f16
{\f20\fs96 Longue vie \'88 l\rquote acte authentique \'8electronique!}
{\f2010\fs96 \par }}
```

Les informations du fichier RTF permettent donc à chaque application de reconstruire le document, incluant les notes de renvois, de gérer les caractères accentués, etc. Cette traduction n'est pas toujours parfaite, dans le cas de documents très complexes.

2.4 Le format HTML

Le HTML *(Hyper-Text Markup Language)* est évidemment le langage développé pour le Web — c'est celui que les fureteurs *Netscape Navigator*, *Microsoft Explorer* et autres peuvent lire et traduire de façon à afficher des pages Web. Ce langage est fortement inspiré du SGML, langage développé par l'armée américaine dans le but de gérer la documentation des équipements militaires — nous reparlerons des caractéristiques du SGML dans la section traitant du XML. La philosophie ayant guidé la conception du HTML était celle de définir un langage simple permettant de créer rapidement des documents « hypertextes », c'est-à-dire intégrant des liens sur des objets distribués sur l'ensemble du réseau — autres pages, images, documents, etc. Un document n'est donc plus une entité fixe locale, mais devient un assemblage dynamique d'éléments distribués au travers du réseau.

Sa grande simplicité a beaucoup contribué à sa popularité, simplicité qui a permis à nombres de personnes sans formation technique particulière de pouvoir publier sur la toile, sans avoir à absorber des masses d'informations techniques indigestes — on peut créer une page Web en quelques heures à peine, « à la main », ou à l'aide de logiciels conçus à cet effet.

La définition du langage est sous la responsabilité du *Word-Wide Web Consortium* (W3C) et cette définition a été l'objet de guerres rangées entre les fabricants (Netscape et Microsoft) qui ont tenté de créer des marchés pour leur fureteur — un exemple criant où un encodage est devenu un enjeu stratégique crucial. Cette guerre semble actuellement perdre de son importance, alors que le HTML semble vouloir être ultimement être remplacé par le XML. [7]

Le HTML effectue une certain structuration des données à l'aide de « marques ». Par exemple, dans l'exemple ci-dessous, on peut diviser le document en deux parties, d'une part, l'en-tête, incluse entre les marques <HEAD> et </HEAD>, et d'autre part, le corps du document, inclus entre les marques <BODY> et </BODY>. Ces régions du texte sont ainsi structurées et on peut leur appliquer des traitements distincts. Cependant, cette structuration est imparfaite, pour deux raisons : d'une part, les utilisateurs ne peuvent définir une structuration qui leur est propre, et doivent nécessairement utiliser celle définie par le langage, et d'autre part, cette structuration mêle la forme et le fond, c'est-à-dire que le fureteur associe à une structure donnée une représentation donnée. C'est à ce niveau que le XML tente de corriger les faiblesses du HTML.

2.4.1 Exemple d'un fichier HTML

```
<HTML>
    <HEAD>
        <META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
        <META NAME="Generator" CONTENT="Microsoft Word 98">
    </HEAD>

    <BODY>
        <FONT FACE="Times" SIZE=7>
            <P ALIGN="CENTER">
                <A HREF="http://www.internet.gouv.fr/pubs/acte-authentique.html">
                    Longue vie &agrave; l&#146;acte authentique &eacute;lectronique!
                </A>
            </P>
        </FONT>
    </BODY>
</HTML>
```

Le document fait ici référence à un autre document sur la Toile, à travers le mécanisme des liens hypertextes. Les marques <A> et </A> créent un lien entre le document situé à l'adresse `http://www...acte-authentique.html` et le texte « Longue vie à l'acte authentique électronique! ». Ainsi, lorsque l'on clique sur le ce texte, le fureteur localise le document indiqué dans le lien et le charge à

7. Il est cependant à parier que Microsoft développera ses propres modifications au standard XML, de façon à en faire un outil stratégique de structuration du marché. Ce type de logique est particulièrement tenace chez ce fabriquant et les premiers signes sont déjà dans l'air : voir Margret JOHNSTON « XML Factions Develop Along Familiar Lines » InfoWorld.com, 14 décembre 2000, qui note que « si Microsoft est largement en avance sur ses compétiteurs dans le marché du XML, la société n'entretient pas une relation exceptionellement ouverte avec les gens qui définissent les mécanismes de la conversation ».

l'écran.

On voit aussi ici la façon dont différents type de normes sont intégrés au sein du format HTML. Par exemple, la référence à `CONTENT="text/html; charset-iso-8859-1"` fait référence à la norme multimédia de types MIME, qui permet à différents logiciels (principalement, les logiciels de courriels et les fureteurs Web) de gérer correctement les différents types d'objets que ces applications rencontrent. Dans ce cas-ci, un fureteur sait qu'il a affaire à un fichier HTML, de type « texte », que ce texte est encodé en ISO-8859-1, ce qui permet de choisir l'affichage approprié pour les caractères accentués. On voit bien ici comment les différentes normes sont imbriqués les unes dans les autres. La référence à `&agrave` permet d'encoder l'accent grave de façon à ce qu'il soit portable entre les différentes plate-formes. De même, l'apparence du texte est déterminé par `FONT FACE="TIMES" SIZE=7` fait référence à une autre norme — celle définissant la police de caractère Times, et une taille, 7.

2.5 Le format XML

Le XML est une norme relativement récente, mais qui connaît actuellement une progression fulgurante. Le XML veut remplacer le HTML comme langage du Web, celui-ci n'ayant jamais été conçu pour répondre aux besoins auquel il fait face aujourd'hui — le commerce électronique entre autres. Le XML est un sous-ensemble épuré du SGML, adapté aux exigences du Web. [8] La finalité du langage en est une d'*échange de données*, mais plus encore, de remplacer complètement tous les formats propriétaires de traitements de texte et d'édition électronique. A long terme, les concepteurs du langage désirent que tous ces programmes produisent du XML et du XSL *(eXtensible Style Language)*, dont la combinaison pourrait répondre à tous les besoins imaginables d'édition, quelque soit la plate-forme informatique, quelque soit l'application. [9]

Le XML est une norme promulguée et gérée par le W3C *(World-Wide Web Consortium)*, organisme fondé par Tim Berners-Lee, un des inventeurs du Web. [10] Le W3C est, avec l'IETF, une de ces nouvelles institutions qui exercent une influence considérable sur le développement des normes techniques du Web et de l'Internet. Est-ce dire que le XML est un standard « ouvert »? On peut dire qu'il n'est pas propriétaire, au sens où aucune société ne contrôle directement la définition de la norme. Cependant, ceci ne signifie pas que tout un chacun peut participer au processus de rédaction de la norme — les membres du W3C sont principalement des corporations, le membership se payant à coup de $50 000 dollars.

Un document XML est en fait composé de trois parties : il faut premièrement définir les catégories qui seront utilisées pour coder les données, au sein d'un DTD, *Document Type Definition*. Alors que cette catégorisation est implicite en HTML et ne peut être étendue par l'usager, Le DTD permet de définir au gré de l'utilisateur la structuration des données. Par exemple, supposons qu'un usage désire définir une catégorie de données « Nom de jeune fille », catégorie susceptible d'être utilisée pour un acte juridique. La catégorie serait définie au sein d'un DTD, selon les règles du langage XML :

```
<!DOCTYPE acte-authentique>[
<!ELEMENT acte-authentique (notaire, parties*, acte)>
```

8. Un tel processus de simplification n'est pas inhabituel en informatique — ainsi, un des langages les plus utilisés en intelligence artificielle, le LISP a incorporé au fil des années tant d'ajouts que sa spécification dépasse les 1000 pages. Le langage Scheme incorpore les principales caractéristiques du LISP, mais sa spécification ne dépasse pas les quarante pages.

9. Voir Bosak, "Four myths about XML", disponible sur le site `www.w3c.org/`.

10. Voir le site `www.w3c.org`.

```
<!ELEMENT notaire (nom, addresse)>
<!ELEMENT nom (famille, prenom, nom-de-jf)>
<!ELEMENT famille (#PCDATA)>
<!ELEMENT prenom (#PCDATA)>
<!ELEMENT nom-de-jf (#PCDATA)>
<!ELEMENT parties ... <!ELEMENT acte ...>
```

Cette DDT fictive et simplifiée définit une structure `acte-authentique`, qui contient des éléments `notaire`, `parties`, et `acte`. L'élément `notaire` est lui même défini comme étant constitué de la composition d'un élément `famille` et `prénom`, ces éléments étant eux-mêmes définis comme correspondants à des chaînes de caractères (`#PCDATA`).

Le document XML lui-même contiendra les données de l'acte authentique, données qui ne seront interprétables qu'en présence du DTD. Un document XML peut aussi contenir un lien sur un DTD, à la façon d'un lien hypertexte. Ainsi, l'interprétation d'un document XML peut être fonction d'un document non-local, situé ailleurs sur le réseau.

```
<acte-authentique>
    <notaire>
        <nom>
            <famille>Gard</famille>
            <prenom>Martine</prenom>
            <nom-de-jf>Gagné</nom-de-jf>
        </nom>
    </notaire>
    <parties>
    ...
    </parties>
    <acte>
    ...
    </acte>
</acte-authentique>
```

L'apparence du document est déterminée par un troisième document, une feuille de style exprimée en XSL. [11] Cette feuille de style a pour but de complètement dissocier l'apparence du document des données contenues dans le document. Ainsi, on peut associer à une donnée structurée une certaine apparence. Dans l'exemple qui suit, la feuille de style traduit un document XML en un document HTML. Pour chaque catégorie de données définie dans le DTD, on définit un patron (« template ») qui traite la représentation de chaque catégorie. Le template `acte-authentique` définit un document HTML dont la section `<body>` comprendra les trois catégories `notaire`, `parties`, et `acte`. La catégorie `notaire` est traitée par un autre patron, qui s'occupe d'aligner le nom et le prénom du notaire, et de les précéder par « Maître ».

```
<xsl:template match="acte-authentique">
  <html>
    <head><title>Un acte authentique</title></head>
      <body>
        <xsl:apply-templates select="notaire"/>
```

11. A noter que la spécification du XSL n'est pas encore, à ce jour, complétée.

```
            <xsl:apply-templates select="parties"/>
            <xsl:apply-templates select="acte"/>
        </body>
    </html>
</xsl:template>

<xsl:template match="notaire">
    Maître
    <xsl:value-of select="famille"/>,
    <xsl:value-of select="prénom"/><p>
    <xsl:value-of select="nom-de-jf"/>,
</xsl:template>
```

Les feuilles de style permettent d'adapter la présentation d'un document XML au périphérique de visualisation : pour un même document, une feuille de style pourra ajuster l'affichage à l'écran d'un portable, d'un ordinateur personnel, ou d'un kioske Internet public. Ce découplement entre forme et fond représente un des atouts majeur du XML, mais évidemment, le document n'est pas — ne peut être — affiché identiquement dans chaque cas !

On voit ainsi que le format XML met en place une machinerie complexe, et que le résultat final, tant à l'écran qu'à l'impression, dépend de l'interaction de plusieurs fichiers, possiblement distribués à différents endroits sur le réseau, de même que de la mécanique d'interprétation contenue dans le logiciel de lecture.

2.6 Format de fichiers d'images

Un format image (on utilise parfois les termes *raster* ou *bitmap*) est un format qui encode une image selon un quadrillage dont la densité définit la résolution de l'image. Pour mieux comprendre cette définition, il est utile de saisir comment fonctionne trois périphériques informatiques essentiels au document numérique : l'écran, l'imprimante, et le scanner.

L'écran d'un ordinateur est composée de centaines de milliers de points lumineux, les *pixels*. La densité des pixels à l'écran varie selon les plates-formes : le Macintosh, par exemple, assigne 72 pixels à chaque pouce d'écran et on dit qu'il a une résolution de 72 points par pouce (ppp). Le pixel est susceptible de variations de couleur (au minimum, le noir et le blanc), et d'intensité lumineuse. A chaque pixel est assigné un certain nombre de bits — l'unité d'information binaire. Pour un écran noir et blanc, un seul bit est nécessaire (0 = pixel éteint, 1 = pixel allumé), alors que pour un écran couleur, le nombre de couleurs détermine le nombre de bits nécessaire (256 couleurs = 8 bits, 16 millions = 24 bits).

Une imprimante laser fonctionne d'une façon similaire : elle divise aussi la surface de la feuille de papier en un quadrillage de minuscules points (d'encre) , mais ce quadrillage est plus dense que celui d'un écran d'ordinateur — une imprimante laser typique assigne 300 ou 600 points par pouce, alors qu'une imprimante de qualité industrielle (RIP) peut atteindre une résolution de plus de 3300 ppp.

De même pour un scanner : il échantillonne la surface (analogue) d'un document en une image (numérique) d'une certaine résolution. Le scanner lui aussi définit un quadrillage dont la densité est

définie par l'utilisateur et/ou par les capacités du scanner. Plus le quadrillage est dense, plus le fichier résultant de la numérisation sera gros : un fichier numérisé à 72 ppp sera 25 fois moins volumineux qu'un autre numérisé à 360 ppp, puisque chaque pouce carré de l'image sera échantillonné selon un quadrillage 25 fois moins dense. Ainsi, il y a un rapport direct entre la taille d'un fichier image et sa résolution.

La résolution finale d'une image est fonction à la fois de sa propre résolution et de celle du périphérique de visualisation : on peut très bien afficher une image de résolution 300 ppp sur un écran de 72 ppp, mais l'image ne pourra avoir plus de 72 ppp de résolution à l'écran. De même, on peut très bien imprimer une image de résolution 72 ppp sur une imprimante de 300 ppp, elle n'aura toujours que 72 ppp de résolution.

L'intérêt du format image, c'est qu'il reproduit, justement, une image. Les caractéristiques visuelles d'un document sont préservés : mise en page, marques manuscrites — la signature, par exemple. De plus, c'est la façon la plus simple de numériser les archives papiers, en obtenant tout simplement une image électronique de chaque page d'un document, et en liant ces pages par un mécanisme d'indexation approprié. Le format image permet ainsi de joindre l'univers papier et l'univers électronique. Cependant, un format image n'assigne aucune structuration sémantique aux données contenues dans l'image. En particulier, le texte écrit est compris en tant qu'image, et non en tant que suite de caractères intelligibles. Pour que l'ordinateur soit en mesure d'effectuer des traitements sur le texte contenu dans un fichier image, il faut effectuer une opération ultérieure de *reconnaissance optique de caractères*.

Il existe des centaines de formats d'image : parmi les plus connus le format JPEG, format produit par ISO et l'ITU, et le format TIFF *(Tagged Image File Format)*, dont la norme appartient à présent à la société Adobe. [12]

2.7 Les formats PostScript et PDF

Un des problèmes des fichiers image que l'on vient de décrire, c'est que l'on doit décider une fois pour toute de la résolution du fichier que l'on crée. Comme on l'a vu, rien ne sert d'imprimer un fichier de résolution 72 ppp sur une imprimante de 2400 ppp. Il faut donc conserver les fichiers à la meilleure résolution possible, mais ceci implique des fichiers de grande taille. Le langage PostScript propose une solution pour résoudre ce problème, en décrivant des images d'une façon uniforme quelle soit la résolution du périphérique d'impression, à l'aide d'équations vectorielles. Ainsi, dans un chaîne de production graphique, on peut disposer d'imprimantes de résolution très différentes connectées au même ordinateur — 300, 600 ppp, ou encore une Linotronic à même de produire du film en quatre couleurs, à des résolutions de 3386 ppp. Un document décrit en langage PostScript peut être envoyé à tout périphérique qui supporte le langage PostScript, quelque soit sa résolution, en produisant un résultat adapté à chaque type de périphérique. De plus, pour des documents de texte, le fichier PostScript correspondant peut être très compact, puisque d'une part, les polices de caractères PostScript les plus courantes sont conservées en mémoire directement sur l'imprimante, et d'autre part, qu'elles sont décrites sous formes d'équations vectorielles.

12. Les services du Journal officiel, par exemple, numérisent chacune des pages du JO sous forme de document TIFF. Ainsi, le texte de la loi du 13 mars 2000 est disponible à l'URL `http://tif.journal-officiel.gouv.fr/2000/03968001.tif`.

Le PostScript est un langage informatique de description de page *(page description language)* — c'est-à-dire que c'est un langage de programmation dont la seule finalité est de décrire des pages. Le langage est produit par un pilote d'impression, qui agit comme une interface entre l'ordinateur et l'imprimante. Le pilote produit un fichier PostScript qui est ensuite envoyé à un *interprète PostScript* résidant sur le périphérique d'impression. Cet interprète (qui prend la forme d'une puce dédiée) effectue la traduction entre les commandes contenues dans le fichier, et les caractéristiques matérielles du périphériques (résolution, taille du papier, couleur, etc.). Ce mécanisme permet donc d'effectuer la traduction entre d'une part, des plates-formes informatiques différentes (Macintosh, Windows, etc), et, d'autre part, des périphériques d'impression extrêmement variés. [13]

Le PostScript a été à l'origine d'une petite révolution informatique qui a fortement contribué à l'essor du micro-ordinateur, en permettant à tout un chacun de disposer d'outils compatibles de mise en page et d'impression de qualité professionnelle, et cette norme est aujourd'hui presque universelle au niveau des imprimantes. Il est aussi possible de représenter des fichiers PostScript à l'écran, à travers des applications comme Ghostview, qui traduisent un fichier PostScript dans le modèle d'image utilisé pour Windows (GDI) et Macintosh (QuickDraw). La défunte plate-forme d'ordinateur NeXT avait adoptée une norme d'affichage Display PostScript, mais cette norme n'a jamais rencontré, de loin, le succès qu'a eu le PostScript au niveau de l'impression.

Le format PDF est basé sur le langage PostScript, et reprend sa philosophie. Alors que l'objectif du PostScript est de pouvoir disposer représenter une page de manière qui soit indépendante de la résolution du périphérique d'impression, l'objectif du PDF est de pouvoir représenter un document de la même manière, indépendamment de la plate-forme et de l'ordinateur utilisé — un document devrait apparaître de la même façon sur un Macintosh, un PC ou une station Unix. Ce problème est loin d'être trivial, puisque ces plates-formes différents dans nombres d'aspects qui influencent directement la représentation d'un document à l'écran : encodage des caractères accentués, standard des polices de caractères (PostScript ou True Type), etc.

Le format PDF peut-être produit à partir de tout logiciel, en utilisant un logiciel qui se substitue à un pilote d'impression : toute application susceptible d'imprimer peut ainsi produire du PDF, de la même façon qu'elle peut produire du PostScript. Le PDF se situe donc à un niveau plus intermédiaire dans la chaîne de production d'un document : on n'écrit pas un document directement en PDF, on produit le document dans le logiciel approprié et ensuite, on produit du PDF à partir de ce logiciel. C'est cette position intermédiaire qui donne au PDF sa grande inter-opérabilité.

A partir d'un document papier, plusieurs stratégies de capture sont possibles : on peut produire un document PDF qui ne contient qu'une image numérique du document, ou appliquer des outils de reconnaissance automatique de caractères, de façon à produire un document qui contient à la fois une image numérique du document et une représentation sémantique du texte, susceptible d'être indexée. Ce format permet ainsi de conserver une représentation visuelle exacte du document tout en offrant la possibilité d'effectuer des recherches dans le texte — un encodage qui tente de mitiger les inconvénients du format image en conservant une certaine « intelligence » au texte.

La société Adobe a habilement manœuvré de façon à promouvoir l'utilisation du PDF comme norme d'échange de documents sur la Toile : tout d'abord, le logiciel de lecture du format PDF est

13. A une certaine époque, l'installation d'un traitement de texte sur PC exigeait au fournisseur de fournir des pilotes d'impression pour *toutes* les imprimantes susceptibles d'être connectées à l'ordinateur (des centaines). Avec le PostScript, un seul pilote est nécessaire et il suffit de développer un interprète PostScript pour chaque périphérique d'impression.

gratuit, facilement disponible, et il a été développé pour toutes les plate-formes — Windows, Macintosh, toutes saveurs d'UNIX, etc. Ensuite, les logiciels Acrobat Capture permet de numériser des documents papier en des documents PDF et en conservant au maximum l'apparence et la mise en page des documents. Le format incorpore en plus des aspects interactifs : liens hypertextes, signets, signature électronique, chiffrement, etc. Au-delà d'un simple encodage de documents, le format PDF tente donc de réaliser tout le potentiel du document électronique. Les qualités de ce format lui assurent un succès important, et il faut compter que celui-ci ira en grandissant.

Les formats PostScript et PDF sont tous deux gérés par la société Adobe, qui précise dans le *PostScript Language Reference, 3rd edition* que la société détient le droit d'auteur sur la spécification écrite du language, mais que toute personne peut 1° Écrire un programme dans le language PostScript; 2° Écrire des programmes qui génère comme sortie un programme se conformant à la spécification PostScript; 3° Écrire des logiciels qui interprètent des programmes PostScript. [14] La norme n'est donc pas ouverte, mais ceci ne l'a pas empêché d'être un instrument fédérateur de l'industrie, et n'a pas nécessairement nui à son adoption.

2.7.1 Exemple d'un fichier PostScript

```
%!PS-Adobe-3.0
%%Title: (aae.doc)
%%CreationDate: (11:43 Lundi 16 octobre 2000 )
%%Pages: 1
%%Orientation: Portrait
%%EndComments
[...]
%%BeginFeature: *PageSize A4Small
<</PageSize_[595_842]_/ImagingBBox_null>>_setpagedevice
%%EndFeature
%%EndSetup
%%Page: 1 1
[...]
gS 0 0 538 781 rC
86 75 :M
f57 sf
-.174(Longue vie \210 l\325acte)A
158 123 :M
-.192(authentique)A
143 171 :M
-.181(\216lectronique!)A
endp
showpage
%%Trailer
end
%%EOF
```

Le fichier commence par un certain nombre de commentaires, ignorés par l'interprète PostScript, qui fournissent certaines informations sur les conditions de création du fichier — titre, nombre de pages, etc. Ensuite, la commande `BeginFeature` montre une commande envoyée à l'interprète indiquant que le document est de format `A4`. La troisième partie du fichier montre les commandes pour

14. Ceci fut initialement l'avantage commercial d'Adobe, qui retirait des droits pour chaque imprimante laser qui incorporait un interprète PostScript, fourni exclusivement par Adobe.

afficher le texte (les accents sont représentés par leur code ASCII). La dernière commande, `showpage`, enjoint à l'interprète d'imprimer la page.

2.8 Pourquoi une norme?

A l'issue de ce rapide survol, on voit qu'il n'existe pas de solution évidente à la question de l'encodage des actes authentiques — aucun des formats d'encodage proposés n'a été conçu pour répondre aux exigences spécifiques de ce type de document. Le décret doit-il alors imposer l'adoption d'une format d'encodage précis pour l'acte authentique électronique? Si c'est le cas, quelles devraient être les caractéristiques de cette norme, et pourquoi? Plus problématique encore, si chacun des formats d'encodage fait jouer une machinerie informatique complexe dont le résultat final est la visualisation d'un document, à l'écran ou sur papier, ce processus n'a que peu à voir avec le concept de « lisibilité » tel qu'on l'entend dans le contexte de l'écrit papier. Comment doit-on repenser ce concept de lisibilité, étant donné la nouvelle donne technologique du document?

Certains ont suggéré qu'il était essentiel que le format adopté soit 1°) normalisé; 2°) que cette norme soit stabilisée; 3°) qu'elle soit aussi ouverte que possible, de façon à favoriser les échanges; 4°), que ce format soit transparent, de façon à garantir au signataire qu'il n'existe aucune donnée ou instruction cachées dans le fichier qu'il valide. Il est utile d'examiner attentivement chacun de ces arguments, car ils reviennent régulièrement dans les discussions portant sur les normes.

Norme: Tout d'abord, pourquoi faut-il déterminer un format particulier d'encodage pour l'acte authentique? Qu'y gagne-t-on, mais aussi, qu'y risque-t-on? Est-ce que d'adopter une norme est la réponse aux besoins exprimés par les acteurs de l'acte authentique? Les normes de format de fichier décrits dans ce chapitre sont, avant toute chose, des instruments stratégiques industriels : leur évolution est soumise à des impératifs qui ont peu à voir avec la logique de l'acte authentique.

Stabilité: Il est difficile de jauger précisément ce que représente la stabilité d'une norme technique, dans l'univers informatique. Parmi les formats que nous avons envisagé dans cette section, le XML est certainement la moins stabilisée de toutes, mais son ampleur probable procure un certain gage de stabilité future.

Ouverture: On entend souvent vanter les mérites d'une norme, en ce qu'elle est « ouverte », par opposition à une autre qui serait, plus vénalement, « propriétaire ». Une norme ouverte est une norme dont le contenu est non seulement connu de plus, mais en plus, qui est déterminée par un processus de discussion et de consultation entre les acteurs du domaine d'intérêt de la norme. Un format propriétaire est défini par une seule société — par exemple, le format de fichier du traitement de texte Word 2000 ne dépend que de la société Microsoft. Malheureusement, la plupart des normes ne peuvent être identifiées à un de ces deux pôles, mais se situent plutôt quelque part dans une vaste zone intermédiaire. En fait, les nouvelles institutions à la base du développement des standards Internet sont difficiles à aligner selon une grille classique « institutions publique $\Longleftrightarrow$ institutions privées » qui produiraient des normes respectivement « ouvertes $\Longleftrightarrow$ propriétaires » : l'IETF, le W3C, l'ICANN sont des instances de normalisation encore difficiles à classer.

Transparence: L'argument revient souvent qu'il faut éviter qu'un fichier informatique encodant un acte authentique électronique ne puisse contenir un virus ou une macro susceptible de modifier le

contenu de l'acte. Le virus « I LOVE YOU » n'était-il pas précisément une telle instance d'un « document exécutable », capable de faire exécuter par l'ordinateur toute une série d'actions néfastes? Selon cet argument, un format d'encodage « transparent », non susceptible de contenir des instructions informatiques serait plus sécuritaire qu'un format « non-transparent ». Une telle analyse ne tient cependant pas compte du fait qu'un document électronique est le résultat de l'interaction entre des composantes fichiers, des composantes logicielles, et des composantes matérielles : un document « transparent » comme du HTML ou du XML peut tout à fait faire appel à des ressources (code Java par exemple) distribuées ailleurs sur le réseau, susceptible d'avoir une influence sur le document. En fait, le problème est beaucoup plus étendu que la simple possibilité de virus cachés dans les fichiers : sur un ordinateur commercial, il est à toute fin pratique impossible de *garantir* que le processus de signature ne soit usurpé, à un moment ou un autre. [15] La notion du *What You See Is What You Sign* ne capture qu'une petite partie de ce problème et va exiger d'être considérablement raffinée et explicitée avant qu'elle puisse être opérationalisée, tant juridiquement que techniquement.

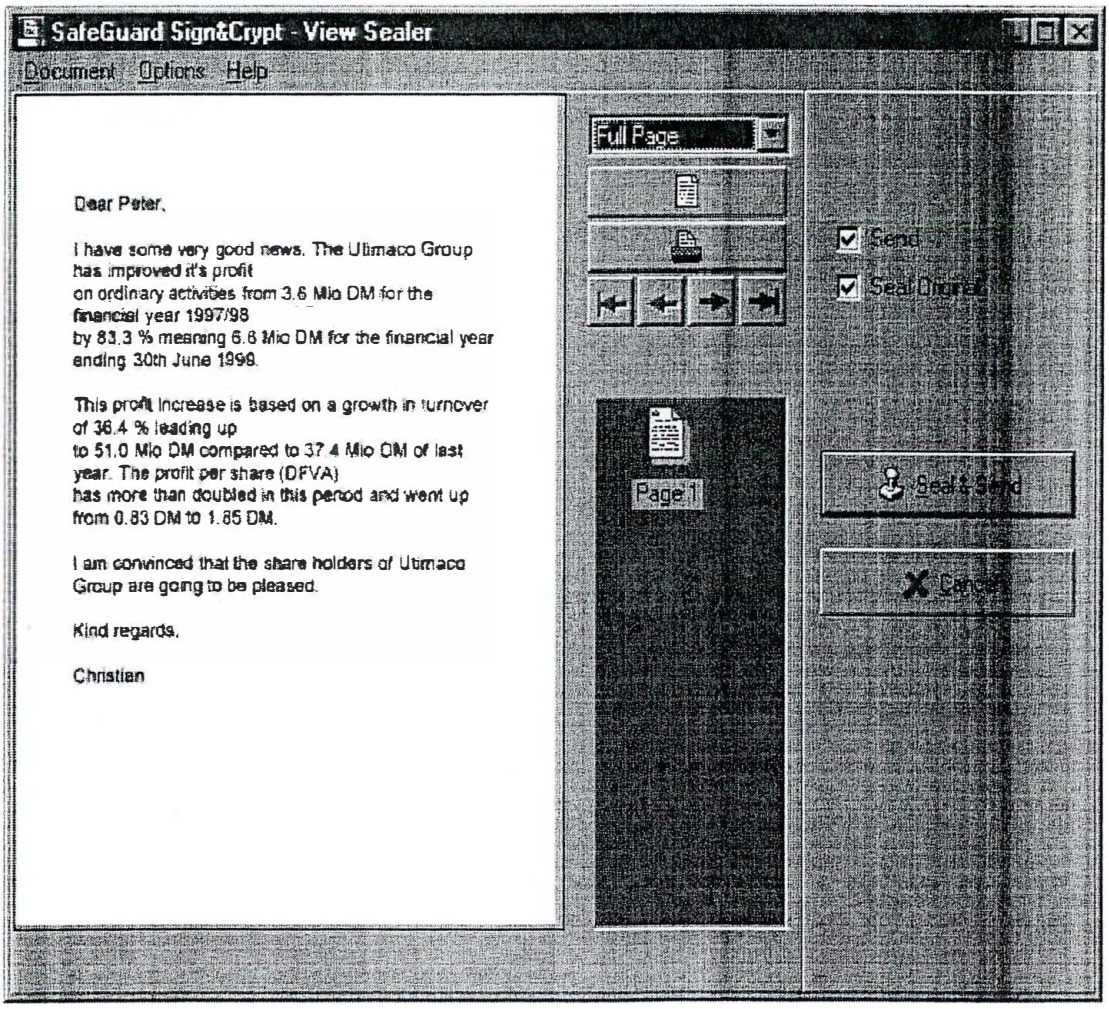


FIG. 2.1 – *Utilisation du format TIFF pour le* What You See Is What You Sign

15. Voir à ce sujet l'analyse de Bruce SCHNEIER, qui considère que la seule solution réside dans l'utilisation d'un terminal de signature dédié et certifié, un ordinateur personnel multi-usages étant, à tout fins pratiques, impossible à sécuriser. Voir Bruce SCHNEIER *Secret and Lies: Digital Security in a Networked World*, John Wiley and Sons, 2000.

Quelque soit la validité de cette analyse, le format TIFF a été adopté pour la réalisation de procédés de signature électronique réalisant le « *What You See Is What You Sign* », par exemple, le procédé « Sign&Crypt » de la société Utimaco : l'idée est d'utiliser un pilote d'impression qui traduit le fichier à signer (fichier Word, par exemple) en un fichier TIFF, de l'afficher à l'écran et de signer ce fichier — voir la figure 2.1. On peut envoyer les deux fichiers, le fichier original et sa version TIFF signée, au destinataire, de façon à pouvoir continuer à travailler sur le document original, tout en disposant d'une image signée du document.

2.9 Quel format d'encodage pour l'acte authentique électronique?

Si l'on décide d'imposer un format d'encodage à l'acte authentique électronique, quel devrait en être les caractéristiques? Les premières réflexions ont désigné le format XML comme celui présentant le plus d'avantages, et ce, pour un certain nombre de raisons : 1°) il permet de distinguer le fond et la forme ; 2°) il se présente sous la forme d'un texte brut encadré par des balises ordonnées hiérarchiquement suivant les spécifications de DTD ou un schéma XML ; 3°) il est directement lisible par l'homme au prix d'un certain effort ; 4°) sa représentation est très simple dans la mesure où un document XML contient uniquement un texte et des balises à l'exclusion de toute macro-commande dans laquelle pourrait être dissimulée un virus ou des données cachées qui viendrait modifier le document après archivage ; 5°) la vision à l'écran ou à l'impression du texte sera toujours la même quel que soit le poste de consultation ou le type de plate-forme ; 6°) il peut être facilement obtenu à partir d'un traitement de texte standard. Il peut être instructif d'analyser ces arguments de plus près.

Le XML permet effectivement de distinguer la forme du fond, mais, dans le contexte de l'acte authentique, c'est plutôt un désavantage, car l'acte authentique, justement, lie intimement la forme et le fond ! [16] Le second argument n'est qu'un constat ; Pour le troisième, pour qu'un document XML soit « directement lisible » par l'homme, il faudrait qu'il puisse simultanément garder à l'esprit le fichier XML, le fichier DDT, et la feuille de style XSL associée, ainsi que tous les documents externes possiblement référencés ; le quatrième argument a été discuté plus haut ; le cinquième est extraordinaire, puisqu'il est difficile d'imaginer comment on peut à la fois dissocier la forme du fond *et*, simultanément, assurer qu'un document aura la même apparence quel que soit le périphérique de visualisation ! ; sixièmement, *chacun* des formats discutés dans cette section sont facilement obtenus à partir d'un traitement de texte standard (Word, par exemple) — texte « brut », RTF, HTML, XML, PostScript, PDF, TIFF.

Il faut donc reposer la question : Quels doivent être les critères de sélection d'un format d'encodage, étant donné les particularités de l'acte authentique électronique? Comment traduire les concepts de lisibilité et de pérennité au niveau du document électronique? [17]

Il faut d'abord considérer que d'autres logiques économiques et techniques sont à l'œuvre. Au niveau de la rédaction de l'acte, le passage à L'XML ne fera que rationaliser un processus déjà largement entamé : la plupart des logiciels de rédaction d'actes combinent actuellement différentes bases de données (bases de clients, clausier, etc) pour produire un modèle de document qui est ensuite

16. Voir à ce sujet les remarques de Mme Yvonne FLOUR, « Les conventions sur la forme » *Répertoire Desfresnois*, 15-16/00, p.911-928, section II: « La forme définit le fond ».

17. Plusieurs excellents documents de réflexion ont été produits à ce sujet par le *Council on Library and Information Resources* — voir *Authenticiy in a Digital Environment*. Council on Library and Information Resources, mai 2000 et G. Lawrence, W. Kehoe, O. Rieger, W. Walters, et Anne Kenney, *Risk management of digital information: a file format investigation*. Council on Library and Information Resources, juin 2000, disponibles sur `www.clir.org`.

transféré à Word pour être sauvegardé et imprimé. L'information est donc déja structurée, mais elle n'est pas susceptible d'être échangée, puisque chaque logiciel définit son propre format de données. Le XML permettra de standardiser ce processus, qui aura alors l'avantage de pouvoir permettre l'échange de données directement entre les administrations et d'automatiser les étapes qui peuvent l'être. Pour tout ce qui concerne les aspects d'échanges de données, le passage à l'XML semble donc assez logique, puisque celui-ci semble vouloir s'imposer comme norme globale de structuration de l'information. La stabilisation de cette norme (et des autres qui lui sont afférentes) sera sans doute néanmoins relativement longue, car on tente ici de définir le langage qui permettra d'effectuer *tous les types d'échanges* de *toutes les sortes d'informations* par le Web.

Le problème, c'est que le XML ne fixe que faiblement la forme visuelle du document — il faut disposer des trois éléments du document, XML, DDT et XSL, et des programmes informatiques qui ont assemblé ces trois fichiers en la représentation visuelle d'un acte juridique. Prétendre que le XML est lisible « directement » ne résout pas la question, puisque c'est faire l'économie de la réflexion qui est l'objet même de la constitution de ce groupe de travail : Que devient la notion de lisibilité à l'ère informatique ? Comment s'assurer que cette lisibilité demeure pérenne ? Il est peu probable que le critère de la « lisibilité directe par l'homme » du fichier d'encodage du document soit la réponse à cette question.

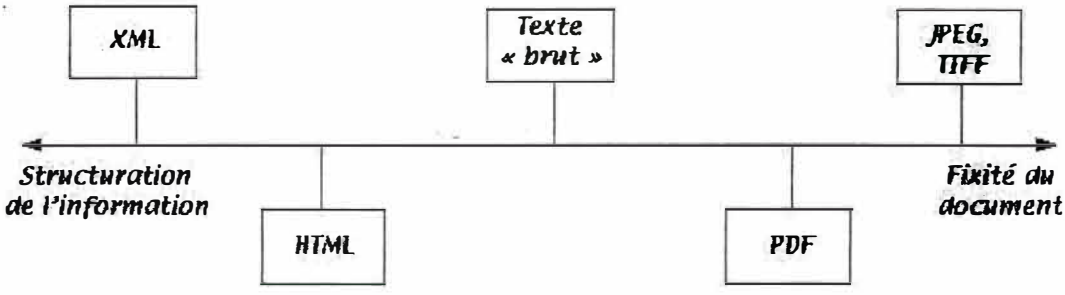


FIG. 2.2 – *Comparaison des différents formats d'encodage*

Les formats d'encodage peuvent être classifiés selon un axe qui oppose structuration de l'information à fixité de la représentation (voir la figure 2.2) : on peut en conclure que l'utilisation du XML comme format d'encodage des actes authentiques électronique est appropriée pour toutes les phases de traitement de l'acte où la finalité d'échange d'information prime, alors que pour les phases de l'acte où l'intégrité visuelle du document prime, il est préférable de se porter vers des formats d'encodage qui nécessitent une machinerie moins lourde que le XML et qui ne concernent que la représentation visuelle de l'acte (PostScript, PDF, JPEG et TIFF).

Chapitre 3

Signature

Plusieurs difficultés se présentent avant même que ne soit possible une discussion de la signature électronique : tout d'abord, le vocabulaire entourant la signature électronique est tributaire des guerres rangées entre les intérêts commerciaux qui s'affrontent pour la conquête des marchés naissants entourant la sécurisation des transactions. Ainsi, alors qu'initialement on utilisait le terme de « signature électronique » pour désigner l'ensemble des technologies de signature et le terme de « signature numérique » pour désigner la signature basée sur la cryptographie, plusieurs documents récents font l'adéquation entre signature électronique et signature cryptographique — par exemple, les rapports de M. Jolibois au Sénat et de M. Paul à l'Assemblée nationale. [1] Dans ce rapport, on utilisera le terme « signature électronique » pour désigner une technologie de signature qui est, à un moment ou à un autre du cycle de vie d'un document, électronique, sans même exclure qu'elle existe sous une forme non-électronique à d'autres moments — ceci dans la perspective d'un œcunémisme technologique le plus inclusif possible.

Ensuite, il faut replacer la signature dans un *contexte global* de sécurité des documents : dans l'immense majorité des cas, l'authenticité — pas celle du droit français, mais la notion plus informelle — du document ne sera jamais contestée, et même dans le cas contraire, la validité de la signature ne sera pas nécessairement au centre du débat, comme le souligne Benjamin Wright :

> « Malgré ce que l'on pourrait en déduire à l'écoute des dramatiques de télévisions axés sur l'univers judiciaire et le procès, l'origine et l'authenticité de la plupart des documents n'est pas prouvée sur la base de signatures. Beaucoup plus souvent, l'origine et l'authenticité sont prouvés à partir d'un ensemble de faits et de circonstances — l'ensemble des relations entre les gens impliqués — le moment, le lieu, les transactions et discussions afférentes, la fonction et le contenu des documents, et non simplement la signature. Plus souvent qu'autrement, l'origine et l'authenticité des documents n'est pas disputée et les parties déclarent simplement que les documents sont bien ce qu'ils apparaissent être. » [2]

Ces remarques sont valables tant pour l'univers du papier que pour l'univers électronique : dans un cas comme dans l'autre, la signature n'est qu'un seul maillon d'une chaîne complexe de facteurs qui, ensemble, garantissent l'authenticité des documents.

Quatre technologies sont ici discutées, chacune représentant trois approches très différentes au

1. De même pour de nombreux commentateurs, par exemple, Thierry PIETTE-COUDOL : « dans la signature électronique, le certificateur vient garantir la clé publique (cryptographique) que le destinataire d'un message signé utilisera pour vérifier la signature. » — *Échanges électroniques, Certification et sécurité*, Paris : Litec, 2000.

2. Benjamin WRIGHT, "The Legality of the PenOp Signature," PenOp White Paper, disponible sur le site www.penop.com.

problème de la signature électronique: la signature cryptographique,[3] la signature biométrique, la signature-tatouage et la signature numérisée. Nous adoptons une attitude agnostique quant à la supériorité de ces méthodes les unes par rapport aux autres.[4] Il faut malheureusement considérer de tels arguments à la lumière des énormes enjeux commerciaux qui entourent l'adoption de ces technologies. Nous considérons que chacune de ces technologies présente des avantages et des inconvénients, mais que ces ceux-ci et ceux-là ne peuvent être évalués qu'à partir d'une caractérisation précise du contexte d'utilisation envisagé.

A tout seigneur, tout honneur: puisque pour beaucoup, la signature électronique est, par définition, la signature cryptographique, c'est cette technologie que nous commencerons par ... déchiffrer.

3.1 La signature cryptographique

Si l'histoire de la cryptographie peut être retracée, selon David KAHN, aux premiers hiéroglyphes hors-normes,[5] elle a connu un essor considérable depuis le début des années 70, alors que son utilité pour sécuriser les échanges bancaires a été reconnu. C'est à cette occasion que la recherche fondamentale en ce domaine devait commencer à se dégager du cadre strictement militaire qui était jusqu'alors le sien et connaître sa première heure de gloire, lorsque Whitffield Diffie et Martin Hellman conçoivent en 1976 le principe de la cryptographie à clé publique et suggèrent pour la première fois que cet outil pourrait fournir un équivalent à la signature au sein des environnements électroniques.[6]

Tout d'abord quelques notions de base : jusqu'à l'invention de Diffie et Hellman, la cryptographie était basée sur le principe suivant, dit de *cryptographie symétrique*, parce que les participants utilisent la même clé tant pour le chiffrement que pour le déchiffrement. Soit deux individus, $\mathcal{A}$ et $\mathcal{B}$, désirant communiquer au sein d'un environnement potentiellement hostile. $\mathcal{A}$ dispose d'un procédé de chiffrement C et $\mathcal{B}$ dispose du procédé de déchiffrement inverse D. La confidentialité de leur communication repose sur une *clé secrète* K, connue à la fois de $\mathcal{A}$ et $\mathcal{B}$, sur laquelle ils se sont entendu au préalable. Pour chiffrer un document M, $\mathcal{A}$ fournit son document M et la clé K au procédé de chiffrement E, qui produit un document chiffré $M\prime$. Ce document est transmis à $\mathcal{B}$ par un canal de transmission quelconque, avec l'hypothèse qu'il est impossible à quiconque ne dispose pas de la clé K de déchiffrer $M\prime$. Après avoir reçu le document $M\prime$, $\mathcal{B}$ le fournit, ainsi que la clé K, au procédé de déchiffrement D, qui produit alors le document M original, en clair.

Diffie et Hellman s'intéressaient au problème de la sécurisation *efficace* des communications entre n individus présents sur un réseau de communication, le réseau téléphonique par exemple. En utilisant les méthodes de cryptographies à clé symétrique, deux scénarios sont possibles: soit que chaque paire d'individus établit une clé de chiffrement commune, dont chacun possède un exemplaire ; soit

3. Les termes de *signature numérique* ou de *signature digitale* sont aussi souvent utilisé pour désigner la signature cryptographique.

4. Cette attitude n'est pas le fruit d'un quelconque relativisme technologique: même quand il s'agit de comparer la sécurité de différents modèles de cryptographie asymétrique — celle-ci peut en effet être réalisée à partir de différents problèmes mathématiques — aucun spécialiste ne s'engage, faute de grille qui permettrait de les comparer. Quand il le fait, il s'agit alors d'un acte de foi ou, plus pragmatiquement, de simple rhétorique commerciale.

5. David KAHN, *La guerre des codes secrets : Des hiéroglyphes à l'ordinateur*, Inter Éditions, 1980 ; un autre ouvrage populaire sur l'histoire de la cryptographie est celui de Simon SINGH, *Histoire des codes secrets : De l'Égypte des pharaons à l'ordinateur quantique*, Lattès 1999 ; un excellent exposé vulgarisé de la cryptographie moderne est celui de Jacques STERN, *La science du secret*, Odile Jacob 1998.

6. W. DIFFIE, M. E. HELLMAN, « New Directions in Cryptography », *IEEE Transactions on Information Theory*, IT-22, pp. 644-654, novembre 1976.

qu'une autorité centrale se charge de coordonner l'échange de clés entre individus. Dans le premier cas, il est nécessaire de gérer n^2 clés sur le réseau, par le biais de n^2 communications ; dans le second, on se doit d'investir de confiance une tierce partie, chose toujours regrettable, du point de vue d'un cryptologue (voir mes remarques plus bas). Diffie et Hellman ont voulu éviter ces deux inconvénients d'un seul coup.

La *cryptographie à clé publique* (ou asymétrique) procède d'un principe simple, mais très astucieux. A chaque individu présent au sein du réseau de communication, est attribuée une paire de clés, une *clé publique* et une *clé privée* (on parle parfois de bi-clés), qui permettent de réaliser et le chiffrement, et la signature. La clé publique de chaque individu est rendue disponible au sein d'un annuaire, alors que la clé privée est conservée secrète. Pour envoyer un message M chiffré à $\mathcal{B}$, A obtient la clé publique de $\mathcal{B}$ et s'en sert pour chiffrer le message. De son coté, $\mathcal{B}$ est en mesure de déchiffrer le message en utilisant sa clé privée. Pour signer un message, A utilise sa clé privée avant de transmettre le message à $\mathcal{B}$. Celui-ci est en mesure de vérifier l'identité de l'envoyeur en se procurant la clé publique de A.[7] Toute la magie du système repose dans l'hypothèse mathématique suivante : *bien que la clé publique et la clé privée soit uniquement complémentaire, même en connaissant la clé publique, il est impossible d'en déduire la clé privée.*[8]

Les conséquences pratiques d'un tel procédé sont importantes : tout d'abord, il n'est plus nécessaire à deux individus, désireux d'échanger des données signées et/ou chiffrées au sein du réseau, de s'entendre au préalable sur une clé, chaque individu se contentant de publier sa clé publique dans un répertoire ; ensuite, le nombre de clés nécessaires sur le réseau passe de l'ordre de n^2 à $2n$, une conséquence d'une grande importance pratique — pour $n = 1000$, on passe d'un million de clés à gérer à 1000 bi-clés. Et, Diffie et Hellman y ont vu l'opportunité de décentraliser la communication des clés, c'est-à-dire d'éviter de faire appel à une autorité de confiance — il faut se replacer dans le contexte post-Watergate de l'époque, de la méfiance caractérisée des citoyens américains face à l'intrusion de l'État dans leur vies, et de l'énorme emphase mise sur la liberté d'expression au sein de cette société.

Initialement, Diffie et Hellman n'ont pu concevoir une réalisation concrète de leur principe et on du se contenter d'en énoncer les principes. Ce n'est que deux années plus tard que Ronald Rivest, Adi Shamir, et Leonard Adleman, du Massachusets Institute of Technology allaient concevoir d'un procédé mathématique qui mette en œuvre le principe de la cryptographie à clé publique, procédé fondé sur l'opération mathématique de l'exponentiation modulaire.[9] C'est ce processus qui est le plus largement répandu aujourd'hui.[10]

7. En pratique, pour éviter de signer de longs messages, les systèmes de signature font appel à des *fonctions cryptographiques de hachage*, qui produisent tout d'abord un *condensé* du message. Un condensé est une représentation du message de taille fixe, avec la particularité mathématique qu'il est « impossible » à un fraudeur de déterminer deux messages qui produirait un condensé identique. C'est le condensé qui est signé, par souci d'efficacité.

8. Il importe de préciser que ceci demeure un hypothèse, c'est-à-dire qu'aucun procédé de cryptographie à clé publique ne peut fonder sa sécurité sur une preuve mathématique : elle est plutôt fondée sur des *hypothèses calculatoires*. Un seul système de chiffrement (symétrique) peut se vanter d'une sécurité absolue, le système dit de *one-time pad*. Cependant, les conditions pratiques de son utilisation (clé de même taille que le message et exigence de renouveler la clé *pour chaque message*) rendent son utilisation confinée aux applications aux plus hautes exigences de sécurité.

9. Cette opération possède la particularité que si l'on connaît des algorithmes efficaces qui permette de l'effectuer, on n'en connaît pas pour *renverser* l'opération, c'est-à-dire retrouver les données de départ de l'opération en partant du résultat. Ceci est plus facile à voir avec l'exemple de la multiplication : tout nombre possède une décomposition unique en nombre premiers — $15 = 3 \times 5$; $16 = 2 \times 2 \times 2 \times 2$. On sait comment efficacement multiplier 3 et 5 ou 4 et 4. Par contre, on ne connaît pas d'algorithme efficace pour effectuer l'opération inverse, déterminer les facteurs premiers d'un nombre. Pour un très grand nombre, cette inefficacité est si coûteuse qu'on dit, par abus de langage, qu'elle est, à toutes fins pratiques, impossible, c'est-à-dire qu'elle nécessiterait des milliards d'années de calcul aux ordinateurs les plus puissants.

10. Le fait que l'algorithme RSA soit utilisé dans le mécanisme de sécurisation des transactions SSL des fureteurs Web

3.1.1 La certification

La solution de Diffie et Hellman souffrait cependant d'une faiblesse importante, propre à invalider les bénéfices du système : supposons qu'$\mathcal{O}$, un être fourbe et malhonnête, désire convaincre $\mathcal{A}$ qu'il reçoit des messages signés de $\mathcal{B}$, alors qu'ils sont en fait de la plume d'$\mathcal{O}$. Celui-ci n'aurait qu'à substituer sa propre clé publique à celle de $\mathcal{B}$ dans l'annuaire, et envoyer ses messages à $\mathcal{A}$ en prétendant être $\mathcal{B}$. Pour vérifier la signature de ces messages, $\mathcal{A}$ se procurerait la clé publique de $\mathcal{B}$ (en fait, celle d'$\mathcal{O}$) et la vérification étant réussie, serait faussement convaincu de l'origine des messages. Il faut donc que les clés publiques soient obtenues de telle façon à ce que l'on soit convaincu de l'identité de la personne reliée à la clé. Deux méthodes ont étés explorées pour résoudre ce problème : la première, dite des *réseaux de confiance*, est basée sur la transmission des clés entre les individus eux-mêmes. Lorsque vous recevez une clé publique, vous évaluez informellement son authenticité, et la transmettez à vos propres correspondants. Chaque clé bénéficie en quelque sorte d'une évaluation de sa qualité, selon la confiance que vous portez en la personne qui vous l'a transmise. C'est cette méthode qui est utilisée dans les versions gratuites du logiciel PGP (mais non dans la version commerciale, qui est basée sur la certification).

Une seconde méthode a été imaginée, présentant le désavantage de reproduire le besoin pour une autorité centralisée au sein du réseau. Elle consiste en l'utilisation d'un *certificat* et d'une *autorité de certification*. Un certificat est tout simplement un document contenant une série d'informations permettant d'associer une clé publique à un individu. Par exemple, un certificat répondant aux exigences de l'annexe I de la Directive européenne sur la signature électronique pourrait ressembler à :

```
-------------------------------------------
Nom               :   BLANCHETTE
Prénom            :   Jean-François
Clé publique      :   AD3456EBE12976EDE
Emission          :   01/01/2000
Expiration        :   31/12/2001
Limite de valeur  :   1000 euros
Emis par          :   CNRS
Algorithme        :   DSA 1.78
Numéro de série   :   34343343434343433
-------------------------------------------
```

La véracité des informations contenues dans le certificat est confirmée par deux processus distincts : 1° d'une part, l'autorité de certification engage une procédure par laquelle l'identité de la personne est confirmée — présentation en personne de pièces d'identités, etc. ; 2° d'autre part, le certificat est lui-même signé électroniquement par la clé privée de l'autorité de certification. Toute personne qui désire vérifier la véracité du lien entre un individu et sa clé publique peut dorénavant le faire en 1° vérifiant la signature de l'autorité de certification sur le certificat de l'individu, en se procurant la clé publique de l'autorité ; 2° se convaincant, par tous les moyens à se disposition, de la probité de l'autorité de certification.

D'entrée de jeu, plusieurs questions se posent : *qui va certifier la clé publique des autorités de certification ?* Cette question fort complexe est à l'origine de plusieurs modèles, et devrait, à elle seule, donner naissance à une riche industrie juridique dans les prochaines années : certification croisée, auto-certification, certification hiérarchique, autant de modèles différents qui induisent des modes de

a fait dire à son fabriquant que l'algorithme RSA est le bout de code informatique aujourd'hui le plus répandu dans le monde.

vérification de signature différentes. Le point le plus important à retenir est que la vérification d'une signature implique la vérification de la totalité de la *chaîne de certification*, c'est-à-dire l'ensemble des certificats des autorités de certification impliquées.

Un individu qui veut, aujourd'hui, obtenir un certificat à clé publique, peut le faire de différentes façons. Soit qu'il l'obtient d'une autorité de certification à partir du réseau. Ce certificat peut ensuite être intégré directement à son ordinateur (Windows 2000 supporte les certificats), soit que ce certificat est intégré à son logiciel de courriel, ou encore à son fureteur Web, qui intègrent différentes fonctions de gestion de certificats.

3.1.2 Les infrastructures à clés publiques

On utilise le terme *infrastructure à clés publiques* (ICP)[11] pour désigner la combinaison d'éléments matériels, logiciels, et procéduraux qui permette d'effectuer l'ensemble des opérations sous-jacentes à la réalisation de la signature (et du chiffrement) cryptographique, c'est-à-dire :

1° *Génération de clés cryptographiques :* il faut produire les paires de clés cryptographiques, de façon hautement sécuritaire ;

2° *Distribution des clés privés aux utilisateurs :* il faut que les clés privés soient distribuées aux utilisateurs — placées au sein d'une carte à puce, par exemple ;

3° *Enregistrement des utilisateurs :* Il faut que l'autorité de certification vérifie l'identité de chacun des utilisateurs, par exemple par une présentation en personne de pièces d'identités ;

4° *Certification des clés publiques :* Une fois l'identité des utilisateurs confirmée, l'autorité de certification doit rédiger le certificat et le signer avec sa clé privée ;

5° *Service d'annuaire :* Le certificat doit ensuite être placé au sein d'un annuaire, de façon à permettre à d'autres utilisateurs de vérifier les signatures ;

6° *Révocation des certificats compromis ou périmés :* Les certificats sont révoqués lorsque ils sont expirés, ou lorsque une clé privée a été compromise. Ainsi, une signature ne pourra être vérifiée à l'aide d'une clé publique dont le certificat est révoqué ;

7° *Archivage :* Il faut conserver l'ensemble des certificats qui permettent la vérification, les listes de révocation, etc., de façon à pouvoir effectuer la vérification ultérieurement ;

8° *Recouvrement des clés :* Dans plusieurs pays, notamment la France, la Grande-Bretagne, et les Etats-Unis, les forces de l'ordre ont exprimé de grande réserves face à l'impossibilité de pouvoir déchiffrer des messages qui circulent sur les réseaux. Les technologies de recouvrement de clés permettent, de différentes façons, d'accéder aux clés de chiffrement d'un utilisateur, ou encore, de récupérer les clés de déchiffrement si elles étaient égarées ;

9° *Horodatage :* les certificats et les signatures doivent faire l'objet d'un datage sûr.

Une organisation désirant déployer une PKI peut déléguer l'ensemble de ces fonctions à un prestataire, ou au contraire, les réaliser toutes ou en partie. Cette liste permet de constater d'un coup d'œil la complexité de l'infrastructure sous-jacente à la signature cryptograhique.[12] Et l'on ne décrit même pas ici les difficultés liés au déploiement, aux facteurs organisationels et culturels. Nous aurons l'occasion d'examiner de plus près le déploiement et le fonctionement d'une PKI dans le chapitre 5, portant sur l'archivage.

11. Ou encore, PKI pour *Public-Key Infrastructures*, ou IGC pour *Infrastructure de gestion de clés.*

12. Face à la lourdeur et la complexité des PKIs, de nouveaux modèles se sont développés, qui raffinent le concept de certification : les LPKIs, pour *Lightweigth PKI.* Au sein de communautés d'utilisateurs réduites, ce concept est prometteur. Voir à ce sujet le système Securicam de la société Atos (`www.atos-group.com`.)

3.1.3 Brèves remarques sur l'histoire de la cryptographie

Effectuons un bref retour sur les circonstances historiques du développement de la science cryptographique. Les technologies de chiffrement ont été conçues dans un contexte militaire, pour permettre à des individus ou des institutions de communiquer au sein d'un environnement *ouvert et hostile*. En cryptographie, un système robuste est un système qui fonctionne au sein de l'environnement le plus hostile imaginable, un environnement où les intervenants malhonnêtes tenteront de faire échouer l'objectif de sécurité par tous les moyens possibles.

Prenons l'exemple des premières techniques du chiffrement, qui faisaient reposer leur sécurité en partie sur le fait que l'ennemi ignorait la technique utilisée, le secret reposant dans l'indisponibilité de la technique en quelque sorte. C'est le Français Auguste Kerckhoffs qui, le premier, a suggéré qu'il était préférable de poser l'hypothèse que l'ennemi avait pleine connaissance de la technique utilisée et que le secret devait reposer dans une unité d'information facilement modifiable et renouvelable : *la clé*.[13] La progression est ici d'une hypothèse de méfiance faible (« l'ennemi ne connaît pas ma méthode de chiffrement »), à une hypothèse de méfiance plus forte (« l'ennemi a pleine connaissance de ma méthode de chiffrement »). La recherche en cryptographie progresse de cette façon : votre système est meilleur s'il peut résister à des adversaires plus puissants et plus hostiles que le système précédent ne le pouvait. En d'autres termes, il est meilleur s'il vous permet d'investir moins de confiance en votre environnement — et de la faire plutôt reposer sur les mérites de votre système cryptographique.

C'est ainsi un des objectifs fondamentaux de la recherche en cryptographie que de faire reposer la sécurité d'un système sur les hypothèses de confiance les plus faibles possibles. Ceci est un point important, puisqu'il offre une clé de lecture fondamentale des technologies cryptographiques : *elles tendent à vouloir réduire le plus possible la confiance que l'on doit accorder aux intervenants institutionnels.* Le très réputé cryptologue David Chaum résume bien cette façon de penser :

> « Ce que nous avons pu démontrer à l'aide des technologies modernes de l'information, c'est que l'on peut résoudre tout problème de sécurité de l'information simplement en laissant chaque personne posséder son propre ordinateur. Laissez-les utiliser leur propre ordinateur pour protéger leurs propres intérêts. *Il n'y a aucun besoin d'établir des mécanismes auxquels les parties accordent mutuellement leur confiance.*[14] »

Ainsi, les technologies cryptographiques ne sont pas neutres, bien au contraire, puisqu'elles tendent à nier la composante institutionnelle de la sécurité de l'information. Ainsi, face à un discours technique qui privilégie systématiquement une approche algorithmique aux différents problèmes de la sécurité de l'information, il faut demeurer vigilant et privilégier une approche qui harmonise les technologies aux institutions concernées.

3.1.4 Normalisation

Au niveau de la normalisation, l'univers cryptographique est très avancé.[15] Très tôt, les industriels et les scientifiques ont compris que le succès de cette technologie dépendrait de leur capacité

13. Kerckhoffs énonce comme deuxième exigence d'un système de chiffrement militaire qu' « il faut qu'il n'exige pas le secret et qu'il puisse sans inconvénient tomber entre les mains des ennemis ; » — Auguste Kerckhoffs, "La cryptographie militaire," *Journal des sciences militaires*, vol. IX, pp. 5–38, Janvier 1883, pp. 161–191, Février 1883.

14. David Chaum, "Digital Money." Présentation donnée à la conférence *Doors of Perception 2*, Amsterdam, 4–6 novembre 1994.

15. Voir à ce sujet Menezes, van Oorschot et Vanstone, *Handbook of applied cryptography*, CRC Press, 1997, chapitre 15.

à développer des normes universellement acceptées. De plus, la sécurité informatique s'est toujours bien prêté à la normalisation — l'administration américaine a stimulé l'essor de la cryptographie civile en établissant les *Federal Information Processing Standards* (FIPS) qui définissent, entre autres, le procédé de chiffrement symétrique DES et la norme de signature digitale DSA. L'*Internet Engineering Task Force* travaille sur un certain nombre de normes — fonction de condensés (MD5) et courrier électronique sécurisé entre autres (S/MIME), PKIs, etc. Certains standards se sont imposés *de facto*, c'est le cas de la série de spécifications PKCS *(Public-Key Cryptographic Standards)* où est définie la norme de chiffrement RSA et l'échange de clé Diffie-Hellman. Ces spécifications ont joué un rôle important dans l'opérationalisation des systèmes cryptographiques.

La communauté académique a pu imposer l'idée que l'échange et la discussion ouverte qui caractérise le processus scientifique seuls permettraient de garantir que les procédés cryptographiques soient sûrs. Tout procédé propriétaire, qui ne puisse être soumis à l'examen de l'ensemble de la communauté scientifique, serait susceptible de contenir des faiblesses non-anticipées par ses concepteurs. Cette vision résultante de l'expérience de la communauté scientifique de la difficulté de réaliser des procédés cryptographiques qui réalisent leurs objectifs de sécurité et que l'ensemble des conditions à considérer est extrêmement vaste et complexe.

Il ne faut cependant pas glorifier le processus scientifique comme garant d'une sécurité absolue. Chaque année, les jeunes cryptologues se font les dents en brisant des procédés cryptographiques dont la sécurité a pourtant été *mathématiquement prouvée*. C'est que, contrairement à la vision populaire de la chose, la preuve mathématique n'est pas unique, elle existe sous différentes formes et il faut donc au préalable que les scientifiques s'entendent sur ce que constitue un preuve valable. Encore plus important, il faut qu'ils s'entendent sur les définitions des objets dont ils tentent de prouver les propriétés. Or, pour beaucoup d'objets cryptographiques, ces définitions ne sont pas encore stabilisées. [16]

D'un coté, donc, le processus d'examen scientifique ouvert des procédés cryptographiques est probablement le mieux à même de produire des technologies dont on soit raisonnablement assuré de la fiabilité. D'un autre coté, il n'est pas clair quelle soit l'importance de cette fiabilité mathématique dans la chaîne de sécurité. Contrairement au discours dominant, il est fort possible qu'elle ne joue, somme toute, qu'un rôle très mineur.

3.1.5 Mesure de la sécurité

Quel type de sécurité offre la cryptographie? Comment cette sécurité est-elle mesurée? Comment les déploiements de la cryptographie dans le monde industriel ont-ils prouvés leur efficacité? Ce sont des questions importantes. L'article de Diffie et Hellman cité plus haut est remarquable pour la richesse de concepts qu'il introduit. Un de ceux-ci était la promesse que la sécurité des mécanismes cryptographiques pourraient être *prouvée mathématiquement*. La cryptographie a énormément profité de cette notion de preuve, même si dans la pratique, les choses se sont révélées un peu plus compliquées, et l'objectif d'une sécurité prouvable reste toujours quelque peu fugace. [17]. Il y a de plus une présomption dans le monde juridique que la preuve mathématique est la démonstration irréfragable

16. Si la définition de certains des blocs fondamentaux de la cryptographie — les *primitives* — font l'objet d'un certain consensus, ce n'est pas le cas pour tout ce qui touche aux interactions et à la composition de ces primitives, que l'on ne sait même pas encore modéliser correctement.

17. Ceci est une discussion qui nous amènerait rapidement dans des eaux presques philosophiques, mais il demeure que la notion même de preuve en cryptographie est loin d'être simple — par exemple, la preuve dans le modèle dit de « l'oracle aléatoire » est considéré par certains comme une forte présomption, plutôt qu'une preuve comme telle.

d'un fait — c'est ce qui donne tant de conviction aux méthodes cryptographiques.

Dans l'univers cryptographique, la mesure de sécurité dominante concerne la taille de la clé : qui n'a pas entendu de ces savants débats sur les mérites respectifs de la clé de 128, 1024, ou 2048 bits ? En mettant l'accent sur la taille de clés, les cryptologues proposent implicitement un modèle de risque, celui d'un adversaire utilisant la force brute de calcul pour briser le système cryptographique. Cette mesure est, selon moi, une des grandes faiblesses de la cryptographie : toute absorbée à ses mathématiques, elle a négligé l'aspect terrain de son domaine, avec comme conséquence que les systèmes cryptographiques ne sont pas brisés par des savantes manipulations mathématiques, mais bien par des bidouillages beaucoup moins glorieux. [18]

Une autre mesure viendra prochainement s'ajouter à l'évaluation de la vérification des signatures — celle d'une mesure de confiance en la validité d'une clé publique. En effet, l'origine d'une clé publique est toujours affaire d'un processus probabiliste d'évaluation de sa source (« Je fais confiance aux méthodes de Certinomis pour s'assurer de l'identité du détenteur de cette clé »), et la question de la certification des clés devient alors une instance du problème de la prise de décision dans des conditions d'incertitude. [19] Cette incertitude est plus forte lorsqu'il s'agit d'évaluer des certificats provenant de sources étrangères et/ou inconnues. Des chercheurs comme Reiter and Stubblebine suggèrent qu'il faut développer une métrique de confiance, une mesure à appliquer à un certificat, selon le degré de confiance qu'on lui accorde. Même en utilisant des méthodes cryptographiques, l'évaluation de la validité d'une signature serait un processus *probabiliste* et non purement déterministe.

Au-delà de la cryptographie prise isolément, force est de constater que *la sécurité et l'efficacité des technologies d'infrastructures à clés publiques est systématiquement surestimée.*[20] Rien ne dit que ces technologies ne rempliront pas leur promesses, mais il faut garder à l'esprit que nous ne disposons d'aucune réalisation qui permette d'évaluer la performance de ces infrastructures sur une échelle substantielle — impliquant plusieurs organisations et plusieurs millions (ou tout au moins, centaines de milliers) d'utilisateurs. [21] Pour les projets existants, la propension des intervenants (à chaque niveau de la chaîne décisionnelle) à exagérer les chiffres est endémique, car nous fonctionnons dans un marché où il faut acquérir le maximum de capital symbolique, et où être le premier sur les lieux *(first to market)* procure un avantage stratégique déterminant.

Ceci n'est pas nécessairement un état de chose qui doit nous désoler car, après tout, toute technologie mûrit, de même que nos capacités à l'exploiter optimalement. Cependant, les très rares études réalisées sur le terrain tendent à démontrer que si la fiabilité des *algorithmes mathématiques* sur lesquels reposent les procédés de signature électronique semble assurée, ceux-ci ne représentent qu'une faible partie de l'ensemble du processus. L'exemple est typiquement donné de la gestion de clés, une opération hautement délicate et souvent mal comprise : peut importe la robustesse des algorithmes

18. Même Whitffield Diffie, grand chantre de la cryptographie moderne, constatait, lors d'un discours, que la cryptographie est « étonnamment difficile à réussir en pratique. »

19. Voir par exemple Reto Kohlas et Ueli Maurer, « Confidence valuation in a Public-Key Infrastructure based on uncertain evidence », in *Proceedings of Public Key Cryptography 00*, Lecture Notes in Computer Science, vol. 1751, pp. 93-112, Janvier 2000.

20. Je ne suis pas le seul à le croire — plusieurs cryptologues réputés ont exprimé cette opinion, par exemple, Ross Anderson, du Laboratoire de recherche sur la sécurité de l'Université de Cambridge, et Bruce Schneir, auteur d'un ouvrage de référence en cryptographie, et plus récemment, de *Secret and Lies*.

21. Un vice-président de la société *RSA Security* confessait récemment que les réalisations d'infrastructures à clés publiques n'ont toujours pas évoluées au-delà de ces vitrines dont on abreuve sans cesse conférenciers et investisseurs.

mathématiques utilisés, ceux-ci seront vulnérables dès lors que la gestion des clés — c'est-à-dire les opérations de création, distribution, conservation, destruction — est incorrectement réalisée. [22]

Ainsi, dire que l'on dispose aujourd'hui d'*algorithmes* de chiffrement ou de signature fiables est une affirmation qu'endosserait une proportion respectable des scientifiques spécialistes de la question ; dire que l'on dispose de *réalisations* fiables d'infrastructures de sécurité — c'est-à-dire permettant la génération, certification, distribution, mise à jour automatique et révocation de clés de signature et/ou de chiffrement, les services d'annuaire, les mises à jour d'annuaire, l'archivage, l'audit, etc. — est une affirmation qui relève de la seule science du ... marketing.

3.1.6 Évaluation

Clairement, la signature cryptographique offre des avantages importants pour la sécurisation des réseaux. En particulier,

1° Elle garantit fortement l'intégrité des donnés qui transitent à travers les réseaux ;
2° Elle garantit un fort lien entre clé et document ;
3° Elle est susceptible d'être automatiquement générée et vérifiée, sans intervention humaine et, de ce fait, idéale pour sécuriser les communications entres machines ;

Cependant, dans le cadre de notre réflexion sur l'acte authentique, le modèle cryptographique de la signature pose des problèmes importants. En particulier,

1° L'héritage militaire de la cryptographie a imposé un modèle où l'environnement est nécessairement et maximalement hostile. Ce modèle implicite a pour effet de dévaloriser le rôle des institutions dans la sécurité juridique ;
2° La sécurité de la cryptographie est toujours évaluée en fonction de taille de clés. Cette mesure est peu pertinente dans un cadre opérationnel ;
3° Le modèle cryptologique est ergonomiquement pauvre, ne tirant aucunement partie de l'héritage culturel de la signature manuscrite et ne préservant pas les solennités de l'acte. En particulier, la signature cryptologique ne dispose d'aucune représentation visuelle ;
4° Une signature cryptographique n'identifie jamais qu'une clé privée, et non un individu ; Ainsi, le « contrôle exclusif du procédé de signature » requis par la Directive n'est assuré, en bout de compte, que par le code personnel à quatre chiffres qui contrôle l'accès à la clé entreposé sur la carte à puce ;
5° La signature cryptographique nécessite une infrastructure extrêmement lourde, les ICPs ;
6° La signature cryptographique exige que toute partie à un acte soit enregistrée au sein du système pour pouvoir signer ;
7° Le modèle cryptographique impose que les signatures soient toujours vérifiées.

Il faut donc considérer attentivement les nouveaux risques associés à l'utilisation de la signature cryptologique. Avant tout, il faut se départir de l'idée que la signature cryptologique représente une « grande et belle » signature électronique, opposé à d'autres formes de signature qui seraient, elles, des « ersatzs ».

22. A ce sujet, on consultera avec horreur et bonheur l'article de Ross Anderson, « Why cryptosystems fail », *Communications of the ACM* 37:11 (novembre 1994), pp.32-40.

3.2 La signature biométrique

La signature biométrique se fonde sur une toute autre approche que celle de la cryptologie, tant dans sa définition de la signature, que dans sa mesure de sécurité et son mode de preuve, que dans l'appareillage requis. La biométrie se rapporte à la mesure de *caractéristiques physiques* uniques à l'individu — la plus connue étant évidemment l'empreinte digitale. De nombreuses mesures ont été développées, chacune pourvues de caractéristiques différentes: parole, rétine, iris, géométrie de la main, et même l'odeur![23] Commençons par dissiper un certain nombre de malentendus à propos de la signature biométrique.

D'emblée, notons qu'une mesure biométrique prise par elle-même n'est pas une signature — on entend souvent que « bientôt nous pourrons signer avec notre œil! (ou son pouce) ». Alors que la signature est couramment utilisée comme marque de manifestation de volonté (j'approuve, je m'engage, j'ai lu, j'ai noté, etc) sans être une marque d'identité — comme dans le contrat notarié — l'inverse n'est pas vrai, c'est-à-dire qu'une marque d'identité seule ne suffit jamais à manifester une intention. Or les mesures biométriques seules, *sans contextualisation* ne sont pas la manifestation d'une intention. En théorie, rien n'empêche que soit développée une technologie — *avec le contexte culturel dont elle dépend* — qui permette de décréter que l'exposition de sa rétine à un lecteur devienne une forme de signature, si ce n'est que depuis un millénaire, la manifestation du consentement contractuel est accompagné de *gestes*, d'une expression corporelle quelconque.

Il faut de plus distinguer entre l'identification biométrique et la signature biométrique, car elles font appel à des opérations techniques différentes: dans la signature, on ne cherche pas à *déterminer* l'identité, mais à la *corroborer*. C'est-à-dire qu'un individu décline son identité, produit sa signature, et on vérifie si cette signature correspond bien à celle associée à l'individu. Le même principe est à l'oeuvre pour la signature cryptographique: lorsqu'on envoie un message signé, le destinataire ne détermine pas l'identité du signataire à partir de la seule signature, en fait, il en serait bien incapable ! Plutôt, il récupère le certificat à clé publique du signataire, et *corrobore* l'identité supputée par le processus de vérification. Tout comme, dans un acte, on obtient l'identité du signataire par le fait que son nom est tapé en toutes lettres au-dessus de signature. [24]

Finalement, les méthodes biométriques sont reliées au problème de la signature électronique de deux façons: (1) dans le contexte de la signature cryptographique, l'ensemble des méthodes biométriques peuvent être utilisées pour assurer le lien entre un individu et sa clé privé, remplaçant par exemple le code personnel à quatre chiffres; (2) une technologie biométrique particulière, *l'analyse dynamique de la signature manuscrite*, est en soi une méthode de signature électronique. Le premier cas, qui correspond à une technologie de *contrôle d'accès*, ne sera pas examiné dans ce rapport — encore une fois, le lecteur est prié de se référer à l'excellent rapport de Dirk SCHEUERMANN pour une discussion assez complète des avantages et des inconvénients de chacune des méthodes biométriques, dans une perspective d'utilisation pour le contrôle d'accès à une clé privée.

23. Chacune de ces techniques présente des avantages et inconvénients — pour un survol, voir le rapport de Dirk SCHEUERMANN, *Usability of Biometrics in Relation to Electronic Signatures*, EU Study 502533/8, GMD Forschungszentrum Informationstechnik GmbH.

24. Cette distinction est importante techniquement: un système biométrique d'identification doit comparer la mesure biométrique avec l'ensemble des patrons des candidats — par exemple, dans le cas des empreintes digitales recueillies sur la scène d'un crime, on compare la mesure avec l'ensemble du fichier d'empreintes de la police, une procédure très laborieuse, évidemment. La corroboration est beaucoup plus efficace, puisqu'elle n'a qu'une seule comparaison à effectuer, avec le patron de l'individu concerné.

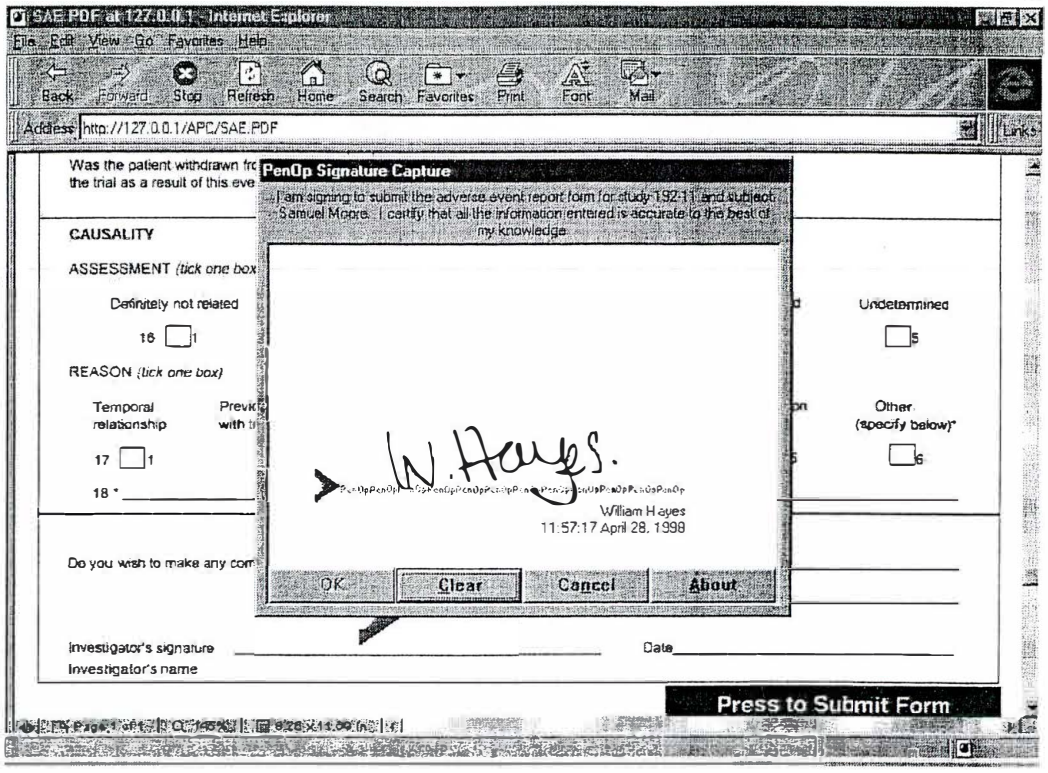


FIG. 3.1 – *Signature biométrique à l'aide du produit PenOp et d'une tablette graphique.*

3.2.1 Mécanisme de la signature biométrique

La particularité de l'acte de signer est que chacune des signatures d'un individu est différente et pourtant, l'identifie uniquement. Les technologies de signature biométrique tire parti de ces caractéristiques pour produire un système qui permet tout à la fois d'améliorer les techniques établies de vérification de signature et de conserver une forme de manifestation du consentement — écrire son nom de sa main — qui jouit d'une acceptation presque totale au sein des cultures occidentales. Un système de signature biométrique consiste en plusieurs opérations : l'enregistrement, la signature et l'identification et l'intégrité.

Enregistrement : Pour signer, l'utilisateur doit disposer d'une tablette graphique et d'un stylet approprié, et le système doit disposer d'un patron. Selon le produit spécifique de signature utilisé, le logiciel effectue différentes mesures lors de la signature : angles x, y et z, pression, vitesse. Ces mesures sont ensuite comparées à un *patron*, c'est-à-dire une sorte de moyenne de la signature d'un individu. Ce patron peut être obtenu soit (1) *avant* la signature, soit (2) *après*.

— (1) Lorsqu'un individu compte utiliser régulièrement le système, sa signature est enregistrée. Cette opération consiste en l'obtention d'un certain nombre d'exemplaires de sa signature — typiquement, de 3 à 10 — de façon à établir un *patron* de sa signature, c'est-à-dire une moyenne des différentes mesures effectuées à partir de la signature : coordonnées x, y et z, pression, vitesse. Le patron est ensuite conservée au sein d'une base de données, pour être utilisé, en temps réel, lors de la vérification d'une signature.

— (2) Dans ce cas, on obtient les exemplaires requis de la signature de l'individu *après* une contestation. Cette type de situation se présente en fait dans la plupart des cas où il n'existe pas de lien préalable entre la personne et le système. La signature n'est pas vérifiée lors de la signature du document, mais les mesures sont simplement conservées avec le document. Ce n'est que lorsque la validité de la signature est contestée que l'on se procure les exemplaires de signature nécessaire à la construction du patron. Ceci reproduit ce qui se passe dans la réalité : la grande majorité des signatures n'est jamais vérifiée, c'est-à-dire que *la signature est uniquement vérifiée en cas de litige* plutôt que systématiquement.

Signature, identification : La signature proprement dite est effectuée à l'aide d'un logiciel intégré à l'application produisant le document (Microsoft Word, ou Adobe Acrobat par exemple). Les mesures effectuées sur la signature sont alors comparées avec le patron. Quatre résultats sont possibles : (a) la signature est jugée conforme au patron, et justement acceptée ; (b) la signature est jugée non-conforme, et justement refusée ; (c) la signature est jugée conforme, et injustement acceptée ; (d) la signature est jugée non-conforme, et injustement refusée. Les algorithmes de vérification de signature doivent tenter de maximiser (a) et (b) et de réduire au maximum (c) et (d). On appelle (c) le taux d'*acceptation erronée* et (d) le taux de *rejet erroné*.

Lien et intégrité : Tout comme la plupart des mécanismes de signature cryptographique, la signature biométrique établit le lien entre la donnée de signature (clé privée, mesure biométrique) et le document par l'utilisation d'une fonction de condensation (ou fonction de hachage) — ceci permet de lier la signature à un message donné, et d'assurer que, de façon pratique, toute altération du message entraîne l'échec de la vérification de la signature.

3.2.2 Quantification, normalisation

Les algorithmes qui effectuent la comparaison entre les mesures prises lors de l'exécution d'une signature et le patron conservé au sein du système retournent une *mesure statistique de confiance*. Puisque le procédé biométrique est fondé sur la propriété que chaque exécution d'une signature est différente de toute les autres, tout en étant unique à chaque individu, la mesure de comparaison ne peut être exacte. En fait, une correspondance exacte entre le patron et une signature donnée serait à coup sûr le signe d'une tentative de fraude. La signature biométrique est donc, en son essence, probabiliste. [25] Ainsi, lors du processus de vérification de la signature, les produits de signature biométrique offrent une mesure de validité de la vérification, laissant à l'utilisateur l'option de déterminer si le contexte d'utilisation impose une vérification plus ou moins certaine. [26]

Ceci dit, à quoi correspond cette mesure de validité ? Malheureusement, la situation n'est pas claire. Comme il n'existe aucune norme — *de jure* ou *de facto* — régissant les algorithmes de vérification de signature biométrique, il est difficile de les comparer entre eux. Pire encore, il n'existe pas non plus de normalisation des mesures que l'on pourrait appliquer pour déterminer les mérites respectifs des algorithmes. La seule mesure communément utilisée est le FA/FR discuté plus haut, mais cette mesure est largement illusoire dans le contexte de la sécurité, puisque il faudrait également déterminer ce que constitue une attaque, quelles sont les moyens à la disposition d'un faussaire, son accès à

25. Dans le modèle cryptographique, l'identification de la clé qui a signé le document est déterministe, mais c'est le lien entre individu et clé qui introduit une dimmension probabiliste au processus.

26. Ceci reproduit assez bien ce qui se produit lorsque l'on signe un chèque important et que l'on doit s'appliquer à « bien » signer, c'est-à-dire à apposer une signature qui ressemble à celle déposée à la banque lors de l'ouverture de notre compte chèques.

des exemplaires de signature manuscrite, etc. [27]

L'absence de quantification et de normalisation est-elle nécessairement un handicap? Il faut réfléchir attentivement à cette question. Indépendamment de cette question, la communauté biométrique a encore beaucoup à faire avant de pouvoir en arriver à un niveau de normalisation comparable à celui de la communauté cryptographique.

3.2.3 Évaluation

La signature biométrique présente des caractéristiques intéressantes pour un grand nombre de contextes :

1° Elle est culturellement ergonomique, en ce sens qu'elle présente une variation minime de la manifestation du consentement telle qu'on la réalise dans les sociétés occidentales, par la signature de son nom ;
2° Du point de vue de l'expertise judiciaire, elle permet de conserver une forme éprouvée de mesure, l'analyse statique d'une signature, et d'y ajouter la mesure dynamique, c'est-à-dire les paramètres de vitesse et de pression. Son expertise s'inscrit au sein d'une tradition d'expertise des signatures aux modalités déjà bien connues ;
3° Elle apporte une certaine sécurité sans nécessairement imposer la vérification automatique de la signature ;
4° Elle produit une représentation visuelle de la signature ;
5° Contrairement à un code d'accès, on n'oublie pas sa signature.

Par contre,

1° Elles peuvent être sensible aux modifications de l'état de la personne, i.e, par exemple, ingestion d'alcool, maladie ou âge provoquant un tremblement de la main (conditions qui peuvent tout aussi bien entraîner l'oubli du code personnel) ;
2° Une fois qu'il est compromis, le patron biométrique ne peut se renouveler! C'est-à-dire que les caractéristiques dynamiques qui identifient uniquement la signature d'un individu ne sont pas observables directement, mais ils ne sont pas non plus renouvelables à loisir, comme l'est un mot de passe, ou une clé cryptographique.

3.3 la signature-tatouage

A celui qui désire protéger un secret, deux approches sont possibles : le chiffrement et la dissimulation. Le chiffrement cryptographique permet de rendre un secret inaccessible, même si le texte crypté est en soi accessible ; les techniques de *dissimulation d'information* [28] tentent, elles, de rendre le secret **invisible**. [29] Cette approche peut s'imposer dans certaines situations, où l'utilisation de la cryptographie est *en soi* un aveu que l'on dispose d'un secret.

27. Voir à ce sujet Nick Mettyear, « Error Rates in Biometric User Authentication », Mémorandum PenOp.
28. *Information hiding*.
29. Note terminologique : le champ scientifique de la dissimulation d'information étant encore très jeune, une terminologie globalement acceptée émerge à peine. Une excellente tentative de classification des nombreux concepts du domaine est celle de Fabien A. P. PETITCOLAS, Ross J. ANDERSON et Markus G. KUHN, « Information Hiding — A Survey », *Proceedings of the IEEE*, 87(7): 1062-1078, juillet 1999.

Historiquement, la dissimulation d'information a connu de nombreuses formes et applications, mais, récemment, cette science a connu un renouveau, alors qu'est apparu l'intérêt de son application à la protection des œuvres numériques. Dans le contexte d'œuvres infiniment copiables, sans dégradation de qualité, à la distribution instantanée et sans frontières géographiques, les technologies de *tatouage*[30] offrent la promesse de pouvoir apposer des « marques » indélébiles aux œuvres numériques, marques qui permettraient de retracer soit les ayant-droits, soit les propriétaires légitimes des ces œuvres. Le tatouage est appliqué directement à l'oeuvre et réside en son sein — c'est-à-dire que le signal encodant le tatouage est intimement mêlé au signal de l'oeuvre elle-même, rendant sa découverte ou son extraction difficile pour ceux ne disposant pas des paramètres ayant permis le tatouage original.

Les tatouages se trouvent en deux saveurs : *fragiles* ou *robustes*. Dans le premier cas, toute manipulation de l'image entraîne la disparition du tatouage — en d'autres termes, la présence du tatouage témoigne de l'intégrité du document. Dans le second cas, éliminer le tatouage exige d'endommager irrémédiablement l'oeuvre au point de la rendre inutilisable, ou à tout le moins de réduire significativement sa qualité. On peut diviser les tatouages robustes en *tatouages visibles* et *tatouages invisibles*.

Les *tatouages visibles* sont un équivalent des marques en filigranes que l'on retrouve sur certains documents sécurisés, le papier à en-tête, ou sur les papiers spéciaux (papier-monnaie, passeports). Ces marques couvrent une grande surface du papier, mais demeurent semi-transparentes, de façon à ne pas affecter la lisibilité du document. Dans le contexte d'une image numérique, elles permettent d'identifier le producteur d'une oeuvre. La figure 3.2 montre un tatouage visible appliquée à une image numérique, obtenue d'un livre appartenant de la Bibliothèque du Vatican. Le tatouage identifie l'origine du document, tout en n'entravant pas sa lisibilité. Toute tentative d'éliminer le tatouage entraîne une dégradation de la qualité de l'image, idéalement.

---

29. Le tatouage des œuvres, numériques ou non, permet de réaliser des objectifs surprenants en terme d'authentification et d'identification. Par exemple, Margaret Tatcher, excédée par les nombreuses fuites de documents confidentiels, utilisa un système qui permit d'identifier la source des fuites ; le système consistait à encoder un identifiant dans chaque copie initiale du document par le décalage d'un $1/300^{e}$ de pouce des lignes du texte — un décalage vers le haut ou vers le bas permettant d'encoder un chiffre binairement. L'intérêt d'un tel système est qu'il est invisible et peut résister à plusieurs copies successives de même qu'à la télécopie. La copie « coulée » aux journaux pouvait donc être retracée jusqu'à l'auteur original de l'indiscrétion. Évidemment, la détection peut être évitée par simple retranscription du document, mais encore fallait-il être conscient du marquage du document. Voir J. BRASSIL, S. LOW, N. MAXEMCHUK, et L. O'GARMAN, « Electronic marking and identification techniques to discourage document copying », *Infocomm*, pp. 1278–1287, IEEE, juin 1994.

30. *Watermarking*.

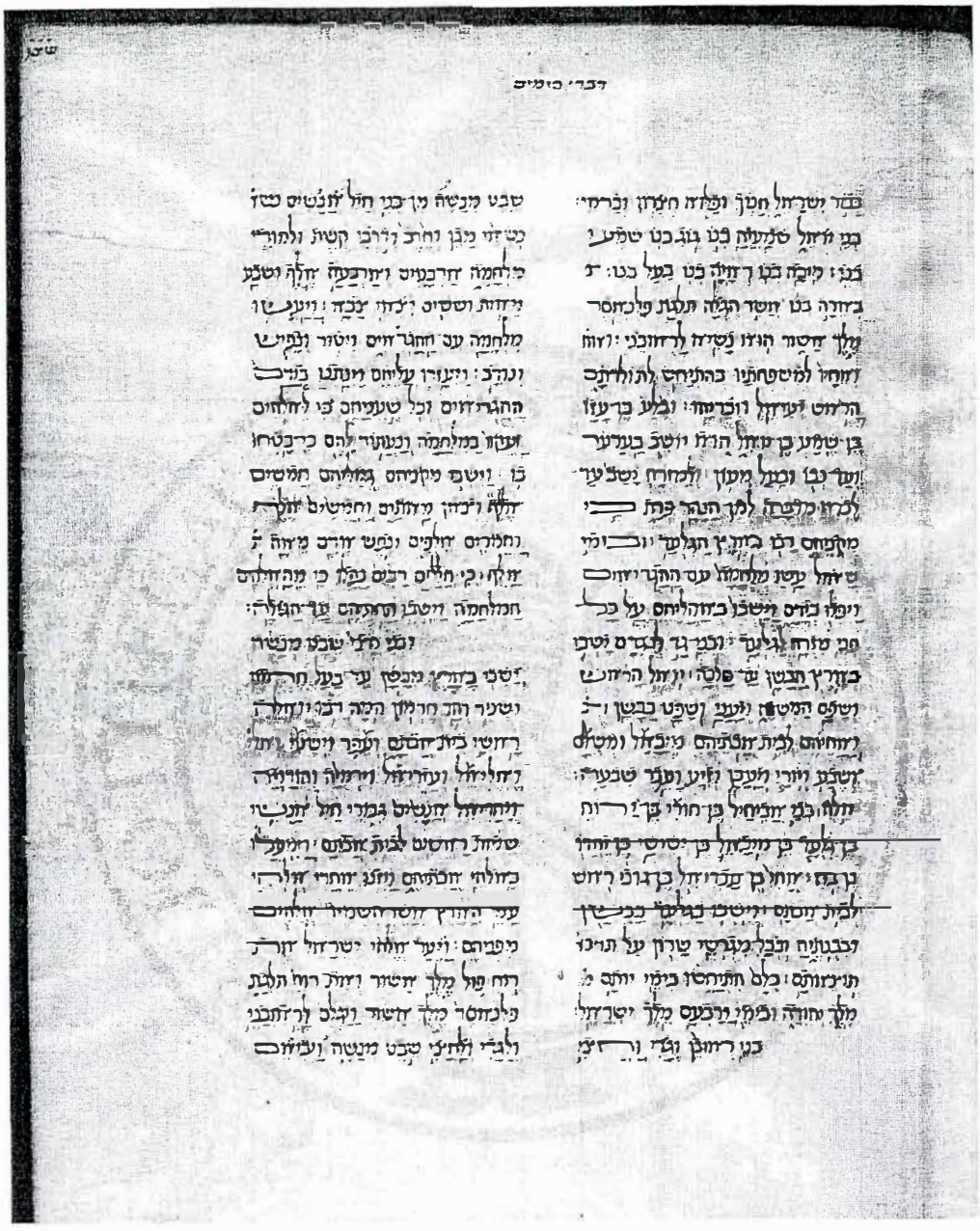


FIG. 3.2 – *Un tatouage visible d'un document numérisé de la Bibliothèque du Vatican. Le tatouage n'est pas sur le papier, mais bien au sein du fichier informatique.*

Les *tatouages invisibles* ne sont pas perceptibles à l'œil. Ils consistent simplement en un identificateur quelconque inséré au sein d'une image. Le procédé d'insertion assure qu'on ne peut supprimer cet identificateur sans irrémédiablement endommager l'image. Pour s'assurer de l'intégrité d'une image, on dispose d'un procédé qui vérifie la présence de l'indentificateur au sein de l'image. Remarquablement, cet indentificateur survit au passage du numérique à l'analogue, i.e., le papier. En d'autres termes, un document contenant une tatouage invisible peut être imprimé (par laser, jet d'encre, etc) et il sera toujours possible à l'algorithme de validation de retrouver l'identificateur, après numérisation du document papier. Ceci est un avantage notable sur les autres technologies de signa-

ture qui perdent tout capacité de vérification dès l'instant où le document est imprimé sur papier.

3.3.1 Mécanisme de la signature-tatouage

Comment le marquage des œuvres fonctionne-t-il au niveau de la signature? En utilisant une combinaison de technologies qui, ensemble, permettent de réaliser les trois fonctions de la signature, telle que décrite par la loi du 13 mars : identification, intégrité, lien avec le document.

Par exemple, la technologie VeriData, dévelopée par la société Signum Technologies, [31] permet de signer un document de la façon suivante :

1° Un condensé de l'image est calculé, à l'aide d'une fonction de hachage cryptographique ; ce condensé est chiffré à l'aide d'un algorithme de chiffrement symétrique ;

2° L'image est divisé en un certain nombre de rectangles ;

3° Chaque signataire dispose d'une clé — un simple code personnel ; cette clé est utilisée pour déterminer un certain nombre de locations au sein de chaque rectangle ;

4° La valeur du condensé chiffré est insérée au sein de l'image en ces locations, en modifiant la valeur de luminosité ou la valeur chromatique des pixels ;

5° Pour valider le document, on doit disposer de l'image originale, et de la clé, de façon à vérifier la valeur des condensés aux locations déterminées par la clé. Si la vérification échoue, on sait que l'image a été modifiée, mais on sait en plus dans quelle région de l'image.

La mesure d'intégrité est évidente — notez qu'elle est encore plus fine que celle fournie par la signature cryptographique ou biométrique, puisque qu'elle permet, le cas échéant, de préciser quelle région de l'image a subi des modifications. Le lien de l'identificateur avec le document est également évident puisque cet identificateur détermine la location des condensés insérés au sein de l'image. Selon le mécanisme de gestion de la clé de signature, celle-ci peut être considérée comme identifiant uniquement le signataire.

3.3.2 Quantification, normalisation

La recherche est encore très jeune en ce domaine, et on peut s'attendre à voir émerger rapidement des solutions de plus en plus sécuritaires et adaptées à des contextes de plus en plus variés. La très forte demande pour de tels produits dans le contexte de la protection de la propriété intellectuelle va pousser vers une très grande activité scientifique et d'innovation technologique. Cependant, le domaine, tout comme celui de la signature biométrique, ne s'est pas encore entendu sur des algorithmes communs, et les sociétés fondent leur avantage commercial sur les différences de performance entre les différents procédés proposés. Au niveau de la mesure et de la quantification, tout reste à faire. [32]

3.3.3 Sécurité

La question de la sécurité des procédés de tatouage numérique est épineuse et fait l'objet de nombreux débats au sein de la communauté des experts en sécurité. Deux conceptions de la sécurité s'affrontent : une veut que les procédés de sécurité soient examinés au sein de la communauté d'experts, cette méthode étant la seule susceptible de fonder notre confiance ; l'autre prétend que rien ne sert de fournir aux fraudeurs plus d'informations qu'il n'est nécessaire. La Banque de France ne publie pas sur son site Web la méthode de fabrication du papier-monnaie après tout, tout comme

31. `http://www.signumtech.com`.

32. Fabien Petitcolas a commencé à débroussailler le terrain de façon remarquable — voir le site Web qu'il consacre à la stéganographie : `http://www.cl.cam.ac.uk/~fap`.

Canal+ ne publie pas les plans de son décodeur. La première conception est celle des chercheurs en cryptographie, alors que la seconde semble, pour l'instant, caractériser les procédés de tatouage de oeuvres. Il est donc difficile de discuter de la sécurité de procédés de tatouage — tout dépendra de l'évolution du marché et de la réglementation. [33]

Les procédés de tatouage seront sans doute utile pour s'assurer qu'un utilisateur lambda ne puisse frauder, mais ils auront peu d'effet envers un attaquant déterminé. Ces procédés doivent donc être intégrés au sein d'autres mécanismes de sécurisation — tout comme les cartes bancaires ou les passeports utilisent toute une panoplie de mesures (hologrammes, polymères spéciaux, filigranes, etc.) pour freiner les faussaires.

3.3.4 Évaluation

La signature-tatouage présente donc des caractéristiques qui la différencie des autres technologies de signature électronique :

1° Elle est entièrement contenue au sein de l'image — pas de méta-données à gérer, elle est littéralement liée au document signé ;

2° Sa notion d'intégrité est plus fine, car elle permet de localiser l'endroit où le changement a eu lieu dans le document, plutôt que de fournir une simple réponse binaire ;

3° Elle survit au passage du numérique à l'analogue et vice-versa.

D'autre part,

1° Les technologies ne sont pas encore bien testées et stabilisées.

La signature-tatouage pourrait donc être mise en oeuvre dans le contexte d'ajout de niveaux de sécurisation supplémentaires au sein des images — possiblement par les pilotes d'impression et de numérisation, de façon à insérer directement au sein de l'image des informations de traçabilité. Ces marques, visibles ou invisibles, en « filigrane » ne seraient pas nécessairement vérifiées, mais fourniraient des sécurités supplémentaires, en cas de contestation de l'authenticité du document. Les indications de traçabilité que fourniraient ces marques sur la provenance ou la date d'un document, bien qu'elles soient pas nécessairement assimilables à une signature, s'ajouteraient utilement au « faisceau de preuves » à partir duquel l'intégrité d'un document est susceptible d'être établie.

3.4 La signature numérisée

La signature numérisée consiste simplement en la capture, au sein d'un fichier informatique, de l'*image* de la signature manuscrite d'un individu. L'image informatique résultante peut ensuite être ajoutée, par différents procédés, à la suite ou au sein d'un document électronique.

Avant de pouvoir discuter des mérites de cette technologie, il me faut tout d'abord prendre un peu de recul et justifier son inclusion dans ce rapport, puisque sa simple évocation mène inévitablement à une violente levée de boucliers : « Mais voyons ! Un tel procédé ne peut être qualifié de signature

33. En effet, aux États-Unis, le *Digitial Millenium Copyright Act* interdit purement et simplement de briser les mécanismes de protection des oeuvres, indépendamment de leur sécurité : section 1201(a)(1) débute par : « Aucune personne ne peut contourner un mécanisme technologique qui a pour effet de contrôler l'accès à une œuvre protégée par ce texte. » *(No person shall circumvent a technological measure that effectively controls access to a work protected under this title.)* Plutôt que d'investir dans la recherche, il est peut-être plus simple de criminaliser la production et la distribution de mécanismes de fraude, mais il est encore trop tôt pour voir si cette approche sera efficace.

électronique ! La signature apposée sur un tel document peut être contrefaite par une simple opération de couper-coller ! » Une telle argumentation procède d'une analyse erronée du cycle de vie d'un document, analyse qui postule que les documents électroniques sont créés, distribués et lus uniquement sous forme électronique. Hors, ceci ne correspond qu'à une infime partie des usages observés dans la pratique : en fait, l'essor de l'outil informatique a stimulé plus que jamais l'usage du papier et des technologies qui assurent la médiation entre le support papier et l'électronique — télécopieurs, imprimantes, scanners. [34] De plus, il y a intensification des connections entres ces outils : les photocopieurs font aussi emploi d'imprimantes réseau, on peut envoyer des courriers électroniques à des télécopieurs connectés à l'Internet et, inversement, des télécopies à un ordinateur. Il n'y a donc pas une « logique du document électronique », fruit de la marche victorieuse et inlassable du progrès technologique, qui supplanterait une « logique du document papier », synonyme d'une civilisation désuète désormais vouée à l'extinction. Il y a plutôt une interaction complexe et synergétique entre deux supports, interaction qui les dynamise mutuellement. [35]

Concevoir l'informatisation des opérations bureaucratiques en tenant compte de cette réalité permet d'éviter de s'enliser dans le dogme du « tout électronique » et de concevoir des solutions technologiques qui intègrent et tirent parti de cette nature hybride du document.

3.4.1 Évaluation

Le système SAGA développé pour le Service central de l'état civil (SCEC) à Nantes nous permettra d'évaluer la signature numérisée dans son contexte global d'utilisation. Le système développé pour le SCEC est remarquable tant pour la simplicité de conception que pour son adéquation aux besoins exprimés. [36] Le système visait à permettre aux officiers d'état civil du SCEC de délivrer le plus rapidement possible des copies conformes d'actes d'état civil, une activité qui occupait une portion de plus en plus importante de leur temps. [37] Ces copies sont remises soit directement au particulier, soit à des notaires ou autres institutions requérantes.

Le système comporte trois éléments distincts : tout d'abord, les 8 millions d'actes numérisés à partir des registres papier [38] ; ensuite, le système qui permet à l'officier d'état civil d'apposer un « pavé » contenant le sceau de l'État et sa signature au sein de l'acte numérique (voir la figure 3.3) ; finalement, le papier sécurisé sur lequel la copie conforme signée est imprimée, papier pourvu de caractéristiques spéciales qui protège son intégrité et en empêche la reproduction. [39]

Au sein même du SCEC, la sécurité est assurée par un ensemble de méthodes et techniques : les officiers d'état civil ne sont pas n'importe quel groupe d'utilisateurs, et la pénalisation sévère du faux en écriture publique assure, plus que toute mesure technologique ne saurait le faire, qu'ils ne soient pas considérés comme des fraudeurs potentiels au sein du système. [40] Des mécanismes de

34. Voir par exemple « What paperless office? Fax usage is up », *Managing Office Technology* 42:1(39).

35. Voir à ce sujet Ziming LIU et David G. STORK « Is Paperless Really More? Rethinking the Role of Paper in the Digital Age » *Communications of the ACM* 43:11(94-97).

36. Si vous ne croyez pas que ce soit remarquable, c'est que vous n'avez pas encore assez fréquenté d'informaticiens...

37. Voir le compte-rendu de Mme BANAT-BERGER pour une description générale du système et du contexte institutionnel — `http://www.gip-recherche-justice.fr/preuve/etatcivilnantais.htm`.

38. La capture des actes sous forme de fichier image est la seule concevable compte tenu de la nature des documents — à moins de considérer la retranscription manuelle des 8 millions d'actes ...

39. Pour un survol des technologies de sécurisation matérielle des documents, voir Rudolf VAN RENESSE, ed. *Optical Document Security*, Artech House Publishing, 1998.

40. Considérez qu'un système de paiement comme celui de la carte bleue doit être protégé des fraudes commises par les consommateurs, mais aussi les commerçants, les employés de banque, etc.

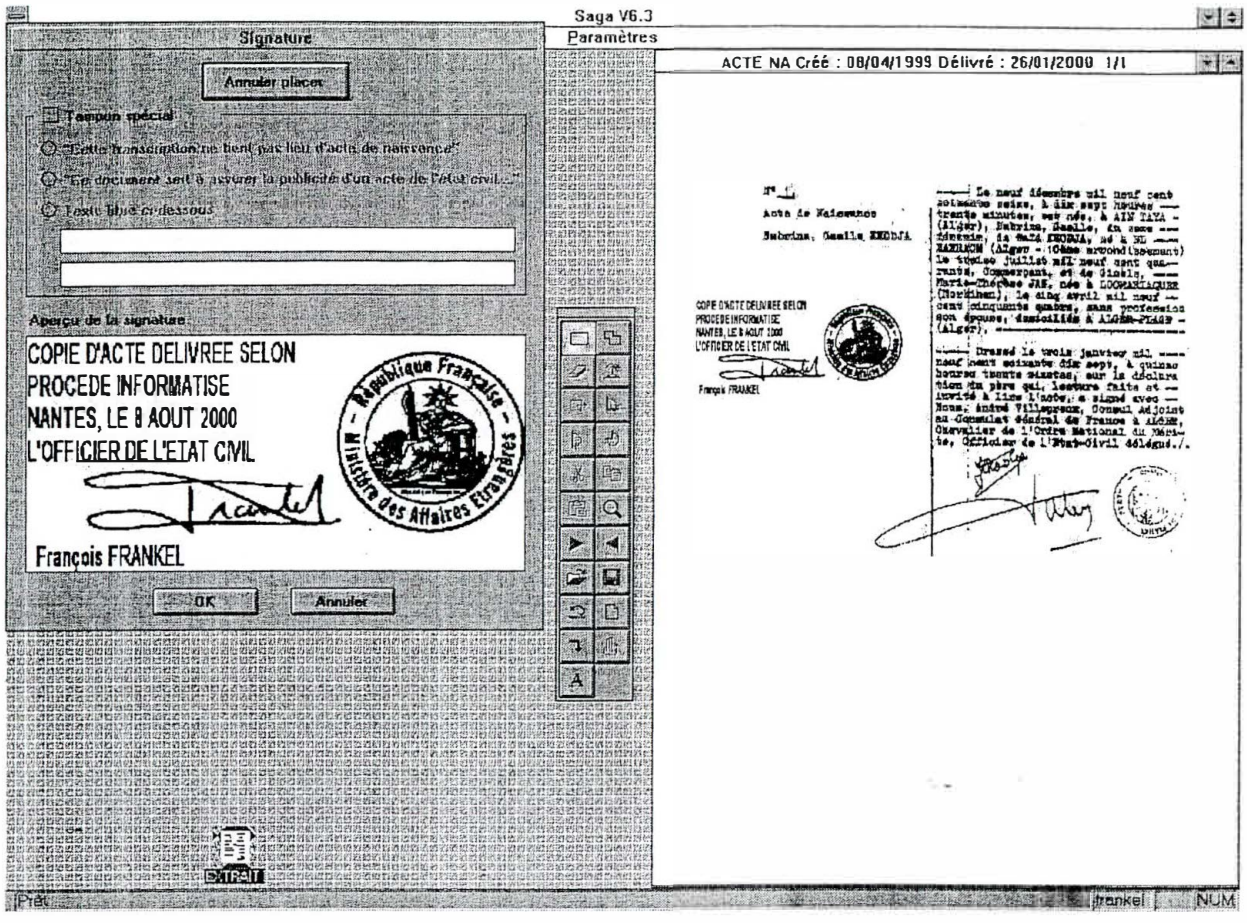


FIG. 3.3 – *Application de la signature de l'officier d'état civil à un acte numérisé — logiciel « SAGA » du Service central d'état civil de Nantes. A gauche, la boite de dialogue contenant le sceau, la signature, la mention « Copie d'acte ... », la date, etc. ; à droite, le document numérisé avec la signature de l'officier, prêt à être imprimé.*

journalisation automatique des prodécures informatiques assurent leur traçabilité. L'accès aux locaux contenant les documents numérisés et au papier sécurisé est contrôlé par les procédés traditionnels de clés et serrures, et l'accès aux postes de travail des officiers d'état civil est quant à lui contrôlé par mot (ou phrase) de passe. De plus, l'utilisation de la signature numérisée de l'officier est strictement guidée par le système : l'image numérisée de la signature ne réside pas sur le poste de travail de l'officier mais bien sur un serveur central, n'étant transférée qu'au moment de l'identification de l'officier à son poste de travail ; la signature n'est utilisable que dans les modalités définies par le système (comme celles visibles à la figure 3.3) et ne peut être extraite pour une utilisation non-conforme.

La solution développée par le SCEC remplit tout à fait les conditions pour la signature énoncées par la loi du 13 mars (article 1316-4, alinéa 2) : elle fournit une identification fiable de l'officier d'état civil ayant apposé sa signature sur l'acte, à la fois par la vérification traditionelle des signatures et par les mécanismes de journalisation qui permettent de retracer les actions sur les actes ; elle garantit le lien avec l'acte auquel elle s'attache, puisque l'acte signé n'est accessible que sur un support papier sécurisé qui assure l'origine et l'intégrité de l'acte.

La solution développée par le SCEC est utilisable *dès à présent* et s'intègre directement dans l'univers bureaucratique *tel qu'il existe aujourd'hui*. En préservant les caractéristiques visuelles des documents d'état civil (sceau, signature), elle s'intègre sans effort aux schémas cognitifs des différents intervenants. Cette solution tire donc son efficacité d'une analyse adéquate du cycle de vie du document et de son réseau de distribution — et non de l'application d'une solution technologique déterminée préalablement à toute évaluation des problèmes à résoudre. Si l'on considère qu'un tel système intégrera éventuellement la distribution des actes par voie électronique, il est clair qu'il faudra alors utiliser des technologies supplémentaires pour assurer l'intégrité des documents en transit — je suggère à cet égard des voies de réflexion à la conclusion de ce chapitre.

En résumé, lorsque l'on considère *l'ensemble global* des procédures de distribution et de sécurisation des documents, la signature numérisée est un élément important dans la boite à outils des institutions qui désirent informatiser leur processus de production et de délivrance de documents administratifs.

3.5 Conclusion

Après la description de ces quatres modèles très différents de réalisation de la signature électronique, on remarque que chacune de ces technologies traite le mieux **un aspect précis** de la signature manuscrite :

1° La cryptographie établit le mieux **le lien entre signature** et **document** dans le contexte de la transmission à distance. Par contre, elle ne dispose d'aucune représentation visuelle et n'établit pas de lien direct avec la personne (c'est le rôle de la certification). Elle est idéalement adaptée à la signature automatique par des machines ;

2° La biométrie permet de s'assurer de **la présence physique du signataire** lors de la signature et, des quatre technologies, reproduit le mieux la dimension rituelle du consentement ;

3° Le tatouage visible et la signature numérisée permettent de traiter **les marques visuelles d'authenticité** comme le sceau et le filigrane, reproduisant, en quelque sorte, l'incrustation de l'encre au sein du papier ;

4° Le tatouage invisible permet de réaliser **la traçabilité des documents électroniques**, en incluant au sein de l'image des informations comme la date, le poste de production et le numéro de série.

Il est tout à fait plausible d'imaginer que des solutions technologiques évolueront qui harmoniseront ces approches en des configurations variables, selon la nature des documents considérés. La préservation des qualités visuelles des documents jouera sûrement un rôle important pour les actes qui ont traditionellement fait usage de la riche palette des signes de l'authenticité — sceau, tampons, filigranes, signature manuscrite, etc. Un rapprochement s'effectura naturellement entre l'exigence de la présence physique de l'officier public et l'utilisation de la biométrie. La cryptographie s'imposera dès qu'il s'agira d'assurer l'intégrité d'un document transitant électroniquement au sein d'un réseau ouvert, sans qu'on doive nécessairement conceptualiser cette « signature » cryptographique comme celle apposée sur le document.

Cependant, contrairement au dogmes qui circulent, **l'utilisation de la cryptographie à des points précis du système n'impose pas que l'on adopte dans son ensemble la (Sainte) Trinité cryptographie-PKI-carte à puce.** Ce modèle de sécurité impose en effet une harmonisation excessive des pratiques bureaucratiques, ne tenant pas compte des différentes cultures organisationelles des institutions. Il est plus efficace, moins coûteux et, en bout de ligne, globalement plus sécuritaire de laisser chaque

institution déterminer la façon dont elle désire sécuriser la circulation des documents à l'interne. En effet, considérons le modèle de circulation des documents présenté à la figure 3.4 : on y voit deux institutions (origine et arrivée) qui échangent des documents entre elles et avec un individu au sein d'un réseau *ouvert* (c'est-à-dire ouvert à des individus susceptibles de commettre des fraudes). Chaque institution dispose de son propre réseau *fermé* (représenté par le cercle intérieur ombré) — ce qui peut être obtenu par différents moyens techniques (mur coupe-feu, contrôle d'accès, etc.) Pour échanger des documents avec des individus, les institutions utilisent un papier sécurisé assurant un minimum de protection contre la contrefaçon et la reproduction. Pour échanger des documents entre elles, les institutions utilisent une *passerelle* (représentée par le cercle extérieur) : c'est cette passerelle qui assure la traduction entre les technologies de sécurisation utilisées à l'interne et les technologies cryptographiques utilisées pour la communication au sein du réseau ouvert.

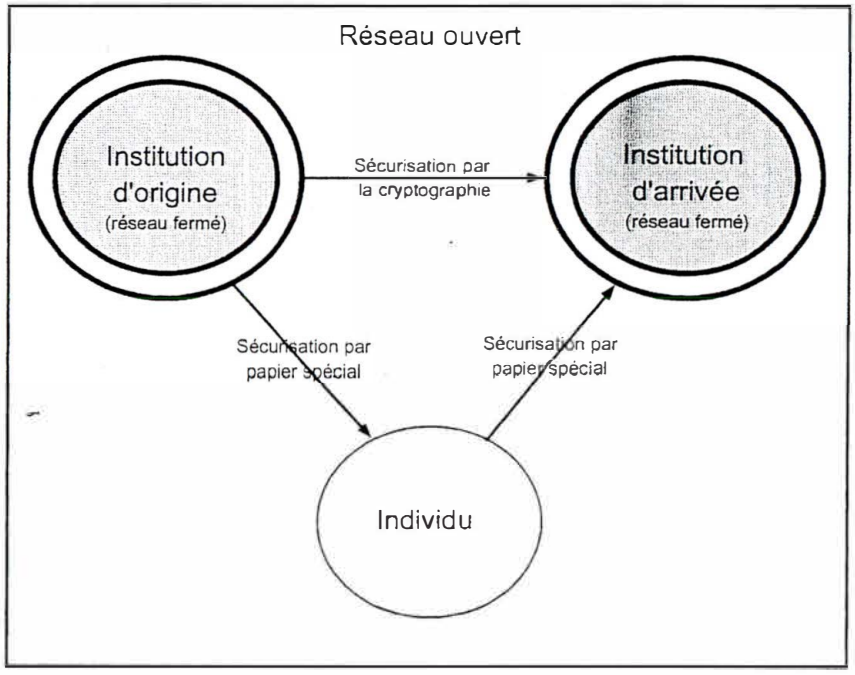


FIG. 3.4 - *Circulation d'un document entre institutions et individus*

Si l'institution d'origine dispose d'une politique de sécurité interne dont la composante principale est l'application de la peine capitale à toute personne tentant de falsifier un document, ceci ne devrait pas avoir d'impact sur l'institution d'arrivée qui peut, quant à elle, décider d'investir dans un système qui soit en accord avec sa propre culture institutionnelle, la nature de documents, les relations avec les partenaires, etc. — par exemple, s'en remettre entièrement à la bonne foi de ses membres. [41]

41. La Loi type de la CNUDCI sur le commerce électronique suggérait à l'alinéa 58 une telle considération de l'ensemble des facteurs de sécurité : « *Pour déterminer si la méthode utilisée en vertu du paragraphe 1 est appropriée, les facteurs juridiques, techniques et commerciaux à prendre en considération sont les suivants : 1) le degré de perfectionnement du matériel utilisé par chacune des parties ; 2) la nature de leur activité commerciale ; 3) la fréquence avec laquelle elles effectuent entre elles des opérations commerciales ; 4) la nature et l'ampleur de l'opération ; 5) le statut et la fonction de la signature dans un régime législatif et réglementaire donné ; 6) la capacité des systèmes de communication ; 7) les procédures d'authentification proposées par les opérateurs des systèmes de communication ; 8) la série de procédures d'authentification communiquée par un intermédiaire ; 9) l'observation des coutumes et pratiques commerciales ; 10) l'existence de mécanismes d'assurance contre les messages non autorisés ; 11) l'importance et la valeur de l'information contenue dans le message de données ; 12) la disponibilité d'autres méthodes d'identification et le coût de leur mise en œuvre ; 13) le degré d'acceptation ou de non-acceptation de la méthode d'identification dans le secteur ou domaine pertinent, tant au moment où la méthode a été convenue qu'à celui où le message de données a été communiqué ; et 14) tout autre facteur pertinent.* »

Plutôt que de tenter d'imposer le même modèle de confiance à chacun des éléments du système, il est beaucoup plus facile et bureaucratiquement écologique d'établir des passerelles qui assurent la traduction entre les différents régimes de confiance et de sécurité propres à chaque institution.

Un telle passerelle pourrait, par exemple, prendre la forme d'une PKI où *une seule paire de clés privée/publique est attribuée à chaque institution.*[42] Les documents qui doivent circuler à l'extérieur de l'institution sur un réseau ouvert comme l'Internet peuvent être sécurisés par l'utilisation de ces clés (signature et/ou chiffrement), chaque institution étant alors en mesure de vérifier que les documents ont transités au sein du réseau sans subir de modifications. Un tel système réduit de façon considérable les inconvénients des technologies de PKI — comme le foisonnement des clés et des certificats — mais présente évidemment peu d'attrait pour les sociétés de certification puisqu'il va à l'encontre de leur intérêt commercial, qui consiste à vendre (et renouveler) le plus grand nombre de certificats possibles. [43]

Il semble clair que l'acte authentique se trouve au seuil d'une mutation profonde et inévitable, fruit de la progression inlassable des technologies de l'information et de la communication au sein des administrations. Cependant, cette mutation est principalement conceptualisée selon la nature de l'outil qui domine actuellement le marché. Cette domination, fruit de phénomènes conjecturels, impose une analyse extrèmement réductrice de la sécurité informatique, analyse qui subit une critique grandissante de la part des experts en sécurité. [44] Il est donc impératif que **la réflexion se poursuive sur les bases d'une analyse des besoins** et dans l'esprit d'une adéquation des technologies à ces besoins. C'est seulement au prix de cet effort que la spécificité de l'acte authentique comme outil de sécurisation juridique de droit civil pourra être maintenue, et non diluée par l'utilisation irréfléchie de technologies difficilement compatibles avec son principe.

42. Ce modèle a été adopté par, entre autres, la société TenFour (`www.tenfour.se`) pour son logiciel de courrier sécurisé, par la société Atos (`www.atos-group.com`) pour son système de cartes Securicam et par la société PenOp (`www.penop.com`) pour l'intégration de son produit de signature biométrique aux PKIs.

43. Peut-être ceci peut-il fournir une motivation supplémentaire à la création d'un service public de la certification?

44. En fait, tout ceux qui ont osé se confronter au terrain: j'ai cité tout au long de ce document Ross Anderson, Bruce Schneier, Dorothy Denning.

Chapitre 4

Archivage

L'archivage des documents électroniques présente en soi des défis extraordinaires, et des problèmes inédits : comment, en effet, s'assurer de la pérennité des documents, quand toute l'infrastructure se renouvelle? L'archivage et l'exploitation des actes authentiques introduit une dimension supplémentaire au problème : comment assurer la pérennité des technologies de signature électronique utilisées sur les documents archivés et/ou exploités? L'interaction entre les multiples technologies utilisées est d'une complexité extraordinaire mais la solution réside peut-être tout simplement dans l'utilisation de mécanismes sociaux avec lesquels nous sommes déjà familiers. Les représentants de la Direction des Archives de France ont suggéré que « [l]a dématérialisation des documents, de leur forme de conservation à long terme et celle à venir de leur communication, est ... susceptible de remettre profondément en cause la structure institutionnelle de la politique d'archivage en France ... ». [1] Ce chapitre suggère que cette dématérialisation est également susceptible d'élargir les missions dont sont investies les institutions d'archivage en France, en leur adjoignant des fonctions supplémentaires de contrôle de l'intégrité. [2]

La première observation qui devrait guider toute réflexion sur l'archivage est que, « dans l'état actuel des choses, il est impossible de garantir la longévité et l'intelligibilité de données numériques pour même une seule génération humaine. » [3] Ceci n'est pas une prédiction négative, mais simplement le constat lucide de l'immaturité de nos connaissances dans ce domaine, constat d'une communauté — celle des bibliothécaires et des archivistes — qui travaille depuis plusieurs années déjà sur la question. Cette communauté est une excellente source d'informations, ayant mené depuis de nombreuses années déjà une réflexion soutenue sur ces questions difficiles, de même que certaines expériences concrètes.

On peut distinguer trois problématiques distinctes concernant l'archivage des écrits électroniques : 1° la pérennité du support de l'écrit ; 2° la pérennité du format d'encodage de l'écrit ; 3° la pérennité des technologies de sécurisation de l'écrit. On connaît pas mal de choses sur le premier, beaucoup moins sur le second, presque rien sur le troisième, et **absolument rien sur l'interaction entre les**

1. CLEYET-MICHAUD, DHÉRENT, ERMISSE, « Remarques de la Direction des Archives de France sur la dématérialisation des actes authentiques », janvier 2001.

2. Fonction qu'elles exercent peut-être déjà implicitement : « Les auteurs classiques du droit de l'Ancien Régime (Pothier, Dumoulin) allaient jusqu'à admettre que la présence d'un document dans les archives publiques lui garantissait *ipso facto* un caractère d'authenticité. La jurisprudence actuelle n'irait sans doute pas aussi loin dans cette présomption ; elle n'en continue pas moins à accorder, en matière de publicité, une place privilégiée à l'entrée dans les fonds publics. » Hervé BASTIEN, *Droit des archives*, Paris : La Documentation Française, 1996, p. 7.

3. G. LAWRENCE, W. KEHOE, O. RIEGER, W. WALTERS, et Anne KENNEY, *Risk management of digital information: a file format investigation*, Council on Library and Information Resources, juin 2000.

trois.

(1) **Pérennité du support**: Le premier sujet a été traité de main de maître par M. Dominique PONSOT, dans son rapport sur les technologies d'archivage numérique ou par microfilm. [4] Je ne reviendrai donc pas sur cet aspect du problème, sauf lorsque nécessaire.

(2) **Pérennité de l'encodage**: Cinq solutions sont possibles pour la préservation de documents électroniques: 1° l'approche « copie papier » — imprimer une copie du document sur le papier; 2° l'approche « standard universel » — développer un format standard et y migrer tous les documents; 3° l'approche « musée de l'informatique » — conserver tout les équipements nécessaires à la lisibilité des formats; 4° l'approche « émulation » — émuler par des logiciels les équipements périmés; 5° l'approche « migration » — migrer périodiquement les fichiers vers les nouvelles versions des formats. Chacune de ces solutions comportent des avantages et des désavantages, [5] mais la solution de migration périodique des fichiers semble la plus réaliste en ce moment. [6]

Pérennité de la sécurisation: Je ne connais *aucune* étude à ce jour qui puisse prétendre avoir sérieusement examiné la question de l'interaction entre la migration des documents et les procédés de sécurisation de ces documents. Très peu d'études *concrètes* existent sur la migration à grande échelle de librairies de documents électroniques, [7] et aucune sur les difficultés que présentent la migration simultanée des procédés mathématiques — qu'ils soient biométriques, cryptographiques ou basés sur le tatouage — vers les nouveaux formats d'encodage et les nouveaux supports. [8]. Or, en matière de sécurité électronique, ce sont les interactions imprévues entre les différents systèmes techniques qui procurent la plupart des failles pouvant être exploitées dans un but de fraude. On ne peut donc considérer les questions de migration de support, d'encodage et de sécurisation des écrits électroniques comme si elles existaient en isolation les unes des autres. [9]

Une solution à la pérennisation des procédés cryptographiques de signature est couramment mentionnée — la *resignature* — sans que l'on sache pourtant de quoi il en ressort exactement. Nous allons donc consacrer un peu d'énergie à explorer la logique de cette solution, en utilisant deux documents — *Electronic signature formats*[10] et *Trusted Archival Services*[11] — produits par le projet de standardisation de la signature électronique en Europe EESSI *(European Electronic Signature Standardization Initiative)*, et nous en servir pour dégager des principes généraux concernant la pérennisation des procédés de signature électronique.

4. M. Dominique PONSOT, *Valeur juridique des documents conservés sur support photographique ou numérique*, Observatoire juridique des technologies de l'information, 1995, disponible auprès des services de documentation du Premier ministre.

5. D. BEARMAN, « Reality and Chimeras in the Preservation of Electronic Records », *D-Lib Magazine*, April 1999.

6. La conservation d'une copie papier est certainement une mesure de sécurisation louable dans le contexte d'une familiarisation graduelle avec le document électronique, ou encore, la conservation simultanée de formats numériques et photographiques, l'approche adoptée par le CNAV pour son programme d'archivage des dossiers de retraire.

7. Une des plus intéressantes: supra, *Risk management of digital information: a file format investigation.*

8. Une étude produite dans le cadre du projet EESSI examine la question de la pérennité des signatures cryptographiques — voir Olivier LIBON, Andreas MITRAKAS, Angelika SCHREIBER, Jos DUMORTIER, Patrick VAN EECKE et Sofie VAN DEN EYNDE, « Trusted Archival Services », EESSI Report, août 2000

9. Par exemple, les fonctions de hachage qui fondent la signature cryptographique permettent de déceler toute modification au document numérique, fut-elle d'un seul bit. Cependant, elles n'effectuent aucune distinction entre une modification qui surviendrait à la suite d'une tentative de fraude, ou à la suite d'une migration du format de fichier.

10. *Electronic Signature Formats*, ETSI TS 101 733 V1.2.2 (2000-12).

11. supra, *Trusted Archival Services.*

4.1 Pourquoi la resignature?

La seule évocation du principe de la resignature fait frémir tant les praticiens que les théoriciens du droit. [12] C'est que ce principe, en tentant de répondre à une problématique particulière à la cryptographie, introduit des modalités d'utilisation de la signature électronique qui semblent difficilement conciliables avec les solennités requises par l'acte authentique : qui peut imaginer que le notaire (ou autre officier public) resigne personnellement et périodiquement chacun des actes de son minutier? Et si cette resignature était plutôt le fruit d'une procédure automatisée, que pourrait bien être sa valeur juridique et sa relation à la signature originale de l'officier public? Pour bien comprendre ces questions et les réponses possibles, il faut une nouvelle fois effectuer un pas en arrière.

Quelle est la finalité de l'archivage des moyens de sécurisation des écrits électroniques? D'un part, on veut pouvoir exploiter ces actes (production de copies conformes, etc.), et d'autre part, on voudrait que, dans l'éventualité d'une opposition à un tel écrit — c'est-à-dire dans le cadre d'un procès, devant un juge — on puisse vérifier que la signature est belle et bien valide. Considérons un instant la figure 4.1 représentant la ligne de vie d'une signature électronique :

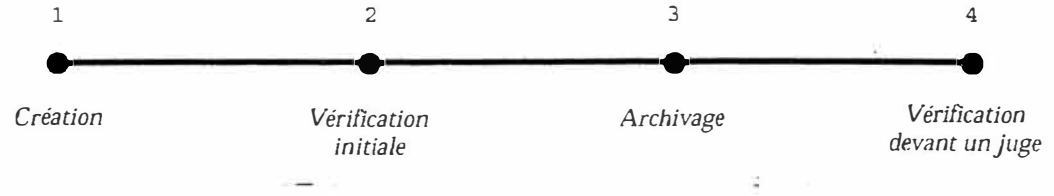


FIG. 4.1 – *La ligne de vie d'une signature électronique*

Au moment (1), la signature est créée par le signataire. Celui-ci l'envoie au destinataire, qui (2) effectue les vérifications nécessaires pour s'assurer de la validité de la signature — nous reviendrons plus tard sur la forme exacte de ces vérifications. Si le processus de validation réussit, le document est (3) archivé de même que la signature électronique, dans l'éventualité d'une contestation qui nécessiterait que (4) la signature sur le document soit vérifiée de nouveau devant un juge. Évidemment, la phase (4) est rarissime, mais tout le but du processus d'archivage est quand même de pouvoir réaliser correctement cette opération si elle doit avoir lieu. **Toute la difficulté vient du laps de temps plus ou moins grand qui sépare les vérifications en (2) et en (4).**

Comme nous l'avons déjà vu (section 3.1.5), la cryptographie fonde et mesure sa sécurité sur la taille des clés : pour rendre un système cryptographique plus sécuritaire, il suffit d'augmenter la taille de la clé utilisée (avec évidemment un coût afférent sur la rapidité du système). Mais quelle taille faut-il utiliser et pour combien de temps procure-t-elle une sécurité suffisante? La recherche d'une réponse à ces questions a donné naissance à une petite industrie académique parallèle : l'amélioration des algorithmes qui permettent de casser les procédés de cryptographie à clé publique — qu'ils soient fondés sur le problème de RSA [13] ou d'autres approches, comme celle des courbes elliptiques. [14]

12. Les réactions de l'audience à la présentation de ce concept lors du colloque *Vers l'authenticité électronique* tenu à Paris le 11 décembre 2000 étaient on ne peut plus explicites.

13. Le dernier record est la factorisation d'un nombre de RSA de 512 bits — voir CAVALAR, DODSON, LENSTRA, et al., « Factorization of a 512-Bit RSA Modulus » in *Advances in Cryptology — EUROCRYPT 2000*. LNCS 1807, Springer 2000, pp. 1-17.

14. Voir, par exemple, `http://www.inria.fr/Presse/pre67-fra.html`.

Ainsi, la sécurité procurée par la cryptographie diminue avec le temps, et il est loin d'être simple d'évaluer avec précision le *taux de cette diminution*.[15] Un message pouvant être chiffré en toute confiance avec une clé de n bits au temps t pourra être déchiffré au temps $t + x$ années — et similairement pour un message signé cryptographiquement. Ceci est problématique car si l'écart entre les moments (2) et (4) est suffisamment grand, alors la vérification devant le juge ne pourra être valide, car l'assise fondamentale de la sécurité cryptographique sera faussée par la possibilité que la taille des clés initialement utilisée soit désormais insuffisante. C'est donc à ce problème que tente de répondre la resignature — resignature qui n'en est pas tout à fait une, comme nous allons à présent le constater.

4.2 L'approche EESSI

L'EESSI est un projet financé par la Communauté européenne dans le but de fournir des standards techniques réalisant les concepts de signature électronique énoncés par la Directive européenne.[16] L'EESSI a déjà produit un certain nombre de documents qui nous permettront de mieux comprendre la logique qui sous-tend à l'archivage des signatures cryptographiques. Ces documents d'une nature extrêmement technique ne sont pas d'un accès facile, même pour des experts chevronnés. La lecture qui s'en suit se veut donc une visite guidée d'une petite partie de cet univers, celle qui se propose de résoudre le problème de l'archivage à long terme des signatures électroniques.

Dans l'optique de la signature cryptographique, *la vérification* de la signature est le seul moyen de s'assurer qu'une signature est valide, c'est-à-dire que l'on doit obtenir toutes les composantes qui forment la signature cryptographique et les fournir à l'algorithme de validation pour obtenir la réponse `valide/invalide`. La figure 4.2 reproduit le processus de validation du format de signature *ES-A (Electronic Signature - Archive Validation Data)*, un format développé pour permettre la vérification de la signature longtemps après sa création. Dans le contexte de la ligne de vie d'une signature électronique (figure 4.1), le processus représenté à la figure 4.2 correspond à la validation effectuée au moment (2), dans le but de former un objet qui puisse être utilisé dans une validation au moment (4).

15. Lors de la présentation du système RSA dans les pages du *Scientific American* d'août 1977, les auteurs offrirent un prix de 100 dollars à quiconque réussirait à déchiffrer un message chiffré à l'aide d'une clé de 425 bits, prédisant qu'un tel exploit nécessiterait des milliards d'années de calcul sur ordinateur. Or, le contenu de ce message (« *and the magic words are squeamish ossifrage* ») fut déchiffré le 27 avril 1994, moins de 20 ans après la publication du défi — voir `http://www.math.okstate.edu/ wrightd/numthry/rsa129.html`.

16. Voir `http://www.ict.etsi.org/eessi/EESSI-homepage.htm`.

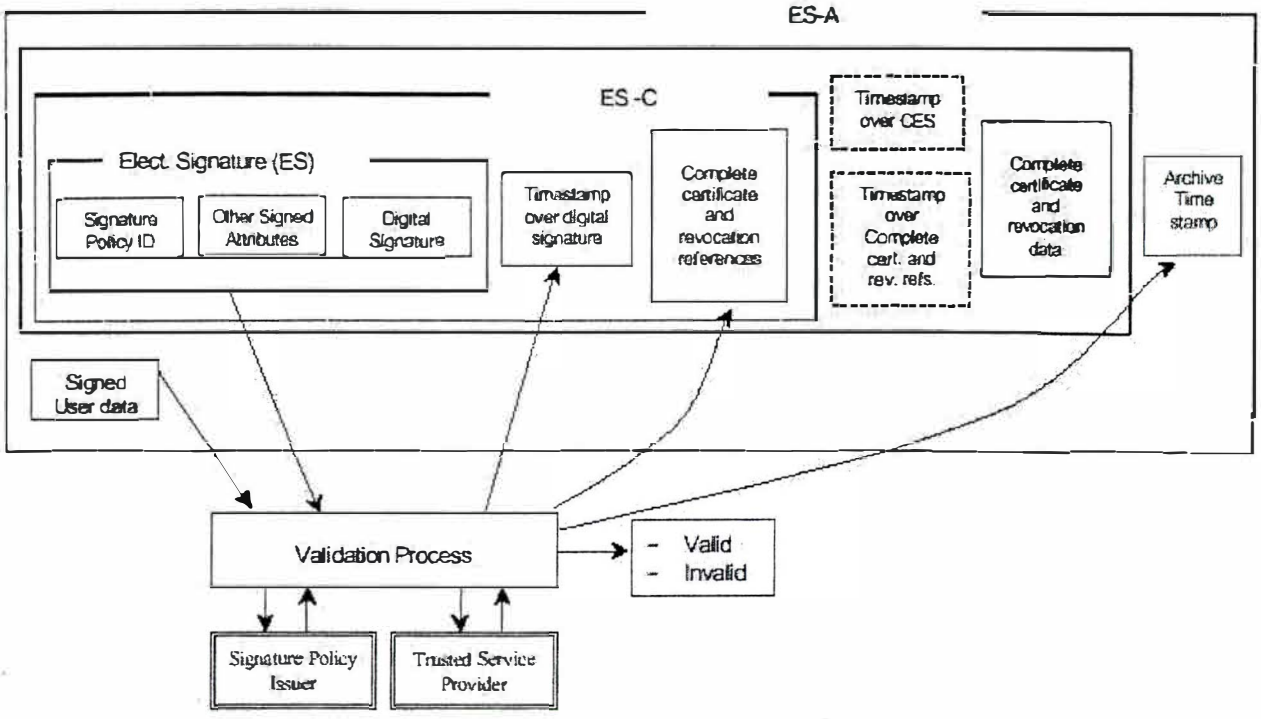


Figure 12: Illustration of an ES with Archive Validation Data

FIG. 4.2 - *Validation du format de signature électronique ES-A — tiré de « Electronic signatures formats » ETSI TS 101 733 V1.2.2 (2000-12).*

Le processus de validation implique six éléments principaux : (1) le rectangle intérieur marqué *ES* ; (2) un algorithme de validation (rectangle marqué *Validation Process*) — qui reçoit en entrée les éléments de (1) et interagit avec (3) l'émetteur de la politique de signature *(Signature Policy Issuer)* et (4) des fournisseurs de service de confiance *(Trusted Service Provider)* pour finalement émettre en sortie une réponse (5) : la signature est valide ou n'est pas valide ; si la signature est valide, alors le processus produit (6) les éléments du rectangle supérieur (marqué *ES-A*), c'est-à-dire l'ensemble des éléments de la signature archivée. Le processus technique est le suivant : tout d'abord, le processus réalise la validation initiale (moment (2) de la ligne de vie), ce qui implique, dans l'ordre, de :

1° Obtenir le certificat à clé publique du signataire d'une des Autorités de confiance *(Trusted Service Provider)* ; obtenir le certificat à clé publique de l'Autorité de certification qui a signé le certificat du signataire ; si nécessaire, obtenir le certificat à clé publique de l'Autorité de certification qui a signé le certificat de la première Autorité de certification ; répéter jusqu'à l'obtention d'un certificat-racine ;

2° Vérifier sur les listes de révocation relatives à chacun de ces certificats si le certificat a été révoqué. Si oui, la signature est invalide ; si non, vérifier, pour chacun des certificats, s'il a été suspendu ; si oui, attendre jusqu'à la fin de la période de suspension du certificat et reprendre le processus à l'étape 1° ;

3° Vérifier chacune des signatures sur les certificats, dans l'ordre du chemin de certification, en partant du certificat-racine ; si l'une de ces signatures est invalide, alors la signature est invalide ;

4° Calculer, à l'aide de la fonction de hachage spécifiée dans la Politique de signature *(Signature*

policy), le condensé du document qui est l'objet de la signature *(Signed User data)* ;

5° Appliquer la clé publique contenue dans le certificat à clé publique du signataire au condensé calculé à l'étape précédente ; si le résultat est identique à la signature numérique (*Digital Signature*, troisième élément du rectangle ES), la signature est valide, sinon elle est invalide ;

Ensuite, le processus de validation construit l'objet qui pourra servir au moment (4), ce qui implique, dans l'ordre, de :

1° Horodater la signature numérique (bloc marqué *digital signature*) de façon à lui donner une date, date qui permettra d'établir l'existence de la signature relative aux listes de révocations et à la période de validité des certificats ; ajouter les références complètes à tous les certificats utilisés de même qu'aux informations de révocation — l'objet résultant a pour nom *ES-C* ;

2° Horodater le bloc *ES-C* ; horodater les références aux certificats et aux informations de révocation ; ajouter les certificats eux-mêmes et les données de révocation ; ajouter le document original, objet de la signature ;

3° Horodater le tout — l'objet résultant est une signature de format *ES-A* ;

4° Répéter l'étape précédente à chaque fois que la taille des clés ou la force des algorithmes utilisé par l'Autorité d'horodatage n'est plus jugée suffisante.

Le document ne précise pas à quoi ressemblerait le processus de validation de l'objet *ES-A* — une omission que l'on ne peut que regretter — mais il faudra ajouter aux vérifications mentionnées ci-dessus la vérification de chacun des horodatages. En effet, dans le modèle EESSI, l'horodatage d'un document par une Autorité d'horodatage s'effectue en deux opérations simples : (a) ajouter au document une date et une heure obtenue d'une source fiable et (b), signer le tout avec la clé privée de l'Autorité. Ces horodatages sont donc en fait des signatures supplémentaires pour lesquelles on devra également vérifier la chaîne de certification. [17]

4.3 Conclusions

Nous sommes donc à présent en mesure d'apprécier que le principe de resignature proposé par l'EESSI pose comme principe que, dans le contexte de la ligne de vie de la signature, le moment (4) de vérification devant le juge doit correspondre en tout point au moment (2), c'est-à-dire que *le juge doit être en mesure de répéter la même expérience qui a eu lieu lors de la vérification initiale*. Un tel principe suppose qu'il dispose également, 30, 60, ou 100 ans plus tard, de réalisations des algorithmes *identiques* à ceux qui ont initialement crées et vérifiés la signature — alors que les plates-formes informatiques, systèmes d'exploitation et logiciels originalement utilisés auront tous disparus depuis longtemps. Si on a depuis longtemps identifié que le changement technologique entrainait des conséquences importantes sur la *lisibilité des écrits électroniques*, on n'a pas constaté que le problème se pose avec tout autant d'acuité pour la *reproductibilité de la preuve électronique*.

Il est donc possible que le désir de construire un objet qui survive à la fois à l'expérience du moment (2) et au moment (4) procède d'hypothèses irréalistes. Une autre voie est-elle possible ? Oui, et elle est en fait discrètement évoquée par le document EESSI à la section 4.3 :

> « *Quand il y a exigence d'une signature valide sur une long durée sans utilisation de l'horodatage, alors il y a nécessité d'un enregistrement sécurisé de la date de la vérification (de la signature*

17. Le cas présenté est le plus simple (et le plus inintéressant, au niveau contractuel) : un document signé par une seule personne. Il ne traite ni la questions des certificats d'attributs, ni celle des signatures multiples sur un même document, chacun de ces certificats et de ces signatures dépendant de leur propre chaîne de certification.

numérique) associé à la signature elle-même. »[18] (*Electronic Signature Formats*, sec. 4.3)
C'est-à-dire qu'une autre façon de procéder est tout simplement d'archiver au moment (3) une *attestation constatant la vérification de la signature* à un certain moment. L'écart entre le moment (2) de la vérification initiale et le moment (3) de l'archivage étant nettement plus court que celui séparant (2) et (4), une similarité satisfaisante entre les deux expériences est nettement plus plausible et permettrait une nette réduction de la complexité de la signature archivée. Le moment le plus approprié pour cette validation reste à raffiner, mais on peut imaginer qu'il pourrait avoir lieu à la fin de la période d'utilisation courante, où un tri est effectué entre les documents destinés à être conservés et ceux destinés à l'élimination.[19]

Quelque soit la solution adoptée, la question de l'archivage des technologies de sécurisation des documents électroniques pose le problème de définir quel sera exactement la forme de l'objet probatoire que l'on désire conserver, et la nature de l'expérience qui sera à même de faire « dire » à cet objet l'événement dont il est le témoin fidèle, longtemps après sa création. Cette question ne fait actuellement l'objet d'aucun débat, si ce n'est au sein de documents techniques inaccessibles aux non-initiés, même si elle est l'une des fonctions essentielles des archives.[20]

18. « *When there is a requirement for long term signatures without timestamping the digital signatures, then a secure record is needed of the time of verification in association with the electronic signature [...].* »

19. Loi no. 79-18 du 3 janvier 1979 sur les archives, article 4.

20. Comme note finale, il est amusant d'observer les procédures que le document EESSI *Electronic Signature Formats*, document consacré à la spécification de mécanismes visant à établir l'origine et l'intégrité d'écrits électroniques, utilise pour établir *sa propre intégrité*: à la page 2, il est précisé que « ce document peut être rendu disponible sous plus d'une version électronique ou imprimée. Dans l'éventualité de différences perçues ou réelles quant au contenu de ces versions, la version de référence est celle en format PDF *(Portable Document Format)*. En cas de dispute, la référence sera l'impression sur les imprimantes d'ETSI de la version PDF conservée sur un disque réseau conservé au secrétariat d'ETSI. » La politique d'ETSI, institution de normalisation des nouvelles technologies, avalise donc explicitement le choix d'un encodage « fixant » l'information, de l'archivage par une institution de confiance et . . . de la copie papier comme témoins privilégiés de l'intégrité de l'information électronique.

Chapitre 5

Conclusions

La sécurité est toujours fonction d'une multiplicité de facteurs : Toute solution de sécurité qui mérite ce nom mêle étroitement technique, déontologie, formation, information, réglementation, et pénalisation. Chacun de ces facteurs est nécessaire au succès de la solution adoptée, et aucun ne fonctionne isolément des autres. Il faut considérer le *faisceau des règles* qui, collectivement, créent une solution de sécurité. Aucune technologie n'est en mesure d'adresser à elle seule l'ensemble des maillons de la chaîne.

Reconfiguration et non pas élimination du risque : L'euphorie qui entoure la nouvelle économie tend à présenter les technologies de signature électronique comme un *progrès* sur la signature traditionnelle. Il faut plutôt réfléchir en termes de nouveaux avantages, et de nouveaux risques. L'informatisation n'a pas éliminé le risque de fraude, bien évidemment. Plutôt, on fait dorénavant face à une nouvelle configuration du risque. Il faut donc tenter de déterminer à quoi correspond cette nouvelle donne, une tâche cruciale puisqu'elle détermine la sélection des technologies de sécurité appropriées à ce risque. [1]

Mixité du papier et de l'électronique : Nous ne vivons pas dans un univers du tout électronique, bien au contraire, et ce, particulièrement dans les professions judiciaires. Plutôt que de partir d'une idéologie de l'électronique à tout prix, il vaut mieux adopter un point de vue pragmatique et tenir compte du fait que le papier et l'électronique s'entremêlent à de multiples points de passage, et ce, pour de nombreuses années encore. Moins esthétique que les fantasmes de virtualité totale, mais plus proche de la réalité. [2]

Sécurisation des documents matériels : Il existe un très riche réservoir d'expérience dans la production de documents sécurisés — passeports, billets de banque, cartes de crédits, etc. Ces documents utilisent typiquement un combinaison de techniques pour faire échec à la fraude, plutôt que de se reposer sur une seule méthode : papiers et encre spéciaux, filigranes, hologrammes, polymères

1. Une tache cruciale et difficile, puisque, comme le souligne Dorothy Denning, experte en sécurité informatique : « *Il est facile d'évoquer des scénarios tels que "la bourse s'effondre après que des* hackers *bidouillent avec les ordinateurs de Wall Street" ou encore "deux avions se heurtent après que des terroristes tripatouillent les systèmes de navigation". Il est beaucoup plus difficile d'évaluer si de tes scénarios sont plausibles ou non. La grande question est celle-ci : Est-ce que quelqu'un peut lancer une attaque avec des conséquences catastrophiques et, si c'est le cas, quelles sont les probabilités qu'un tel événement se produise? En vérité,* personne ne le sait. » Dorothy E. DENNING, *Information Warfare and Security*, Addison Wesley, 1999.

2. Voir à sujet l'article de deux spécialistes du domaine, Ziming LIU et David G. STORK « Is Paperless Really More? Rethinking the Role of Paper in the Digital Age » *Communications of the ACM* 43:11(94-97), qui suggère que le développement du document électronique va stimuler une synergie entre l'univers papier et l'univers électronique, plutôt que l'un supplante simplement l'autre.

et adhésifs, etc. Puisque le papier et l'électronique continueront de co-exister, on peut tirer profit des expériences déjà acquises dans ce domaine. Ainsi, la sécurisation électronique — que ce soit par la cryptographie ou par d'autres méthodes — continuera de co-exister avec des méthodes de sécurisation matérielle.

Hybridicité du document électronique : Il faut considérer le document électronique comme un objet dépendant à la fois de son format d'encodage, du logiciel de lecture, des périphériques de visualisation et d'impression, et du matériel sous-jacent. On ne peut considérer ces éléments de façon indépendante, comme on pouvait le faire dans le cas du papier.

Pluralité des moyens techniques : Une des caractéristiques du débat sur la signature électronique, c'est que la discussion est dominée par des solutions basées sur les technologies cryptographiques. Même les textes qui se réclament d'une approche « technologiquement neutre » — la Directive européenne notamment — sont en fait hantés par la cryptographie. Or, il existe plusieurs autres solutions — la signature biométrique par exemple — qui permettent de réaliser la signature électronique, chacune avec ses caractéristiques. Ce document veut aider les juristes à s'extirper de la pensée unique qui voudrait imposer le couple cryptographie-PKI comme la seule réalisation possible de la signature électronique.

Efficacité juridique : D'où provient l'efficacité juridique de l'acte authentique? On désire un acte qui soit sûr, c'est-à-dire, entre autres choses, qui ne soulève pas de contentieux au niveau de son intégrité. Il y a tout lieu de se poser la question de la relation entre efficacité technologique et efficacité juridique. Un acte authentique électronique où, par exemple, le consentement des parties est pauvrement constaté risque d'être peu efficace juridiquement — il faut attentivement examiner la relation entre signature électronique et engagement moral. [3] Cette question de la *mise en scène* de l'acte authentique a été peu discutée et pourtant, elle semble névralgique. [4] Comme l'a récemment fait remarquer Me Lambert, la mise en scène de l'acte authentique doit permette d'exprimer l'autorité de l'État qui est délégué à l'officier public et qui, en droit français au moins, garantit l'authenticité. Cette question d'apparence secondaire va, en fait, au cœur du problème de la relation entre technologies et institutions en sécurité informatique. L'ergonomie des procédés de sécurité informatique commence à provoquer de plus en plus d'intérêt au sein de la communauté scientifique : certaines études ont suggéré que 95% des atteintes à la sécurité étaient le fait d'erreurs de configuration dues à la pauvreté des interfaces. [5]

---

3. C'est-à-dire que d'appuyer sur un bouton de souris n'a pas la même force d'*expression du consentement et de solennité* que la signature manuscrite.

4. Comme le souligne Pierre LEGENDRE : « *Faire tenir ce que nous appelons l'État exige les grands moyens théâtraux, et l'Occident rationaliste ne déroge pas à l'expérience de l'humanité en matière d'institutions : il faut y croire, comme on croit à sa propre image. À propos des constructions, les architectes antiques parlaient de fermeté (firmitas), au sens où un bâtiment non seulement doit tenir debout selon les lois de la physique, mais aussi doit avoir l'air de tenir debout; il a la force d'une image. Il en est ainsi de l'État : ce sont les rites qui le font exister pour en faire une image au regard des croyants que nous sommes. ... Il faut de la colle pour que tienne un État. Il faut les ancêtres, les images nostalgiques et tout le saint-frusquin des mises en scène ; ça passe par les liturgies politiques, par l'architecture des lieux, par toutes les formes d'écriture nécessaires à la ritualisation du pouvoir.* » Pierre LEGENDRE, *Miroir d'un nation — l'École nationale d'administration*, Milles et une nuits, 2000.

5. Bien que la littérature soit encore assez mince, plusieurs études commencent à soulever les préjugés anti-utilisateurs qui sous-tendent souvent les procédés de sécurité informatique : on tente de domestiquer l'usager à utiliser un procédé qui va contre son entendement, et lorsque celui-ci se réticent, on le décrit comme "le maillon faible", "l'incompétent", de la chaîne. Voir, par exemple, Anne Adams et Martina Angella Sasse, "Users are not the ennemy: Why users compromise security mechanisms and how to take remedial measures". *Communications of the ACM* **42**:(12), p. 40-46 ; Alma Whitten and J.D. Tygar, "Usability of security: A case study", Carnegie Mellon University Technical Report, décembre 1999.

RAPPORTS PARTICULIERS

A. CONTRIBUTIONS

DES PROFESSIONS JURIDIQUES

1. La dématérialisation des actes notariés

-Note remise par le Conseil supérieur du notariat-

NOTE DU CONSEIL SUPERIEUR DU NOTARIAT SUR LA DÉMATÉRIALISATION DES ACTES NOTARIES

Dans sa lettre de mission du 31 mars 2000, Madame la Directrice des Affaires Civiles et du Sceau exposait dans les termes suivants, les questions sur lesquelles le groupe de travail sur la dématérialisation des actes était invité à réfléchir et à proposer des solutions :

« Le groupe de travail pourrait, me semble-t-il, être investi d'une double mission de réflexion et de propositions.

Il pourrait avoir pour mission de rechercher les conditions d'un nouveau formalisme électronique venant se substituer aux actuelles exigences liées au support-papier.

Outre les réflexions particulières qui devraient être menées pour chaque catégorie d'actes (jugements, actes de l'état-civil, actes notariés), le groupe pourrait mener une réflexion générale visant à répondre notamment aux questions suivantes :

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 ?

2 – dans quelles conditions et suivant quelles modalités pourra être apposée la signature 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 ?

Après avoir mené ces réflexions, il pourrait émettre des propositions de mesures, nécessaires à la réalisation de la dématérialisation des actes authentiques, et ce dans la perspective de l'élaboration du ou des décrets d'application prévus par la loi. »

Avant de présenter les réflexions et propositions du notariat qui seront bien entendu centrées sur l'acte notarié, il a paru utile de dresser un panorama général des actes authentiques, dans le but de dégager leurs traits communs et ainsi de mieux cerner la notion d'authenticité.

I – CONSIDÉRATIONS PRÉALABLES SUR LES ACTES AUTHENTIQUES EN GÉNÉRAL

A – La diversité des actes authentiques

Mis à part les actes à caractère législatif, qui ne présentent qu'un intérêt secondaire sur le terrain de la preuve, on distingue classiquement, en fonction de leur objet, trois catégories d'actes authentiques (voir notamment D. MONTOUX, J. Cl. Not. Form. Acte notarié Fasc. A5) :

- ✓ les actes à caractère administratif ;
- ✓ les actes judiciaires et extrajudiciaires ;
- ✓ les actes de juridiction volontaire.

1) Les actes à caractère administratif

Les actes dressés par un fonctionnaire compétent dans les limites de ses attributions et dans l'étendue de son ressort ont, de manière générale, le caractère authentique. Il en est ainsi, notamment, des actes publics dressés par les préfets, sous-préfets, maires et adjoints, dans l'exercice de leurs fonctions.

Sont, par suite, assimilés aux actes authentiques les actes de gestion passés dans la forme administrative ; l'article L. 76 du Code du domaine de l'Etat dispose en effet que *« les préfets reçoivent les actes intéressant le domaine privé immobilier de l'Etat, confèrent à ces actes l'authenticité et en assurent la conservation »*. L'art. 98 III de la loi modifiée du 2 mars 1982 confère ce même pouvoir aux maires, présidents de conseils généraux et régionaux pour les actes intéressant les collectivités locales.

En ce qui concerne l'état-civil, les actes consignés dans les registres de l'état-civil sont également des actes authentiques.

Les actes et documents établis par le directeur de l'office français de protection des réfugiés et apatrides ont aussi le caractère d'actes authentiques. *(Cf. L. n. 52-893, 25 juill. 1952, art. 4, al. 2 in fine).*

2) Les actes judiciaires et extrajudiciaires

Les actes judiciaires dressés par les juges dans l'exercice de leur fonction ont naturellement un caractère authentique. Spécialement, les jugements, de quelque juridiction qu'ils émanent, « ont la force probante des actes authentiques » *(Nouveau C. proc. Civ., art. 457).*

Les rapports d'expertise établis en vertu d'une délégation de justice sont des actes authentiques et font foi jusqu'à inscription de faux des constatations personnelles que l'expert a effectuées dans les limites de sa compétence.

Les actes dressés par les greffiers, dans les limites de leurs attributions, sont également des actes authentiques.

Enfin les actes des huissiers faits en vertu d'une délégation de la loi ont le caractère authentique et font foi jusqu'à inscription de faux. Il en est ainsi des exploits qu'ils délivrent. Mais lorsque l'huissier a fait des constatations distinctes, celles-ci n'ont la valeur que de simples renseignements et n'ont aucun caractère d'authenticité, que le constat ait été dressé à la requête d'un particulier, ou que l'huissier ait été commis par décision de justice.
Il a été jugé aussi que faute de compétence, les actes d'huissiers constatant l'existence d'une convention (qui aurait dû être notariée) sont dépourvus d'authenticité *(Cass. Civ. 1ère - 19.2.1991).*

3) Les actes de juridiction volontaire

Ce sont ceux qui, sur l'initiative des parties, sont dressés par un officier public compétent pour constater un acte ou un fait juridique. Parmi ces actes, les actes notariés occupent une place de premier plan, en raison du monopole dont bénéficient les notaires pour recevoir tous les actes et contrats auxquels les parties doivent ou veulent donner le caractère d'authenticité attaché aux actes de l'autorité publique *(Cf. art. 1er Ord. 2.11.1945).*

Les agents diplomatiques et consulaires exerçant les attributions notariales ont qualité, à l'étranger, pour établir les actes authentiques *(D. 7.2.1991).*

Enfin, il est des actes pour lesquels le notaire partage la faculté de conférer l'authenticité avec d'autres officiers ministériels (c'est le cas pour certaines formes de testaments), ou des fonctionnaires (pour les actes intéressant les collectivités publiques).

B – LES CARACTÈRES COMMUNS DES ACTES AUTHENTIQUES

La définition de l'acte authentique est donnée par l'art. 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 ».*
A partir de cet article et des articles suivants du Code civil ainsi que des textes d'application, cinq traits communs aux actes authentiques peuvent être dégagés :

- l'établissement par une autorité publique,
- l'importance des formalités,
- la signature par l'autorité publique,
- l'exigence d'une conservation quasi-illimitée,
- la puissance des effets juridiques.

1. **L'acte authentique est établi par une autorité publique :**
Cette autorité peut être un officier public au sens de l'art. 1317 (notaire, officier de l'état-civil, greffier des tribunaux de commerce), mais aussi un magistrat ou un fonctionnaire (greffier des tribunaux, préfets et maires pour les actes intéressant l'Etat ou les collectivités locales).

2. **L'acte authentique est entouré de formalités** (les « solennités ») :
Pour l'acte sous seing privé, la loi n'exige qu'une formalité : la signature des parties. Pour l'acte authentique, la loi est plus contraignante et plus méticuleuse :

   a. Au premier rang des solennités figure « la réception » pour les actes notariés (art. 1er de l'Ordonnance du 2.11.1945 : « les notaires sont les officiers publics établis pour **recevoir** tous les actes et contrats… ») ou les actes d'état-civil, (art. 34 du Code civil : « les actes d'état-civil énonceront les année, jour et heure où ils seront **reçus**… »), ainsi que le prononcé pour les jugements (art. 452 NCPC : « le jugement est **prononcé** par l'un des juges qui l'ont rendu… »).
   La réception (de même que le prononcé) implique la présence physique et personnelle de l'officier public. La mission de ce dernier est d'être témoin : le notaire est témoin de l'échange de consentement comme l'officier d'état-civil est témoin de la déclaration des parties. L'officier public est investi d'une mission de service public, celle de rapporter la preuve de l'événement auquel il assiste ou participe. C'est lui seul qui est investi personnellement de la confiance de l'Etat pour assurer cette mission.

   Avec le temps, ce principe de réception personnelle a subi quelques aménagements : depuis 1954, le maire peut déléguer à ses agents communaux le droit de recevoir des déclarations de naissance et de décès et de délivrer des actes de l'état-civil ; depuis 1971, le notaire peut habiliter des clercs à recevoir les parties et à recueillir leur signature (pour certains contrats).

   On peut néanmoins considérer que la condition de réception, même aménagée, demeure la condition première de l'authenticité. Elle implique donc, lors de l'établissement d'un acte sur support électronique, la présence physique de l'officier public. On voit tout de suite la difficulté avec les actes notariés, puisque l'une des caractéristiques du support électronique est de permettre les échanges à distance.

Il est bien évident que le notaire, en raison de la distance, ne pourra être présent avec les parties signataires lorsqu'elles interviendront sur le réseau électronique alors qu'elles sont éloignées géographiquement ; ou, s'il est présent avec l'une, il ne l'est pas avec l'autre. Une solution sera d'admettre que des notaires différents soient placés à chaque extrémité de la chaîne et recueillent, sur des actes séparés, le consentement des parties. Ainsi, l'exigence de la présence physique du notaire témoin sera préservée.

b. Les autres formalités nécessaires à l'acte authentique sont plus contingentes : ce sont les prescriptions purement matérielles de rédaction, comme par exemple : les mentions obligatoires des nom, prénom, domicile des parties, l'inscription des dates en lettres, l'approbation des ratures et des renvois, etc.
Toutes ces formalités sont précisées dans des décrets, notamment le Déc. n°71-941 du 26.11.1971 pour les actes notariés et le Déc. du 3.8.1962 pour les actes de l'état-civil. Parmi les prescriptions, certaines visent directement le support papier (par exemple art. 7 al. 1er du Déc. du 26.11.1971), d'autres y renvoient indirectement, compte tenu des formalités exigées (c'est le cas pour les actes d'état-civil inscrits sur un registre, lui-même tenu en double).

c. Par-delà les « solennités », il faut souligner l'importance de la solennité elle-même : les rites de recueil des déclarations et signatures, l'exigence de la « lecture » de l'acte (Article 38 du Code civil : « L'officier d'état-civil donnera lecture des actes... » ; Article 7 du décret du 26 novembre 1971 : « L'acte porte mention qu'il a été lu par les parties, ou que lecture leur en a été donnée »), la présence de témoins contribuent à une mise en scène de l'événement qu'il s'agit de relater par écrit. Cette mise en scène renforcée par le caractère public de l'autorité qui officie et de ses attributs (sceau, écharpe tricolore du maire, robe du magistrat...) ont pour but d'attirer l'attention des parties sur la gravité de leur engagement et de mieux marquer les mémoires.
L'utilisation du réseau électronique risque t-elle de banaliser la signature des actes ? Ce risque est justement évité par la présence de l'officier public.

3. **L'acte authentique est signé par l'autorité publique qui l'a établi :**
Cette signature pourrait figurer parmi les formalités nécessaires décrites ci-dessus. Mais, participant à la substance-même de l'authenticité, cette solennité mérite d'être distinguée pour deux raisons :

   a. Les textes, par leur insistance, montrent bien l'importance de la signature :
   - l'article 11 du décret du 26.11.1971 vise par deux fois la signature : *« les actes sont **signés** par les parties, les témoins et le notaire (1er alinéa)...Il est fait mention, à la fin de l'acte, de la **signature** des parties, des témoins, du notaire et, s'il y a lieu, du clerc habilité ».*
   - *le jugement est **signé** (art. 456 NCPC).*
   - *l'officier d'état-civil **signe** l'acte d'état-civil (art. 39 du Code civil)*
   Par ailleurs, l'absence de la signature est sanctionnée par la nullité de l'acte. La Cour de Cassation a eu l'occasion de préciser que « la nullité d'un acte authentique pour défaut de signature du notaire est une nullité absolue qui se trouve soumise non pas à la prescription quinquennale de l'Article 1304 du Code civil, mais la prescription trentenaire » (Civ 1ère 29.11.1989 Rép. Def 1990 Article 3480)

b. Cette importance de la signature est confirmée par la loi du 13.3.2000 qui, dans le dernier alinéa du nouvel article 1316-4 qui définit la signature, prend soin de préciser : *« Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte ».*

4. L'acte **authentique est conservé de manière quasi-illimitée :**
   - Le notaire est tenu par la loi non seulement de recevoir tous les actes, mais aussi « d'en conserver le dépôt » (article 1er de l'ordonnance du 2 novembre 1945).
   - Les greffiers ont pour mission de conserver les documents de la juridiction.
   - « Les actes de l'état-civil sont inscrits sur un ou plusieurs registres tenus en double » (article 1er du décret du 3 août 1962), dont la conservation est minutieusement réglementée.

5. **Les effets principaux de l'acte authentique sont les mêmes pour tous les actes :** Ils sont au nombre de trois : force probante (art. 1319 du Code civil), date certaine, force exécutoire.
   A ces effets juridiques, on pourrait ajouter la pérennité et la facilité de duplication.

C – Rappel terminologique : certification et authentification

Les mots ont un sens juridique précis. Or, une confusion existe dans leur utilisation par la technique, confusion encore aggravée avec l'introduction des technologies informatiques. Notamment, le vocable « authentification » est ambigu car il a été abusivement utilisé en pratique comme une traduction du terme anglais « authentication » ; l'« authentification » se limite alors à l'identification d'une signature électronique et aux moyens mis en œuvre pour y parvenir. En matière juridique, l'authentification a un tout autre sens.

Une clarification est donc nécessaire :

- **Certifier** est « assurer qu'une chose est certaine » (Littré), « attester, affirmer, confirmer, garantir qu'une chose est vraie » (Robert).

  Un certificat est « un document écrit qui atteste un fait, un écrit émanant d'une autorité compétente » (Robert).

- **La certification** est une technique de contrôle, de vérification qui est de plus en plus utilisée. Le code de la consommation l'a faite entrer dans notre droit positif (section 4, « certification des services et des produits autres qu'alimentaires »). Son article L 115-27 (loi du 3 janvier 1994) en donne la définition suivante : *« Constitue une certification de produit ou de service... l'activité par laquelle un organisme, distinct du fabricant, de l'importateur, du vendeur ou du prestataire, atteste, à la demande de celui-ci, qu'un produit ou un service est conforme à des caractéristiques décrites dans un référentiel et faisant l'objet de contrôles ».*

  La certification de signature est la simple reconnaissance matérielle de cette signature.

- **La légalisation de signature** est l'attestation écrite par une autorité publique de l'exactitude de la signature apposée sur un document. C'est une formalité administrative qui comporte à la fois la reconnaissance matérielle de la signature, mais également, l'attestation de l'identité et de la qualité du signataire.
  Toutefois, la légalisation ne porte jamais sur le contenu de l'acte sur lequel est apposée la signature légalisée.

- **L'authentification** est l'opération visant à conférer l'authenticité à un acte. Elle implique la vérification par l'officier public de l'identité des parties, du consentement des parties et de la légalité de l'acte avant l'apposition de sa signature.

L'authenticité :

*« Etymologiquement, l'adjectif authentique provient de deux mots grecs ; c'est un composé de "auto" et de "hentés" qui réalise, achève ; d'où la définition du Littré, "qui agit par soi-même". Et c'est bien cette idée que traduit la définition que donne de l'acte authentique le 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" (Tome 6 **V° Notaire-Notariat. p. 2912-70. n° 2).*

L'acte authentique est un acte qui se suffit à lui-même, un acte complet, à raison de ces deux bienfaits que confère la vertu de l'authenticité : la force probante et la force exécutoire. » (Professeur OLIVIER Colloque ARNU 1992 « La modernité de l'authenticité »).

Il est intéressant de relever que Mme de la PRESLE, dans une étude sur la signature électronique (Rapport 1998 sur la nouvelle donne du commerce électronique Mission LORENTZ), soulignait également le besoin de clarification :

« L'essentiel est bien de distinguer le volet juridique de la signature (identification consentement, intégrité du message signé) de son volet technique (description des moyens mis en œuvre pour atteindre, autant que faire se peut, les finalités précédentes). Dans toute la mesure du possible, il faut se rappeler que le terme « authentification » ne recouvre pas le terme anglais « authentication », car la signification technique (identification d'objet) ne recouvre pas la signification juridique (identification de personne en vue de la délivrance d'un « acte authentique »).

...

La certification peut se définir de façon abstraite par l'attribution sûre d'« identités électroniques ». Dans la mise en œuvre de la signature électronique et l'identité réelle, en garantissant l'appariement entre une clé et l'identité de son possesseur. La forme technique ce cet appariement s'appelle un certificat. Les certificats peuvent être de plusieurs types : simple identité, ou identité avec attributs (habilitation à signer dépendante de diverses vérifications). »

II – LES CONDITIONS DU FORMALISME ÉLECTRONIQUE, RELATIVEMENT AUX ACTES NOTARIÉS

Le nouvel alinéa 2 de l'article 1317 du Code civil précise que l'acte authentique peut être dressé sur support électronique, s'il est établi et conservé dans des conditions fixées par décret en Conseil d'Etat. Seront donc examinées tour à tour les conditions d'établissement et de conservation puis, pour répondre au point IV de la lettre de mission, les conditions de délivrance des copies des actes authentiques dématérialisés et la force probante de ces copies.

D'ores et déjà, l'acte notarié électronique est technologiquement réalisable. Le notariat s'est doté d'un réseau sécurisé qui le permet.

C'est en 1998 que le notariat a commencé la mise en place d'un réseau Intranet sécurisé et d'un service d'émission de cartes à puce destinées à l'ensemble des notaires de France. Cette carte, baptisée Réal, permet l'identification des signataires dans le cadre d'échanges de documents électroniques.

L'objectif du réseau R.E.AL. est d'abord de permettre une communication en temps réel entre tous les notaires, et ensuite un accès direct à un certain nombre de fichiers de la profession : registre des testaments, CRIDON, fichiers de référence de valeurs immobilières ; dans un troisième temps, il doit permettre l'accès aux services administratifs : cadastre, registre du commerce, services de l'état-civil, enfin et surtout bureaux des hypothèques.

La mise en place de ce réseau est un succès puisque, à l'heure actuelle, plus des 2/3 des études sont abonnées (exactement au 1er décembre 2000, 4 532 notaires sur 7 700). La moitié des notaires ont commandé leur carte REAL.

A terme, cette carte est destinée à servir de support à la signature électronique du notaire.

A. LES CONDITIONS D'ÉTABLISSEMENT DE L'ACTE NOTARIÉ ÉLECTRONIQUE
(réponse aux points 1 et 2 de la lettre de mission)

1°) 1ère **étape : l'élaboration :** il n'y a pas de difficultés à ce stade. Le support est aujourd'hui déjà électronique, puisqu'il s'agit de traitement de texte.

Faut-il normaliser la saisie ?

La normalisation semble effectivement souhaitable, ne serait-ce que pour maintenir une certaine unité à tous les actes notariés dressés sur support électronique. Il reviendrait à un arrêté ministériel de définir les normes d'encodage à utiliser.

2°) 2ème **étape : le recueil des consentements :** Deux hypothèses sont à distinguer :

a) – soit les parties sont toutes présentes au rendez-vous de signature dans le bureau du notaire : leur contrat peut alors être établi sur le support papier ou sur le support électronique selon leur souhait.

En effet, alors même que le rendez-vous se passe chez le notaire, le support électronique peut se révéler plus pratique : il permet des gains de temps, car il circule plus facilement ; le notaire peut avoir aussi besoin d'annexer à son acte des pièces ou documents qui lui sont arrivés sous forme électronique. (Ce cas sera de plus en plus fréquent avec la dématérialisation des documents administratifs ou fiscaux).
Enfin, il y a tous les actes unilatéraux pour lesquels la notion de distance ne joue pas forcément, sans oublier les actes que le notaire établit sous sa seule signature.

b) Soit, deuxième hypothèse, les parties ne sont pas situées géographiquement au même endroit et elles souhaitent exprimer leur consentement sur un support électronique. L'exigence de la présence physique de l'officier public les conduit à se rendre chez un notaire qui n'est pas le notaire instrumentaire. Deux techniques sont envisageables, en l'état actuel de la réflexion :

- la technique classique du mandat. Le consentement est alors recueilli au moyen d'une procuration authentique reçue par le notaire en second et transmise au notaire instrumentaire grâce au réseau sécurisé. La copie authentique électronique de cette procuration est annexée à la minute électronique de l'acte, qui est ainsi scellé technologiquement et juridiquement.

- la technique de la pollicitation : le notaire en second rédige un acte contenant l'engagement du cocontractant présent devant lui. Cet engagement est définitif, mais il peut être assorti d'un certain délai. A l'autre extrémité, chez le notaire instrumentaire, l'autre cocontractant signera un acte d'acceptation ou d'acquiescement. La rencontre des volontés est opérée et le contrat est noué.

Ces techniques sont conformes aux principes de l'authenticité. Elles peuvent paraître introduire une certaine complexité ; on leur reprochera de scinder les étapes du consentement par des actes séparés et de ne pas utiliser les facilités procurées par le réseau électronique.

Toutefois, elles évitent les risques d'altération qui peuvent survenir sur le réseau et présentent l'avantage de constituer la preuve immédiate de l'engagement : une fois que le cocontractant a signé soit une procuration, soit une pollicitation, le notaire rédacteur peut en tirer immédiatement une copie. D'abord, cela rassure le client qui peut voir sur la copie ce qu'il vient de signer. Ensuite, comme cette copie est authentique, elle servira facilement à prouver le contenu de l'engagement du cocontractant.

3°) **Dernière étape : les signatures :**

- La signature des parties :

Il n'est pas nécessaire que ce soit une signature électronique au sens de la loi du 13 mars 2000. En effet, s'agissant d'un acte authentique, le notaire qui le reçoit est présent et naturellement en mesure de vérifier l'identité du signataire et la réalité de son consentement. En outre, c'est lui, le notaire, qui va garantir l'intégrité de son acte, le lien entre la personne signataire et l'acte qu'elle signe.

La signature des parties pourra donc être recueillie par tous moyens appropriés (tablette graphique, écran tactile, ou autres).

- La signature du notaire :

Il s'agit de sa signature électronique. Les caractéristiques du procédé de signature que le notaire va utiliser doivent être conformes à l'article 1316-4 qui prévoit : *« la fiabilité de ce procédé est présumée jusqu'à preuve 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. »*

A ce niveau d'élaboration de la réglementation, deux points peuvent poser problème :

- On peut noter une sorte de contradiction interne entre la fiabilité de la signature électronique du notaire qui « serait présumée jusqu'à preuve contraire... » et la nature de l'acte authentique qui, par définition, fait « pleine foi jusqu'à inscription en faux ».
- Par ailleurs, cette fiabilité va résulter de l'utilisation d'un certificat électronique lui-même délivré par un prestataire de services de certification. Tout ceci va être organisé par le décret. Mais déjà une question se pose :

Ce prestataire peut-il être un des opérateurs accrédités qui vont intervenir sur le marché ? Cela paraît peu conciliable avec le statut du notaire qui est officier public et qui délivre l'authenticité au nom de la République et sous le sceau de l'Etat. Il paraît donc invraisemblable de faire certifier sa signature par un opérateur privé. Il faudra imaginer le recours à un opérateur public ou un système d'autocertification au sein de la profession.

B. LES CONDITIONS DE CONSERVATION ET ARCHIVAGE DE L'ACTE NOTARIÉ ÉLECTRONIQUE

La durée de conservation de ses minutes a été fixée pour le notaire à 100 ans (article 17, décret du 3 décembre 1979). Au-delà, il doit les verser aux Archives départementales.

Jusqu'à présent, le support d'archivage des actes a été le papier. Désormais, il peut être aussi le support électronique dès lors qu'il lui suffit de répondre aux exigences d'intégrité et d'imputabilité énoncées par la loi du 13 mars 2000. Il est vraisemblable que les deux supports vont coexister pendant longtemps, mais également que le support électronique prendra de plus en plus d'importance à l'avenir.

Une précaution peut sembler utile au moins dans les premiers temps d'application du nouveau système : celle de procéder à un tirage papier de l'acte que le notaire certifierait conforme et conserverait au rang de ses minutes.

Un autre problème va aussi se poser : peut-on imaginer que les 7 700 notaires de France se dotent chacun d'un système informatisé de conservation de leurs actes ?

Avec les progrès de l'informatique, l'archivage est devenu une fonction de plus en plus technique, d'autant plus technique qu'il faut prévoir, sur une longue durée, des processus de resignature à intervalles réguliers, sans parler de la restitution intégrale à tout moment. Il sera sans doute souhaitable de mettre en commun, à l'échelon régional, voire même national, les moyens et les systèmes de stockage et de reproduction. Des raisons financières plaident aussi en faveur d'une solution collective, la maintenance technologique pouvant représenter un coût important.

Le notariat autrichien s'est lancé dans cette voie depuis le 1er janvier 2000 avec la constitution du système CYBERDOC, qui est une sorte de minutier électronique centralisé de tous les notaires autrichiens. Le Conseil Supérieur du Notariat autrichien a été chargé de « créer, gérer, diriger et surveiller les archives des actes du notariat autrichien » (art 1er Directives du 23 novembre 1999 UAR 2000).

Il sera utile que les procédés technologiques et les procédures qui seront adoptés pour l'archivage des actes électroniques soient établis en concertation avec la Direction des Archives de France puisque ces actes sont transférés dans les services départementaux ou nationaux des Archives au bout de 100 ans.

Mais il paraît essentiel que le notariat garde la maîtrise des instruments technologiques qui assureront à la fois le stockage, la conservation et la restitution des actes.

Il paraît également essentiel que le système actuel qui confie aux notaires la responsabilité de la garde de leurs actes sur de très longs délais soit maintenu. 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 signé ainsi que le contenu des contrats qu'ils ont fait constater ou des faits qu'ils ont révélé.

Cette sécurité a un corollaire, s'agissant d'actes conclus 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. Cette règle fondamentale de secret professionnel est ancienne. Elle a été fixée par l'ordonnance de Villers-Cotterêts de 1539 et elle figure actuellement dans des termes inchangés sous l'article 23 de la loi du 25 Ventôse an XI.

Cette obligation au secret est en outre renforcée par les dispositions légales (art. 6 du Code civil) et supra légales (art. 8 Convention Européenne des Droits de l'Homme) qui protègent l'intimité des personnes et le respect de la vie privée.

Il est vrai que les minutes des actes notariés sont expressement considérées comme des « archives publiques » (art. 3 loi du 3 janvier 1979). Cette qualité qui leur était reconnue en pratique depuis bien longtemps, se justifie par le fait *« que le notaire est un officier public investi par l'Etat et que la conservation de leurs actes est d'intérêt public pour la sécurité des transactions et des preuves »* (Jean Favier). Mais elle n'a jamais impliqué le dessaisissement du notaire qui a rédigé les actes et encore moins son dessaisissement immédiat juste après leur signature. Il n'y a aucune raison pour que l'utilisation du support électronique vienne modifier cette règle.

S'agissant des actes notariés, il ne serait 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.

C. LES CONDITIONS DE DÉLIVRANCE DES COPIES

L'article 1335 du Code civil stipule que les *« grosses ou premières expéditions font la même foi que l'original »*. L'article 17 du décret 71-941 du 26.11.1971 prévoit que *« le droit de délivrer des copies exécutoires et expéditions appartient au notaire détenteur de la minute ou des documents qui lui ont été déposés pour minute »*.

Les copies délivrées par le notaire ont donc même force probante que la minute dès lors qu'elles sont certifiées conformes à la minute, soit par lui-même, soit par son successeur ou l'officier public dépositaire de la minute.

C'est un des avantages de l'authenticité d'attacher la force probante aux copies délivrées par les officiers publics. La nouvelle loi ne change rien à la règle et ce qui est valable pour les actes sur support papier doit être étendu aux actes sur support électronique. Il suffit d'adapter sur ce point l'article 15 actuel du décret du 26.11.1971 qui a été uniquement prévu pour le support papier.

III – PROPOSITION DE RÉFORME DU DÉCRET 71-941 DU 26.11.1971 RELATIF AUX ACTES ÉTABLIS PAR LES NOTAIRES

Il n'existe pas de texte commun aux actes authentiques en général, en dehors des articles 1317 et suivants du Code civil. Chaque catégorie d'acte authentique fait, en revanche, l'objet de dispositions spécifiques. Il semble difficile d'élaborer un texte nouveau traitant de tous les actes authentiques et plus pragmatique de procéder aux adaptations nécessaires de chacun des textes les régissant respectivement.

Au surplus, un tel texte précisant la notion d'authenticité et les conditions générales de sa délivrance relèverait plus du domaine législatif que du domaine réglementaire.

Enfin la loi du 13 mars 2000 n'a pas eu pour objet de modifier les règles de l'authenticité mais de poser le principe de l'équivalence pour l'admission en preuve de l'écrit sous forme électronique et de l'écrit sur support papier. Dans la rédaction de ses décrets d'application, il s'agit seulement de transposer au support électronique les règles actuelles de l'acte authentique sur papier.

C'est le décret n° 71-941 du 26 novembre 1971 sur « la forme des actes notariés » qui traite des conditions de rédaction et de présentation propres aux actes notariés. Ces conditions sont liées pour certaines au support papier. Le notariat propose de transposer ces conditions au support électronique et a élaboré dans ce but un avant-projet de réforme de ce décret qui a été soumis au sous-groupe de travail constitué pour les actes notariés et adopté par lui dans sa réunion du 15 septembre 2000(*).

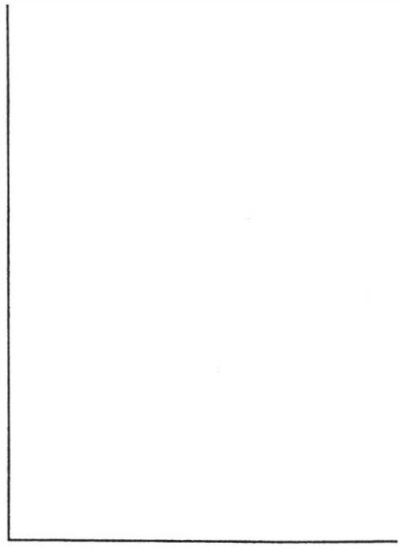
Ci-joint, cet avant-projet présentant sur la première colonne le texte actuel du décret et sur la deuxième colonne, les modifications proposées.

Le 23 Février 2001

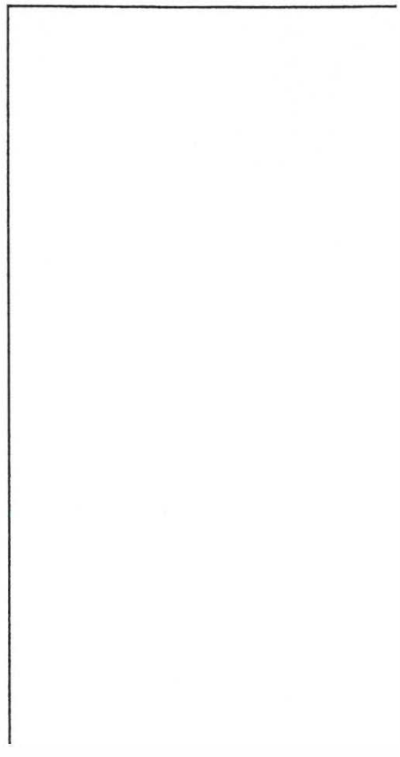
Jacques MOTEL
Président du Conseil Supérieur du Notariat

(*) Lors de cette réunion, le sous-groupe de travail était composé de :

- Pierre CATALA, Professeur de droit à l'Université de Parie II,
- Isabelle de LAMBERTERIE, Directrice de recherche au CNRS,
- Michel VIVANT, Professeur,
- Alain LAMBERT, Président Honoraire du CSN,
- Jean-Pierre DELPEUCH, Directeur des Affaires Juridiques au CSN,
- Jean-Dominique MATHIAS, Administrateur du Département de la Réglementation et de l'Ethique Notariale au CSN,
- Jean-François BLANCHETTE, CECOJI - CNRS.



2. Notes sur l'état civil



a) Les actes d'état civil face à la dématérialisation des actes authentiques : état des lieux concernant les règles de l'Instruction générale relative à l'état civil et les pratiques administratives en vigueur.

-Note rédigée par M. Jean-Luc IFFRIG-

Jean-Luc IFFRIG
Directeur du Service Population-Accueil et Mairies de quartier
Mairie de Strasbourg
✆: 03.88.60.97.53

Les actes d'état civil face à la dématérialisation des actes authentiques : état des lieux concernant les règles de l'Instruction générale relative à l'état civil et les pratiques administratives en vigueur.

(1ère étape d'une réflexion menée dans le cadre du groupe de travail sur la dématérialisation des actes authentiques, coordonné par la Mission de Recherche Droit et Justice).

- Ont participé à ce sous-groupe de travail :

  - Madame Isabelle GUYON-RENARD, Conseiller juridique au Service Central de l'Etat civil du Ministère des Affaires Etrangères à Nantes,
  - Monsieur Jean-Claude BLOCH, Directeur du Service des Formalités Administratives de la ville de Besançon,
  - Monsieur Jean-Michel BRUNTZ, Avocat général près de la Cour d'Appel de Paris,
  - Monsieur Denis HUBERT, Procureur adjoint de la République près le T.G.I. de Nantes,
  - Monsieur Jean-Luc IFFRIG, Directeur du service Population de la Ville de Strasbourg.

L'ETABLISSEMENT DES ACTES DE L'ETAT CIVIL

I L'établissement d'un acte de naissance

II L'établissement d'un acte de mariage

III L'établissement d'un acte de décès

IV Transcriptions

I - ETABLISSEMENT D'UN ACTE DE NAISSANCE

① Procédure légale et réglementaire d'établissement d'un acte de naissance : règles de l'Instruction générale relative à l'état civil.

1) Règles concernant les déclarations de naissance

- Toute naissance survenue sur le territoire français doit faire l'objet d'une déclaration à l'officier de l'état civil de la commune sur le territoire de laquelle l'enfant est né, alors même que les parents étrangers auraient déclaré cette naissance aux autorités consulaires de leur pays.
  La déclaration peut être reçue soit à la mairie, soit dans les maternités ou cliniques lorsque l'officier d'état civil s'y déplace (n°269).
- Les naissances survenues dans les maternités ou cliniques peuvent être enregistrées sur place. A cet effet, l'officier d'état civil se rend auprès des accouchées, porteur soit du registre des naissances de la mairie, soit de la feuille mobile destinée à recevoir l'acte de l'état civil (n°94).
- l'officier de l'état civil peut également attirer l'attention des personnes concernées sur les sanctions encourues dans le cas de déclarations mensongères
  * Ainsi, lorsqu'il enregistre des faits matériels qui sont portés à sa connaissance en matière de naissance ou de décès, l'officier d'état civil doit s'assurer par lui-même, soit plus généralement par l'intermédiaire d'un médecin.
  * De plus, bien que l'officier d'état civil soit tenu d'inscrire dans l'acte de naissance les prénoms de l'enfant tels que choisis par les parents "lorsque ces prénoms ou l'un d'eux, seul ou associé aux autres prénoms ou au nom, lui paraissent contraires à l'intérêt de l'enfant et au droit des tiers de protéger leur patronyme, l'officier d'état civil en avise sans délai le procureur de la République (article 57 al 3 C.C) (n°12-1).

2) Formalités postérieures à l'établissement de l'acte de naissance

- Lorsque la naissance d'un enfant légitime aura lieu dans une commune autre que celle du domicile des parents, elle sera inscrite sur la table annuelle et la table décennale des actes de la commune du domicile (n°293).
- Obligations de l'officier d'état civil
  * il doit, en principe, recevoir l'acte "à la maison commune" (sauf cas particuliers)
  * il ne doit consigner dans les actes que "ce qui doit être déclaré par les comparants" (art 35 E.C.).
  * Il ne peut dresser d'office un acte de l'état civil. S'il apprend qu'une naissance ou un décès ne lui a pas été déclaré, il en informe le Procureur de la République.
  * L'identité des parties, des déclarants et des témoins étant destinée à figurer parmi les énonciations de l'acte civil, il appartient à l'officier de l'état civil, en raison du caractère authentique attaché à cet acte, d'inviter les personnes concernées à justifier de leur identité afin d'éviter le risque d'erreur dans la rédaction de celui-ci.
  * Il doit donner "lecture des actes aux parties comparantes ou à leur fondé de procuration, et aux témoins", et les inviter "à en prendre directement connaissance avant de les signer" (art 38 C.C.).

A cet effet, l'officier d'état civil qui a reçu l'acte de naissance ou de reconnaissance en avisera dans les trois jours l'officier de l'état civil du lieu du domicile.
L'officier d'état civil adresse également à l'INSEE un bulletin statistique relatif à la naissance (n°94).

3) Rôle de l'officier de l'état civil

* L'officier d'état civil est chargé :
  - de constater les naissances et d'en dresser acte,
  - de recevoir, concurremment avec le notaire, les reconnaissances d'enfants naturels et d'en dresser acte.

↳ Procédure d'établissement d'un acte de naissance

L'officier de l'état civil doit :

* *Enregistrer la déclaration du ou des comparants*
* *Identification des déclarants (les déclarants doivent justifier de leur identité devant l'officier d'état civil).*
* *Donner lecture des actes aux parties comparantes et les inviter à en prendre directement connaissance*
* *Faire signer les comparants*
* *Attirer l'attention des comparants sur les sanctions encourues en cas de déclarations mensongères*
* *S'assurer par lui-même (ou par l'intermédiaire d'un médecin) de la réalité des faits matériels enregistrés.*

② Procédure d'établissement d'un acte de naissance : pratiques administratives en vigueur

- *Etape 1 : établissement du projet d'acte de naissance en liaison avec les services de la maternité*

Dans le cadre des 3 jours légaux, envoi par la maternité, au service de l'état civil, d'un projet de l'acte de naissance.

↳ *vérification par la sage femme de l'identité des parents (livret de famille, acte de reconnaissance anticipée)*
↳ *projet établi par la sage femme sur déclaration du père*
↳ *signature du déclarant*
↳ *signature du médecin*
↳ *signature de la sage femme.*

- *Etape 2 : établissement de l'acte de naissance définitif*

Rédaction de l'acte de l'état civil par l'officier d'état civil et mise à jour du livret de famille
↳ retour à la maternité du livret de famille mis à jour + délivrance d'extraits de naissance

- *Etape 3 : signature de l'acte de naissance par le déclarant (en général la sage femme) qui se déplace en mairie.*

II - ETABLISSEMENT D'UN ACTE DE MARIAGE

① Procédure légale et réglementaire d'établissement d'un acte de mariage : règles de l'Instruction générale relative à l'état civil.

1) Rôle de l'officier d'état civil

* L'officier d'état civil est chargé :
  - de recueillir, concurremment avec le notaire, les consentements à mariage (art 73 C.C.),
  - de célébrer les mariages après avoir fait la publication prescrite par la loi, et d'en dresser acte (art 63,75, 165 C.C.) (n°11).

* L'officier de l'état civil ne peut dresser d'office aucun acte. Dès lors qu'il en est légalement requis, il doit enregistrer les déclarations qui lui sont faites, en conformité à la loi (art 35 C.C.).
  Toutefois, l'ordre public étant intéressé à ce que toute personne soit pourvue d'un état civil régulier, la vigilance de l'officier d'état civil est requise lors de l'établissement de l'acte de l'état civil comme lors de l'apposition de mentions ou de la délivrance de copie ou d'extrait d'actes (n°12).

* Rôle de l'officier de l'état civil au moment de l'établissement de l'acte.
  L'identité des parties, des déclarants et des témoins étant destinée à figurer parmi les énonciations de l'acte de l'état civil, il appartient à l'officier d'état civil, en raison du caractère authentique attaché à cet acte, d'inviter les personnes concernées à justifier de leur identité afin d'éviter le risque d'erreur dans la rédaction de celui-ci.
  Il peut également attirer l'attention des personnes concernées sur les sanctions encourues dans le cas de déclaration mensongère.
  En matière de mariage, l'officier d'état civil doit vérifier que les conditions légales de forme (publications ...) et de fond (vérification de l'intention matrimoniale, vérification de l'absence d'union antérieure non dissoute, absence de lien de parenté constituant un empêchement à mariage, capacité...) sont bien réunies.
  Plus particulièrement "lorsqu'il existe des indices sérieux laissant présumer que le mariage envisagé est susceptible d'être annulé au terme de l'article 146 du présent code, l'officier d'état civil peut saisir le Procureur de la République. Il en informe les intéressés (n°12-1).

* Les attributions des agents communaux délégués par le maire sont limitativement fixées :
Les agents communaux n'ont jamais compétence pour célébrer un mariage et en dresser acte, ni pour établir l'acte authentique de consentement des parents au mariage de leur enfant mineur, ni pour établir les déclarations de reprise de la vie commune enregistrées sur les registres de mariages.
En revanche, les affiches de publication de mariage qui ne sont pas des actes de l'état civil, ainsi que les copies de ces affiches, peuvent être établies et délivrées par tout agent communal, sans qu'une délégation expresse du maire soit nécessaire à cet égard (n°15).

2) Constitution du dossier :

* L'officier d'état civil appelé à célébrer un mariage doit s'assurer que les conditions de fond et de forme, posées par la loi, sont remplies.
Le jour de la célébration est fixé par les parties sous réserve que le dossier de mariage soit complet.
L'officier d'état civil n'a pas à effectuer d'investigations pour s'assurer de la réalité du consentement. En revanche, il doit informer le Procureur de la République de tout élément qui laisserait supposer que le consentement au mariage ne serait pas réel et sérieux, afin de permettre au Ministère Public de surseoir à la célébration et de faire opposition au mariage (n°347).

* Liste des pièces exigées pour constituer le dossier de mariage (n°348 et suivant).

3) Célébration du mariage

- **Lieu de célébration (n° 392 à 395)**

* Le mariage sera célébré dans la commune où l'un des deux aura son domicile ou sa résidence établie par un mois au moins d'habitation continue à la date de publication prévue par la loi (art 74 C.C.) et, en cas de dispense de publication, à la date de dispense prévue à l'article 169 (art 165 C.C.).

* Le mariage doit être célébré à la mairie (art 75 C.C.). Il convient, dans la mesure du possible, qu'une salle spéciale soit réservée à cet effet. Cette règle est sanctionnée par les articles 192 et 193 du C.C..
Des exceptions sont prévues par l'art 75, al2 du C.C.

- **Règles relatives à la célébration (n° 396 à 402)**

* les mariages doivent être célébrés avec le maximum de solennité, l'officier de l'état civil ceint de son écharpe (art R 122-2 du C.C.).
* l'article 146-1 du code civil prévoit que le mariage d'un français requiert sa présence. La comparution personnelle de tout français constitue désormais une condition de fond de l'union matrimoniale ; son absence est sanctionnée par la nullité de l'acte, en application de l'article 184 du code civil
*Le mariage doit être célébré en présence d'au moins deux témoins.

* Lecture des pièces : si les pièces produites par l'un des deux futurs époux ne concordent pas entre elles quant au prénom ou quant à l'orthographe des noms, l'officier d'état civil interpelle celui qu'elles concernent et, s'il est mineur, ses plus proches ascendants présents à la célébration, d'avoir à déclarer que le défaut de concordance résulte d'une omission ou d'une erreur (art 75 C.C.).
* Lecture de certains articles du code civil :
En application de l'art 75 du code civil, l'officier de l'état civil doit donner lecture des articles 212,213, alinéa 1er et 2, 214 alinéa 1er et 215 alinéa 1er du même code.
* Interpellation des parties sur leur régime matrimonial :
L'officier de l'état civil interpellera les futurs époux et, s'ils sont mineurs, leurs ascendants présents à la célébration et autorisant le mariage, d'avoir à déclarer s'il a été fait un contrat de mariage et, dans le cas d'affirmative, la date de ce contrat ainsi que les nom et lieu de résidence du notaire qui l'a reçu (art 75 al 4 C.C.).
Cette interpellation doit avoir lieu même si les futurs époux ont remis à l'officier d'état civil le certificat du notaire constatant qu'un contrat de mariage a été passé.
* Interpellation des futurs conjoints et prononcé de l'union :
L'officier de l'état civil recevra de chaque partie, l'une après l'autre, la déclaration qu'elles veulent se prendre pour mari et femme ; il prononcera, au nom de la loi, qu'elles sont unies par le mariage et il en dressera acte sur-le-champ. L'officier de l'état civil s'adressera d'abord à la future épouse puis, après avoir recueilli le consentement de celle-ci, au futur époux.
* Rédaction et signature de l'acte :
L'acte doit être immédiatement dressé (art 75 in fine C.C.).et signé (art 39 C.C.) sur les deux exemplaires des registres après que les époux en ont eu pris connaissance.
Rien ne s'oppose à ce que l'acte de mariage soit préparé avant la cérémonie.
L'ordre des signatures est le suivant :
Les époux, respectivement sous leur nom respectif, éventuellement les ascendants des époux qui doivent consentir au mariage lorsqu'ils ne l'ont pas fait par écrit antérieurement, les témoins, l'officier de l'état civil.

↳ Procédure d'établissement d'un acte de mariage

Etape 1 : préparation du dossier de mariage

L'officier de l'état civil doit :

** vérifier l'identité des parties déclarantes et des témoins,*
** attirer l'attention des personnes concernées sur les sanctions encourues dans le cas de déclaration mensongère,*
** vérifier l'intention matrimoniale, l'absence d'union antérieure non dissoute, l'absence de lien de parenté constituant un empêchement à mariage, la capacité des parties,.*
** saisir le Procureur de la République s'il existe des indices sérieux laissant présumer que le mariage envisagé est susceptible d'être annulé ou s'il existe des éléments qui laisseraient supposer que le consentement au mariage ne serait pas réel ou sérieux,*
** réunir les pièces exigées pour constituer le dossier de mariage.*
** procéder à la publication des bans au lieu du domicile de chacun des futurs époux et s'assurer qu'aucune opposition n'est survenue*

Etape 2 : célébration de la cérémonie de mariage.

** le mariage doit être célébré avec le maximum de solennité*
** le mariage doit être célébré dans la commune où l'un des deux époux aura son domicile ou sa résidence et dans la mesure du possible, dans une salle spécialement réservée à cet effet.*
** la célébration du mariage requiert la présence des parties et des témoins*
** l'officier de l'état civil doit :*
- interpeller les parties si les pièces produites ne concordent pas
- lecture de l'acte
- donner lecture de certains articles du code civil
- interpeller les parties sur leur régime matrimonial
- recevoir le consentement des parties et prononcer l'union
- rédiger l'acte (possibilité de préparer la rédaction avant la cérémonie) et faire signer les parties et les témoins.

② Procédure d'établissement d'un acte de mariage : pratiques administratives en vigueur

1ère étape : préparation du dossier de mariage par les futurs époux

**1ère rencontre au bureau de l'état civil entre l'officier de l'état civil délégué (fonctionnaire territorial) et les futurs époux. Retrait du dossier par les futurs époux, examen de la liste des pièces à produire par les parties et, le cas échéant, renseignements complémentaires dans l'hypothèse d'un cas particulier lié notamment à la nationalité d'un des futurs époux.(Possibilité d'un retrait du dossier en mairie de quartier).*

** 2ème rencontre entre l'officier de l'état civil délégué et les futurs époux :*
- *vérification par l'officier de l'état civil des pièces produites par les parties*
- *réservation de la date de la cérémonie*
- *mise au point, le cas échéant, de l'organisation de la cérémonie (choix de l'officier de l'état civil célébrant, organisation pratique…)*
- *vérification, le cas échéant, par l'officier de l'état civil, de la réalité et du sérieux du consentement au mariage des futurs époux (difficultés à obtenir les pièces du dossier, comportement des futurs époux…) et éventuelle transmission, en cas de doute, au procureur de la République qui est seul compétent pour surseoir à la célébration*
- *signature du dossier par les futurs époux*

2ème étape : célébration du mariage

** vérification de l'identité des futurs époux et des témoins ainsi que de la concordance entre les pièces produites et le projet d'acte de mariage par l'officier de l'état civil*
** célébration*
** éventuel échange d'alliances*
** signature de l'acte par les parties, les témoins et l'officier de l'état civil*
** remise d'un cadeau souvenir, du livret de famille, des extraits de mariage et de la fiche de célébration.*

3ème étape : formalités postérieures à la célébration

** envoi d'un avis de mention à la commune du lieu de naissance de chaque époux*
** envoi d'un avis de légitimation aux communes du lieu de naissance des enfants à légitimer, s'il y a lieu*
** les différentes pièces du dossier ainsi que le double du registre de mariage font l'objet d'une transmission annuelle au tribunal de grande instance du lieu de célébration.*

III - ETABLISSEMENT D'UN ACTE DE DECES

① Procédure légale et réglementaire d'établissement d'un acte de décès : règles de l'Instruction générale relative à l'état civil.

1) Règles concernant la constatation du décès et l'établissement de l'acte

- Constatation du décès.

  Dans les communes où aucune habilitation particulière n'a été donnée par l'officier d'état civil, tout médecin appelé par la famille est compétent pour établir le certificat médical de décès.

  En revanche, dans les communes où l'officier d'état civil a spécialement désigné "des médecins de l'état civil", ceux ci sont seuls habilités à constater le décès et à établir le certificat médical (n°425).
- Lorsque le décès est établi par l'examen du corps, un acte de décès est dressé par l'officier d'état civil (n° 422)
- Opérations consécutives à la constatation du décès.

  Dans le cadre de ses attributions d'autorité de police administrative, le maire délivre les autorisations de transport de corps sur le territoire français, d'inhumation, de crémation et d'exhumation.

  Pour les transferts de corps à l'étranger, seul le Préfet est compétent. En revanche, en qualité d'officier d'état civil, le maire autorise la fermeture de cercueil, délivre les autorisations de visite au "médecin de l'état civil" qu'il aura préalablement désigné et signe l'acte de décès
  (n° 425).

2) Règles concernant les déclarations de décès.

- L'acte de décès sera dressé par l'officier d'état civil de la commune où le décès a eu lieu, sur la déclaration d'un parent du défunt ou sur celle d'une personne possédant sur son état civil les renseignements les plus exacts et les plus complets qu'il sera possible (art 78 C.C.) (n°423)..
- Les déclarations de décès prévues par l'article 78 du C.C. doivent être faites dans un délai de 24 heures depuis le décès.

  L'acte de décès peut être dressé aussitôt la déclaration effectuée et sans attendre que le certificat médical de décès prévu ait été établi par un médecin.

  Cette manière de faire ne présente, dans la pratique, aucun inconvénient sérieux dès lors que le certificat médical de décès doit être produit pour la délivrance de l'autorisation de fermeture de cercueil.

  Il est souhaitable que l'officier d'état civil rassemble le plus grand nombre possible de renseignements pour éviter la rectification ultérieure de l'acte et invite le déclarant à présenter des pièces d'identité concernant le défunt, telles que le livret de famille, l'acte de naissance et autres (décret du 15 avril 1919).

3) Rôle de l'officier de l'état civil

L'officier de l'état civil est chargé :

- de constater les décès et d'en dresser acte (n°11).
  Rôle de l'officier d'état civil au moment de l'établissement de l'acte.
  L'identité des parties, des déclarants et des témoins étant destinée à figurer parmi les énonciations de l'acte de l'état civil, il appartient à l'officier d'état civil, en raison du caractère authentique attaché à cet acte, d'inviter les personnes concernées à justifier de leur identité afin d'éviter le risque d'erreur dans la rédaction de celui-ci (n°12-1).

↳ Procédure d'établissement d'un acte de décès

L'officier de l'état civil doit :

** Constater le décès sur certificat établi par un médecin*
** Recevoir la déclaration du déclarant après avoir vérifié son identité*
** Inviter le déclarant à présenter des pièces d'identité concernant le défunt*
** Donner lecture de l'acte au déclarant et l'inviter à signer*
** Signer lui-même l'acte.*

② Procédure d'établissement d'un acte de décès : pratiques administratives en vigueur

1ère étape :

- *Cas général*

Dans le cadre du délai légal de 24 heures, rédaction du projet de l'acte de décès par l'officier d'état civil en présence du déclarant (en général, une entreprise de pompes funèbres).

↳ *vérification de l'identité du déclarant*
↳ *présentation, par le déclarant, du certificat de décès signé par un médecin (+ inscription par l'officier d'état civil du n° d'ordre du décès sur le registre des actes d'état civil).*
↳ *présentation par le déclarant d'une pièce d'identité (livret de famille) concernant le défunt.*

- *Cas d'une entreprise de Pompes Funèbres locale*

↳ *dans le cadre du délai légal de 24 heures, l'entreprise locale dépose le projet de l'acte de décès accompagné d'une pièce d'identité du défunt (livret de famille) au bureau des décès.*

2ème étape :

- *Cas général*
  - *rédaction de l'acte de décès par l'officier de l'état civil*
  - *lecture de l'acte de décès au déclarant et signature du déclarant et de l'officier de l'état civil*
  - *mise à jour du livret de famille*
  - *délivrance des autorisations d'inhumation ou crémation ou transport de corps*
  - *délivrance de copies d'acte de décès et le cas échéant de certificats d'hérédité*

- *Cas d'une entreprise locale*
  - *l'entreprise retire au bureau des décès les copies des actes de décès, le livret de famille mis à jour et les autorisations sollicitées.*

LA MISE A JOUR DES REGISTRES DE L'ETAT CIVIL

L'apposition de mentions marginales

L'APPOSITION DE MENTIONS MARGINALES

① Procédure légale et réglementaire concernant les mentions marginales : règles de l'I.G.E.C

1) Définition et nature des mentions

- La mention marginale est une mesure de publicité destinée à établir une relation entre deux actes de l'état civil ou entre un acte et une décision judiciaire ou administrative. Elle consiste en une référence sommaire, en marge de l'acte antérieurement dressé ou transcrit, ou nouvel acte (ou décision judiciaire ou administrative) qui vient modifier ou compléter l'état civil de l'intéressé.
- Seules doivent être portées les mentions prévues par la loi ou ordonnées par décision de justice (n° 218)
- Certains actes reçus ou transcrits par l'officier de l'état civil font l'objet d'une mention en marge d'un acte précédemment dressé ou transcrit. Sont mentionnés :
  - ↳ l'acte de mariage, en marge de l'acte de naissance de chacun des époux (art. 76 C.C.)
  - ↳ l'acte de décès, en marge de l'acte de naissance (art.79 C.C.)
  - ↳ l'acte de reconnaissance d'enfant naturel, y compris anténatal en marge de l'acte de naissance (art. 62 C.C.)
  - ↳ le consentement du majeur au changement de son nom par suite d'une modification de sa filiation (art. 61-3 al. 2 et 331 – 2 C.C.) en marge de son acte de naissance et, le cas échéant, de son acte de mariage, des actes de naissance de son conjoint et des actes de naissance de ses enfants
  - ↳ la déclaration à l'officier de l'état civil de reprise de vie commune par les époux séparés de corps, en marge de l'acte de mariage et des actes de naissance des époux (art. 305 C.C. et art. 1140 N.CP.C).
- D'autres actes et décisions judiciaires ou administratives, bien que non inscrits ou transcrits sur les registres sont néanmoins mentionnés en marge d'un acte précédemment dressé ou transcrit.

  Sont ainsi portées sous forme de :
  - ↳ mentions relatives au lien matrimonial
  - ↳ mentions relatives à la filiation
  - ↳ mentions relatives aux noms et prénoms
  - ↳ mentions relatives à la rectification et à l'annulation

- mentions relatives au répertoire civil
- mentions relatives au régime matrimonial
- mentions spécifiques relatives à la nationalité
- mentions diverses.

Certaines décisions judiciaires préalablement transcrites sur les registres sont également mentionnées en marge d'un acte précédemment dressé ou transcrit.

2) L'avis de mention

- Il y a lieu à l'envoi d'un avis aux fins de mention marginale quand l'officier de l'état civil qui a reçu ou transcrit l'acte (ou la décision) donnant lieu à mention ne détient pas tous les exemplaires des registres où celle-ci doit être apposée (n° 228-1).

- Il convient d'utiliser, pour les avis aux fins de mention marginale, des formules imprimées. Ces formules comporteront un récépissé destiné à être renvoyé à la mairie qui aura expédié l'avis, permettant d'établir que celui-ci est bien parvenu à destination (n° 229).

3) Officiers d'état civil compétents pour apposer les mentions

- L'officier d'état civil compétent est celui qui détient l'acte qui doit être mis à jour en priorité. En principe, il s'agira du lieu de naissance. Par exception, en matière de divorce, il s'agit de l'officier de l'état civil détenteur de l'acte de mariage (n° 230).

4) Manière dont les mentions sont apposées

- Les mentions des actes de l'état civil apposées en marge d'autres actes énoncent la nature, la date et le lieu de l'évènement qui a fait l'objet de l'acte mentionné ainsi que les principales énonciations de celui-ci. Si l'acte n'a pas été établi par l'officier de l'état civil, les mentions comprennent, en outre, le nom, l'adresse et la qualité de l'autorité qui a établi l'acte. Elles énoncent également la date et le lieu de transcription ainsi que les références de l'acte lorsque celui-ci est détenu par le service central d'état civil du ministère des affaires étrangères.
- Les mentions marginales des décisions judiciaires et administratives énoncent la nature, l'objet et la date de la décision ainsi que la désignation de l'autorité dont émane la décision.
- Toute mention marginale énonce en outre le lieu et la date de son apposition ainsi que la qualité de l'officier de l'état civil qui a procédé à la mise à jour ou, lorsqu'elle est manuscrite, signé la mention (art. 71 du décret n° 62-921 du 3 août 1962).
- Les mentions marginales doivent être rédigées avec concision. Il est recommandé de les inscrire en écriture fine et serrée, de manière à laisser la place nécessaire pour l'insertion d'autres mentions. S'agissant des dates, il convient d'inscrire les jours et années en chiffres. Mais les abréviations restent, en principe, interdites, notamment les mois et dates doivent être indiqués en toutes lettres, leur éventuelle inscription en chiffres constituant des abréviations.

S'agissant des lieux, il convient d'inscrire :

* en lettres majuscules ; la commune
* la première lettre en majuscule, les autres en minuscules et le tout entre parenthèses:
  - ↳ le département, le cas échéant le district, l'Etat, le pays
* pour Paris, Marseille et Lyon :
  - ↳ les numéros d'arrondissement.

- Les mentions doivent être apposées suffisamment en retrait de manière à éviter qu'elles ne soient prises dans la reliure.
- Les mentions manuscrites apposées par les fonctionnaires délégués sont revêtues de leur seule signature (n° 237).

5) Délai d'apposition des mentions

- Les mentions marginales doivent être apposées par les officiers de l'état civil dans les trois jours de la réquisition (art. 49 C.C./n° 237-1).

6) Rôle de contrôle des officiers de l'état civil

- L'attention des officiers de l'état civil est appelée sur la nécessité de vérifier soigneusement, lors de l'apposition de la mention, l'identité entre la personne indiquée dans l'avis de mention et celle désignée sur l'acte où la mention doit être apposée.
- L'officier de l'état civil ou le fonctionnaire délégué requis d'apposer une mention en marge d'un acte dressé sur les registres de sa commune ne peut, en principe, s'abstenir d'obtempérer à cette réquisition.
- Toutefois, il peut ne pas ni donner suite, d'une part, s'il y a doute sur le point de savoir en marge de quel acte la mention doit être portée, d'autre part, si la mention contient une énonciation contraire à des indications de l'acte lui-même. En effet, l'officier de l'état civil, qui est gardien de la régularité intrinsèque de ses actes et qui devrait, à ce titre, se refuser à recevoir un acte contenant des indications contradictoires et donc apparemment mensonges, doit s'abstenir d'apposer en marge d'un acte une mention inconciliable avec les énonciations qu'il contient. Il doit surseoir à l'apposition de la mention et solliciter aux fins d'instruction le procureur de la République.
- L'officier de l'état civil doit toujours signaler à l'autorité requérante les lacunes, erreurs ou irrégularités, dont les indications portées dans l'avis de mention reçu seraient entachées (n° 237-3).
- Il importe de vérifier si les avis de mentions sont bien parvenus à leurs destinataires : à cet effet, le maire du lieu où la mention a été portée doit renvoyer au maire expéditeur le récépissé prévu sur l'imprimé d'avis de mention.
  La mention une fois apposée, le récépissé est renvoyé à la mairie expéditrice.
  Quel que soit le procédé employé, l'officier de l'état civil est tenu de conserver une trace des récépissés d'avis de mention pendant dix ans au moins, de vérifier périodiquement si tous les récépissés lui ont été renvoyés et, le cas échéant, de procéder à des rappels.
  Il s'expose, en cas de défaillance, à l'amende prévue à l'article 50 du code civil.
  Par assimilation avec les récépissés, il est recommandé de conserver les avis de mention pendant au moins dix ans.

↳ Procédure d'apposition de mentions en marge d'un acte de l'état civil

- *Règles de base :*

  ** La mention marginale vient modifier ou compléter un acte de l'état civil antérieurement dressé.*
  ** Les mentions marginales peuvent être apposées à la requête du procureur de la République, de l'administration, d'un officier de l'état civil ou des parties à l'acte (ainsi que par l'intermédiaire de leur avocat ou avoué).).*
  ** Un avis de mention est envoyé par l'officier de l'état civil aux mairies ou greffes dépositaires des registres dans lesquels sont contenus les actes de l'état civil concernés par les informations objet de la mention marginale.*
  Un formulaire comportant un accusé de réception est utilisé à cet effet.

- *L'officier de l'état doit :*
  ** envoyer un avis de mention aux communes et greffes concernés*
  ** apposer les mentions marginales dans un délai de trois jours à compter de la réquisition et renvoyer en retour un récépissé à l'autorité expéditrice*
  ** vérifier la cohérence entre l'avis de mention et l'acte concerné.*
  ** refuser l'apposition en cas d'irrégularité et solliciter le procureur de la République*
  ** signaler les erreurs et irrégularité à l'autorité requérante*
  ** revêtir de sa signature les mentions manuscrites qu'il a apposées*
  ** conserver les récépissés d'avis de mention pendant 10 ans au moins et vérifier si tous les récépissés lui ont bien été renvoyés*
  ** conserver les avis de mention envoyés pendant 10 ans au moins.*

② Procédure d'apposition et d'avis de mentions : pratiques administratives en vigueur

- *L'apposition de mentions est réalisée par l' officier de l'état civil délégué, (double opération):*
  - l'apposition manuscrite sur le registre d'une formule pré-établie (apposition d'un tampon) personnalisée, datée et signée de sa main par l'officier de l'état civil délégué.
  - La saisie informatisée de la mention dans le cas où l'acte de base a été informatisé.

- *L'envoi d'un avis de mention est réalisé par l'officier de l'état civil délégué qui a dressé l'acte. Cette opération est réalisée par l'envoi par le courrier postal d'une fiche pré-établie personnalisée, datée et signée par l'officier de l'état civil.*

IV LA TRANSCRIPTION D'ACTES DE L'ETAT CIVIL ET DE DECISIONS JUDICIAIRES

① Procédure légale et réglementaire concernant les transcriptions: règles de l'Instruction générale relative à l'état civil.

1) Définition et nature des transcriptions.

↳ Définition :

- la transcription est l'opération par laquelle un officier de l'état civil reporte sur ses registres un acte de l'état civil reçu ailleurs que dans sa circonscription, ou une décision judiciaire relative à l'état civil.
- Pour certains d'entre eux, la transcription a essentiellement pour but d'assurer une meilleure publicité ; pour les autres, elle vise à remplacer un acte manquant ou à constituer un acte de naissance (n° 207

↳ Transcriptions effectuées dans un intérêt de publicité.

- Transcriptions sur les registres communaux.

Est transcrit sur les registres de la commune du dernier domicile du défunt, l'acte de décès dressé dans une commune autre que celle ou le défunt était domicilié (art. 80 C.C.).

Cette disposition est applicable aux actes de décès dressés au cours d'un voyage maritime ou aux armées.

A la requête du procureur de la République est également transcrit sur les registres des décès du lieu du domicile de l'absent ou de sa dernière résidence, le dispositif du jugement déclaratif d'absence (art. 127 C.C.).

L'acte de reconnaissance d'enfant naturel dressé par un notaire peut être transcrit sur les registres de la commune du lieu où l'acte de naissance a été dressé ou transcrit. Aucun texte n'imposant cette transcription, elle est effectuée uniquement sur demande des intéressés (n° 209).

- Transcriptions sur les registres du service central d'état civil.

L'institution par le décret n° 65-422 du 1er juin 1965 du service central d'état civil rattaché au ministère des affaires étrangères, a permis de centraliser en un lieu unique la plupart des transcriptions prévues dans un but de publicité.

↳ Transcriptions effectuées en vue de remplacer un acte manquant.

Sont transcrits sur les registres de la commune ou l'acte a été dressé ou aurait dû - l'être :

- les jugements ou arrêts déclaratifs de naissance (art. 55 C.C)
- les jugements ou arrêts déclaratifs de mariage lorsque la preuve d'une célébration légale du mariage se trouve acquise par le résultat d'une procédure criminelle (art. 198 C.C.)
- les jugements ou arrêts déclaratifs de décès (art. 91 C.C.)
- les jugements ou arrêts remplaçant des actes non dressés, perdus ou détruits (art. 46 C.C.).

Le service central d'état civil du ministère des affaires étrangères est compétent lorsque les actes de l'état civil ont été ou auraient dû être dressés à l'étranger.

↳ Transcriptions des jugements d'adoption plénière.

- L'article 354 du code civil prévoit que la décision prononçant l'adoption plénière d'un enfant est transcrite sur les registres de l'état civil du lieu de naissance de l'adopté et que la transcription ainsi opérée tient lieu d'acte de naissance à l'adopté, l'acte de naissance originaire et, le cas échéant l'acte de naissance établi en application de l'art. 58 du code civil sont annulés.
- L'article 354, alinéa 2, du code civil, tel qu'il résulte de la loi n° 96-604 du 5 juillet 1996 relative à l'adoption, prévoit que, lorsque l'adopté est né à l'étranger, la transcription du jugement est effectuée sur les registres du service central d'état civil du ministère des affaires étrangères.

2) Procédure de transcription

↳ Auteur de la demande :

- la transcription est demandée à l'officier de l'état civil détenteur des registres sur lesquels elle doit être effectuée
  * par l'officier de l'état civil "dans le plus bref délai", pour les actes de décès reçus dans une commune autre que celle où était domicilié le défunt (art. 80 C.C.°
  * par le procureur de la République, les parties, leurs avocats ou leurs avoués, pour les décisions de justice dont la transcription est ordonnée par la loi ou le juge
  * par l'autorité maritime ou le consul de France, pour les actes reçus en mer
  * par le ministre de la défense ou ministre chargé des anciens combattants, selon le cas, pour les actes dressés par les officiers de l'état civil militaire (n° 212).

↳ Présentation des demandes

- Transcription d'un acte de l'état civil. Il suffit d'adresser à l'officier de l'état civil une copie de l'acte à transcrire, avec le motif de l'envoi.
- Transcription d'une décision judiciaire
  * l'article 506 du nouveau code de procédure civile prévoit que "les mainlevées, radiations de sûretés, mentions, transcriptions ou publications, qui doivent être faites en vertu d'un jugement sont valablement faites au vu de la production, par tout intéressé d'une expédition ou d'une copie certifiée conforme du jugement, et, s'il n'est exécutoire par provision, de la justification de son caractère exécutoire. Cette justification peut résulter d'un certificat établi par l'avocat ou l'avoué".
    Les officiers de l'état civil sont soumis par, lettre - missive émanant des intéressés eux-mêmes, ou de leur avocat ou avoué, devant la cour d'appel.
    Lorsque la demande émanera de ces auxiliaires de justice, il y aura lieu de présumer qu'ils sont les mandataires de leurs clients.
    Bien que les textes ne le prévoient pas, l'officier de l'état civil ne peut refuser de recevoir une décision judiciaire qui aurait été signifiée par voie d'huissier (n° 214-1).
  *Lorsque la demande de transcription émane d'un avocat ou d'un avoué, la justification du caractère exécutoire de la décision résultera du certificat qu'il établira ou des termes mêmes de sa lettre (n° 214-2).
  * Seul le parquet peut requérir la transcription des décisions rendues en matière d'adoption plénière, d'adoption simple et en matière d'absence.
    Compte tenu des dispositions de l'article 90 du code civil, c'est généralement le parquet qui requiert la transcription du jugement déclaratif de décès (n° 215).

↳ Modalités de la transcription.

- La transcription doit être effectuée dès que l'officier de l'état civil est en possession des documents nécessaires.
  Les actes de l'état civil sont transcrits intégralement, mais seul le dispositif des décisions judiciaires donne lieu à transcription (n° 216).

↳ Procédure de transcriptions d'actes de l'état civil et de décisions judiciaires

- *Règles de base :*

** L'officier de l'état civil reporte sur ses registres un acte de l'état civil reçu ailleurs que dans sa circonscription ou une décision judiciaire relative à l'état civil.*
** Les transcriptions sont effectuées dans un but de publicité (acte de décès ou jugement déclaratif d'absence dans la commune de dernière résidence, acte de reconnaissance d'enfant naturel dans la commune du lieu où l'acte de naissance a été dressé), en vue de remplacer un acte manquant (jugements déclaratifs de naissance, de mariage ou de décès, jugements remplaçants des actes non dressés, perdus ou détruits), en vue de tenir lieu d'acte de naissance suite à un jugement d'adoption plénière.*
** Un avis de mention est envoyé par l'officier de l'état civil aux mairies ou greffes dépositaires des registres dans lesquels sont contenus les actes de l'état civil concernés par les informations objet de la mention marginale.*
Un formulaire comportant un accusé de réception est utilisé à cet effet.

- *Procédure :*

** la demande de transcription est adressée à l'officier de l'état civil sous forme de copie de l'acte à transcrire avec le motif de l'envoi*
** la transcription est effectuée par l'officier de l'état civil détenteur des registres sur demande d'un autre officier de l'état civil, du procureur de la République, des parties et leurs avocats ou avoués, du juge, du ministre de la défense ou des anciens combattants et de l'autorité maritime ou le consul de France.*
** la transcription est datée et signée par l'officier de l'état civil qui l'a reçue.*

② Procédure de transcription d'actes et de décisions judiciaires : pratiques administratives en vigueur.

L'officier de l'état civil procède à la transcription de l'acte, suite à la demande des intéressés. Copie de l'acte est ensuite transmise au demandeur.

En guise de conclusion provisoire...

- Un premier constat au vu des règles de l'Instruction générale relative à l'état civil et des pratiques administratives en vigueur permet de penser que la dématérialisation des actes de l'état civil pourrait être engagée avec plus ou moins de facilités selon qu'il s'agisse de la procédure d'établissement, de mise à jour, de communication ou de conservation des actes.

↳ Etablissement des actes :

Les règles actuelles de l'I.G.E.C. ne permettent une dématérialisation de la procédure aboutissant à un traitement à distance, que dans des cas marginaux (envoi d'un dossier de mariage à remplir par les futurs mariés avant un premier rendez-vous à la mairie par exemple).

Dans la plupart des cas il y a nécessité de déplacement et de comparution des parties à l'acte ou des déclarants devant l'officier de l'état civil. Pour l'acte de mariage il y a de surcroît des règles aboutissant à une solennité lors de l'établissement.

Néanmoins, dans la pratique administrative quotidienne des procédures proches d'un traitement à distance existent.

* Pour l'établissement d'un acte de naissance des procédures permettant d'éviter le déplacement des parents en mairie existent dans certaines communes (liaison entre la mairie et les maternités).
* Pour l'établissement d'un acte de décès, il y a aujourd'hui dans la plupart des cas une sorte de "déclarant délégué" l'entreprise de Pompes Funèbres. Pour cette entreprise, du fait de sa notoriété sur la place publique, des procédures limitant les déplacements ou l'attente aux guichets sont mises en place.

Il y aurait lieu dans ce contexte de vérifier de quelle manière des traitements à distance pourraient être mis en place avec ces partenaires identifiés et connus (maternités, entreprises de Pompes Funèbres par exemple).

↳ Mise à jour des actes

Tant pour l'envoi d'avis de mentions que de transcriptions, les échanges par voie électronique ne devraient pas poser de problème de sécurité particulier dans la mesure où ces échanges ont lieu entre des partenaires institutionnels identifiés.

Il est de même pour toutes sortes d'échanges d'informations concernant l'état civil entre administrations.

- Communication des actes de l'état civil

  La difficulté de la délivrance de copies ou d'extraits des actes de l'état civil sous forme dématérialisée est principalement liée à la diversité des destinataires. L l'GEC impose des vérifications afin de pouvoir identifier ces derniers.
  Cette prudence est fondamentale dans la mesure où la délivrance de copies et d'extraits est soumise à des restrictions.
  Il y aurait donc lieu de trouver, dans l'hypothèse d'une transmission dématérialisée, le moyen technique permettant d'identifier le demandeur et le destinataire ainsi que celui de garantir l'intégrité de la pièce envoyée.
  Pour les échanges entre les partenaires institutionnels, l'envoi de pièces dématérialisées ne devrait pas poser de problème fondamental.

- Conservation des actes de l'état civil sous forme dématérialisée

  A priori la conservation dématérialisée des actes soulève les mêmes interrogations que pour la conservation des registres papier ; celui de la durée dans le temps des techniques utilisées.
  Pour la conservation dématérialisée s'ajoute la question d'un éventuel piratage informatique des fichiers.

  Néanmoins, des expérimentations de certaines collectivités devraient être examinées avec précision : la ville de Karlsruhe en Allemagne par exemple, n'utiliserait plus pour ses archives relevant des diverses formalités administratives, que des supports électroniques.

ANNEXES

Annexe 1

LES PRESTATIONS DE L'ETAT CIVIL DE LA VILLE DE STRASBOURG EN CHIFFRES*

*(chiffres moyens par an)

Nombre d'actes conservés (naissances, mariages, décès)	1.050.000 dont 70 % sont conservés sur support informatisé en parallèle du support papier
Nombre d'actes établis par an	15 000
Nombre de mentions apposées	15 000
Nombre de livrets de famille délivrés	4 000
Nombre de pièces d'état civil délivrées (fiches, extraits, copies) dont 95 000 délivrées à distance	500 000

b) Note sur la finalité du décret d'application de l'article 1317 du code civil et sur les différentes phases du processus d'établissement de l'acte authentique.

-Note rédigée par Mme Isabelle GUYON-RENARD et M. Louis-Denis HUBERT-

MINISTÈRE
DES
AFFAIRES ÉTRANGÈRES

REPUBLIQUE FRANCAISE

Nantes, le

Service Central d'Etat civil

Adresse Postale
44941 NANTES
CEDEX 9

Téléphone: 02.51.77.34.45
Référence: n°

Note sur la finalité du décret d'application de l'article 1317 du code civil et sur les différentes phases du processus d'établissement de l'acte authentique

Rédacteurs: I. GUYON-RENARD et L-D. HUBERT/VD

A/S. **Eléments pour la pré-synthèse**

1. La finalité du décret d'application de l'article 1317 du code civil

Faute de certitude sur les nuances que le législateur a souhaité exprimer en utilisant les mots "dressé" et "établi", il est apparu nécessaire de vous faire part de notre interprétation.

* Le terme *"dressé"* se rapporte à l'existence de l'acte authentique, c'est-à-dire qu'un acte peut être authentique même s'il n'existe pas sous une forme papier,

* 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 [1] à l'acte et, plus particulièrement, l'officier publie sous l'autorité et la responsabilité duquel les comparants et les témoins interviennent.

Pour résumer, le mot "établi" paraît équivalent à "créé".

* 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). L'archivage des actes n'a d'intérêt qu'en vue de

(1) Aux no 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.

leur exploitation au profit des intéressés. En effet, ceux-ci peuvent se prévaloir régulièrement de la force probante particulière de ces actes auprès de tiers ou d'administrations. C'est la principale spécificité de la tenue de l'état civil.

Pour résumer, le mot "conservé" pourrait être remplacé par "archivé et exploité".

2. Différentes phases du processus d'établissement de l'acte

(a) Points communs à tout le processus

• Ne pas interdire le recueil des déclarations ou des consentements dans les formes actuellement en vigueur, qui peuvent coexister avec celles offertes par les nouvelles technologies.

• La création et l'exploitation des actes authentiques sur support électronique implique l'abandon de leur impression sur papier puisque celle-ci n'aurait aucune valeur juridique. La sauvegarde doit nécessairement être électronique.

• La signature de l'officier de l'état civil ou des parties ne doit pas forcément être visible sous une *forme identique* à celle pratiquée aujourd'hui. Il peut s'agir d'une phrase, d'un mot, d'un signe etc... qui doit en revanche être immuable et inaltérable.

• Chaque fois que l'on a envisagé de scinder les étapes de la création de l'acte authentique entre deux officiers de l'état civil, il a été prévu qu'il en soit fait état dans l'acte authentique et que les documents ou fichiers justificatifs soient conservés aux pièces annexes.

Par voie de conséquence, il semble nécessaire de prévoir l'horodatage de toutes les informations recueillies ou transcrites par l'officier de l'état civil.

(b) Phase 1 : Etablissement de l'acte

Dans la réflexion, cinq éléments ont été pris en considération :

1. Constat préalable

- saisie des actes sous forme de traitement de texte (plus aucun acte n'est manuscrit)
- et vœu corollaire : présentation des actes sous forme de rubriques et non plus de texte. Voir pour l'importance de cette présentation la phase 2 (solution 1. 1.).

2. Les critères de l'authenticité sont différents selon que l'on se situe *lors de sa création ou lors de son exploitation*

Lors de sa création ce qui est important c'est :

- la solennité

- la vérification de la déclaration d'un fait (naissance, décès) ou de la réalité de la liberté et de l'étendue d'une volonté (mariage, reconnaissance) et de l'identité des personnes qui s'engagent par leur signature[2]

- signature, par l'officier de l'état civil compétent, de l'acte dans lequel est relaté ce fait ou cette (ces) volonté(s).

Lors de son exploitation, seul un de ces éléments est important :

[2] En cas de suppression de ce critère, voir annexe.

- 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.

Les caractéristiques de l'authenticité et la responsabilité corollaire de l'officier de l'état civil sont donc différentes lors de la création ou lors de l'exploitation de l'acte alors que dans les deux cas il produit bien un acte authentique (Pacte original ou sa copie).

En conséquence, il nous est apparu que les conditions "d'établissement" (création) de l'acte authentique peuvent être différentes des conditions de conservation" (exploitation), c'est-à-dire que l'on peut choisir un procédé pour l'établissement de l'acte et un autre pour sa conservation.

3. L'intérêt majeur de la loi est d'ouvrir la réflexion sur d'autres modes de tenue de l'état civil qu'il nous appartient de définir en prenant en considération les demandes suivantes exprimées par les usagers et les professionnels :

- 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),

- éviter des déplacements ou renforcer la simultanéité des manifestations de volonté (mariage ou reconnaissances conjointes),

- simplifier les démarches des usagers et limiter la fraude en dématérialisant l'échange d'informations relatives à l'état civil.

4. On ne prend pas position sur les procédés, on imagine des situations dans lesquelles les critères fondamentaux de l'acte authentique sont respectés et on laisse aux techniciens le soin de définir les outils adéquats (signature numérisée, stylo électronique, signature par clés ...).

Comme nous avons considéré que le déclenchement d'une signature manuscrite numérisée est une signature électronique au sens de l'article 1316-4 du code civil ([3])[4], nous n'avons pas développé notre réflexion sur la conservation de la trace d'une signature qui ne serait pas visible à l'écran. Elle pourrait l'être dans un second temps, après détermination par le groupe de travail du processus de création de l'acte et des choix technologiques adaptés.

Sur la base de ces considérations, il nous est apparu que diverses solutions peuvent être proposées :

1. Premier éventail de solutions dans lequel les conditions "d'établissement" (création) de l'acte sont différentes de celles de son exploitation (c'est-à-dire que l'acte n'est pas forcément signé électroniquement alors qu'il sera exploité électroniquement)

Solutions 1. 1. (officier de l'état civil territorialement compétent seul intervenant)

1.1.1. - Projet d'acte établi par l'officier de l'état civil sur du papier signé seulement par les comparants.

- qui devient authentique après numérisation de ce document et signature électronique (par exemple, numérisée) de l'officier de l'état civil déclenchée (ou apposée) par lui.

---

[3] Ce mode de signature, déjà pratiqué au service central d'état civil pour la délivrance de copies ou d'extraits comme substitut de la signature à l'aide d'un stylo, consiste en l'apposition d'un "pavé de signature" comportant, outre la signature manuscrite numérisée de l'officier de l'état civil, le lieu, le nom, le prénom, la qualité et le sceau de l'officier de l'état civil authentificateur. L'apposition de ce "pavé" sur la copie ou l'extrait ne peut être déclenchée par l'officier de l'état civil qu'en tapant un mot de passe personnel et confidentiel,

[4] Cette analyse présente aussi l'avantage de réduire le nombre de questions à résoudre à ce stade de la réflexion puisque le contenu de l'acte n'est pas fondamentalement modifié.

L'acte authentique est crée grâce à la signature par l'officier de l'état civil du document, signé par les parties, qui a été préalablement numérisé. L'acte authentique est celui conservé à l'écran puisqu'il est le seul à avoir été signé par l'officier de l'état civil. Il est de ce fait prêt à l'exploitation. Il sera donc délivré en copie un document, différent de celui signé par les comparants, puisqu'il y figurera en plus la signature de l'officier de l'état civil.

1. 1.2.- Acte établi sur du papier signé par les comparants et l'officier de l'état civil.
Il est donc authentique, conformément aux pratiques actuelles de création de l'acte.

- Il est ensuite numérisé en vue de son exploitation informatique par le même officier de l'état civil ou par un autre dans le même service. Lors de l'exploitation, il sera communiqué à l'intéressé une copie fidèle de l'acte signé par les comparants.

L'officier de l'état civil engagera sa responsabilité soit en clair (par une mention du type "acte authentique numérisé par ..... le .....) soit grâce à l'informatique (traçabilité des opérations de numérisation).

Il garantira ainsi la mue de l'acte de l'état civil traditionnel en acte exploitable informatiquement qui deviendra le nouvel acte authentique de référence.

Solution 1.2. (deux officiers de l'état civil [celui du domicile et celui territorialement compétent] pour la déclaration de faits (naissance, décès»[5])

- Projet d'acte établi par l'officier de l'état civil du domicile signé par les comparants.

- Numérisation en vue de la transmission sans délai à l'officier de l'état civil territorialement compétent. L'officier de l'état civil engage sa responsabilité non seulement sur les deux premiers critères de création de l'acte (solennité et vérifications (cf. (b) 2.) mais aussi sur la fiabilité de la numérisation.
- Signature sans délai du projet d'acte par l'officier de l'état civil territorialement compétent qui ainsi le transforme en acte authentique après y avoir ajouté en formule finale : "Dressé le ..... à .....sur transmission électronique des données par (Prénom(s) NOM, qualité de l'officier de l'état civil qui a transmis le projet) le ....."

Dans ces trois solutions, on doit [ou on peut seulement ? compte tenu de l'engagement de responsabilité de l'officier de l'état civil chargé de la numérisation] transmettre le projet d'acte (1. 1. 1 . ou 1.2.) ou l'acte (1. 1.), qui sont sur support papier, à l'officier de l'état civil qui a créé ou exploitera l'acte authentique électronique, afin qu'il le conserve comme pièce annexe.

2. Second éventail de solutions dans lequel les conditions d'établissement (ou de création) sont identiques à celles de son exploitation (c'est-à-dire, abandon du papier, le processus est entièrement informatisé).

Elles reposent toutes sur l'idée que l'on peut partager entre officiers de l'état civil les trois phases de la vie d'un acte authentique au cours desquelles la responsabilité de l'officier de l'état civil est engagée (recueil des déclarations ou des consentements, établissement de l'acte, conservation de l'acte).

[5] Pour le mariage, l'officier de l'état civil chargé d'établir l'acte étant compétent à raison du domicile, cette situation a été exclue de la réflexion.

Solutions 2. 1.

Cas des déclarations des faits d'état civil (décès, naissance)

2. 1. 1. - le déclarant donne des éléments d'information à l'officier de l'état civil le plus proche de son domicile qui rédige un projet d'acte. Il est signé par le déclarant[6] de façon électronique (par exemple avec une signature numérisée).

- cet officier de l'état civil transmet électroniquement le projet d'acte à l'officier de l'état civil territorialement compétent qui le signe électroniquement (par exemple avec sa signature numérisée) après y avoir ajouté en formule finale : "Dressé le .....à .....sur transmission électronique des données par (Prénom(s) Nom, qualité de l'officier de l'état civil qui a transmis le projet) le ....."

2. 1.2. Le déclarant transmet les données, par intranet ou internet avec des niveaux de sécurité adéquats, à l'officier de l'état civil qui établit un acte signé par lui seulement. L'officier de l'état civil engage sa responsabilité sur le contenu de l'acte, le déclarant s'étant lui-même engagé préalablement en assurant la transmission de sa déclaration. Dans la formule finale de l'acte, il sera ajouté : "Dressé le .....à .....sur transmission électronique des données par (Prénom(s) NOM, qualité du déclarant)."

Dans les deux cas, la déclaration transmise électroniquement est conservée dans un fichier réservé aux pièces annexes, après attribution d'une référence qui permette de faire un lien entre la déclaration et l'acte.

Solution 2.2.

Cas du recueil de l'échange de consentement ou de manifestations de volonté (mariage, reconnaissances conjointes).

2.2.1. Préparation du projet d'acte de mariage ou de reconnaissance et apposition simultanée de signatures par les futurs époux ou par les parents (numérisée ou autre) (avantage : créer une véritable simultanéité de l'échange des consentements qui n'existe pas actuellement).

2.2.2. En l'absence de déplacement des futurs époux ou des auteurs de la reconnaissance devant le même officier de l'état civil mais déplacement de chacun d'eux chez un officier de l'état civil différent.

2.2.2.1. Recueil du consentement par chaque officier de l'état civil et apposition simultanée de la signature de chaque futur époux (ou parent) et de l'officier de l'état civil. Dans ce cas, les parties et l'officier de l'état civil ont accès à l'acte concomitamment.

2.2.2.2. Recueil du consentement du futur époux absent par un autre officier de l'état civil qui en informe, le jour du mariage, l'officier de l'état civil chargé d'établir l'acte. Celui-ci est signé par l'officier de l'état civil et un seul époux (parent). Dans la formule finale de l'acte, il sera ajouté : "Lecture faite et invités à lire, M .....a transmis électroniquement son consentement et M ..... a signé avec Nous ..... "

2.2.2.3. Utilisation d'une webcam qui permet à l'officier de l'état civil, chargé d'établir l'acte, de s'assurer également par lui-même de l'expression du consentement de l'autre partie devant un autre officier de l'état civil. Faut-il prévoir la conservation du film aux pièces annexes ? Il devra être ajouté l'acte que le consentement a été constaté par webcam sous le contrôle de ..... (Prénom(s), NOM, qualité de l'officier de l'état civil).

[6] Dans le cas où la signature du déclarant ne serait pas exigée, voir annexe.

(c) Phase 2 : Délivrance de copies

Bases de la réflexion :

- l'intérêt majeur de la nouvelle loi est de permettre la délivrance de copie d'acte authentique sur un support dématérialisé sans jamais avoir besoin de se reporter à un quelconque acte authentique sur support papier,

- compte tenu de ce que nous avons écrit sur la phase 1, l'acte authentique, dont une copie doit être délivrée, peut comporter ou non une image de la signature des parties ou de l'officier de l'état civil.

Solution 1. 1.

Entre service administratif producteur et service administratif utilisateur (exemple : mairie/préfecture).

Transmissions (par intranet ou internet) :

- de copies ou d'extraits d'actes,
- de fichiers de données.

Pour limiter les demandes de copies ou d'extraits formulées auprès des particuliers par les administrations, des documents ou certificats, ne comportant que certaines rubriques de l'acte original et répondant ainsi strictement aux besoins des administrations concernées, devraient être créés. Leur délivrance directe aux administrations par l'officier public détenteur de l'acte devrait être autorisée. On pourrait considérer que ces documents ou certificats n'ont aucun caractère authentique. Ils comporteraient l'identification de l'officier public émetteur et la date de l'émission. Ils pourraient être réclamés et délivrés par voie télématique sécurisée sans cryptage et sans obligation, pour l'administration réceptionnaire, de les éditer sur support papier. La seule obligation pour elle étant de conserver la trace horodatée de la demande et de la réception du document.

Solution 1.2.

Entre services d'état civil pour le compte du particulier.

Un particulier devrait pouvoir s'adresser à n'importe quel officier public auprès duquel il justifierait de son identité et de son droit d'obtenir une copie ou un extrait d'un acte authentique et qu'il mandaterait à cette fin. La même mandat devrait être possible afin d'autoriser l'officier public détenteur de l'acte à délivrer une copie ou extrait à une administration désignée par le mandataire.

- La demande de délivrance de l'acte d'officier publie à officier public devrait se faire par transmission télématique sécurisée. Elle serait horodatée automatiquement et comprendrait, le cas échéant, les énonciations prévues par la loi à peine d'irrecevabilité. L'existence du mandat serait présumée et garantie par la sécurisation du mode de transmission qui garantirait que la demande provient bien d'un officier public. Cette demande de copie ou d'extrait devrait être conservée par l'officier public détenteur de l'acte original et serait complétée automatiquement, au moment du déclenchement de la transmission, par l'indication de l'identité de l'officier public qui l'a satisfaite, de la date et de l'heure de la transmission de la copie ou de l'extrait réclamé.

- La transmission de la copie intégrale ou de l'extrait par l'officier public détenteur de l'acte à l'officier public mandataire ou à l'administration se ferait aussi par voie télématique sécurisée après signature électronique horodatée de la copie ou de l'extrait certifié conforme (par exemple, avec une signature numérisée).

- L'officier publie mandataire délivrerait sans délai à son mandant un tirage sur papier sécurisé de l'acte reçu sur lequel serait imprimé automatiquement l'identification de l'officier public émetteur détenteur de l'acte original, la date de la réception de l'acte par l'officier public mandataire, et celle de sa remise par celui-ci. Sur cette impression, il apposerait sa signature manuscrite et son sceau. Ainsi, l'officier public détenteur de l'acte prendrait la responsabilité du certificat de conformité à l'original tandis que l'officier publie mandataire destinataire de la copie ou de l'extrait prendrait la responsabilité de l'absence de modification du contenu de la transmission, et des conditions de remise du tirage papier à son mandant.

- Dans le cas d'un mandat de transmission d'une copie ou d'un extrait à une administration, celle-ci, à réception du document, ne serait tenue qu'à l'impression de celui-ci sur papier libre sur lequel serait imprimée automatiquement l'identification de l'officier public émetteur détenteur de l'acte original, et la date de la réception de l'acte par l'administration. Le fonctionnaire réceptionnaire apposerait sur ce document sa signature manuscrite et son sceau avant de le verser au dossier.

Voir aussi solution 1.2. du (e)

(d) Phase 3 : Mise à jour

Postulat : L'acte authentique est totalement dématérialisé. Il n'existe pas de double sur support papier.

- Mise à jour de l'acte informatisé sans signature (art. 7-1 alinéa 3 Décret du 3 juin 1962)

- Nécessité de créer des sauvegardes ou/et des historiques de mise à jour (conservation des différentes images de l'acte avec un horodatage ?).

Voir aussi solution 1.2. du (e)

(e) Phase 4: Archivage

Base de la réflexion :

Dans un système entièrement dématérialisé, le tirage papier ne sert à rien. Il faut réfléchir à des modes de sauvegarde adaptés.

Rappel : En effet, si l'on édite l'acte authentique sur du papier, il faut aussi le mettre à jour et considérer que l'acte authentique dématérialisé n'est qu'une copie (on est donc censé aussi vérifier sa conformité à l'original papier).

Constat : Le problème de l'archivage se pose à l'officier de l'état civil uniquement pour les actes de plus de cent ans. Avant, comme il doit les exploiter (voir phases 2 et 3), il est censé veiller à la pérennité des systèmes informatiques.

Deux solutions :

1. 1. L'officier de l'état civil assure lui-même la pérennité des systèmes pour la mise à jour, l'exploitation et l'archivage.

1.2. L'officier de l'état civil sous-traite la numérisation (solution 1. 1.2. du (b) et par voie de conséquence, la mise à jour, l'exploitation et l'archivage à un service central d'état civil qui se chargerait de la maintenance de l'outil informatique.

Cette solution qui semble viable *a priori* pour les communes, qui ne sont pas informatisées, pourrait le cas échéant être étendue aux services d'état civil informatisés qui souhaiteraient sous-traiter l'exploitation et la conservation des actes qu'elles ont créés.

Ainsi pourraient être instaurées des liaisons du type de celles existant actuellement entre l'INSEE et les mairies. L'usager ne s'adresserait plus qu'à un seul service chargé de l'état civil en France.

Au-delà de cent ans, deux solutions pourraient être proposées :

- création d'un centre d'archives qui assure la maintenance de son système informatique et sa compatibilité avec les systèmes provenant des services d'état civil qui procèdent aux versements.

- mise en place pour les archives d'un acte aux fichiers informatisés des données ou actes de l'état civil, qui serait limité à ceux qui ont plus de cent ans./.

Isabelle GUYON-RENARD
Conseillère juridique au service central d'état civil

Louis-Denis HUBERT
Procureur-adjoint chargé
du service civil du parquet de Nantes

ANNEXE

Si l'on change les critères de l'authenticité en supprimant la signature de l'acte authentique par les comparants, on peut imaginer cette solution, limitée aux déclarations de faits [7]

L'officier de l'état civil du domicile peut recevoir la déclaration et la signer. Il la transmet à l'officier de l'état civil territorialement compétent qui signe, seul, l'acte qu'il a établi. La déclaration est conservée aux pièces annexes après avoir été transmise par l'officier de l'état civil qui a recueilli la déclaration.

Une réflexion approfondie pourrait être engagée si le groupe de travail choisit cette option de suppression de la signature des comparants.

[7] En cas de recueil du consentement, cette solution ne paraît pas transposable du fait que par hypothèse l'officier de l'état civil sera compétent pour dresser l'acte.

c) Premières réflexions rapides sur l'acte d'état civil dressé sur support électronique eu égard aux contraintes actuelles de l'état civil.

-Note rédigée par M. Louis-Denis HUBERT-

PREMIERES REFLEXIONS RAPIDES SUR L'ACTE D'ETAT CIVIL DRESSE SUR SUPPORT ELECTRONIQUE EU EGARD AUX CONTRAINTES ACTUELLES DE L'ETAT CIVIL

1. NOTION D'ACTE D'ETAT CIVIL

La définition est donnée par Cass. civ. 1 14 juin 1983 Bull Civ I 174 : "*Ecrit* dans lequel *l'autorité publique constate* d'une manière *authentique* un événement ont dépend l'*état* d'une ou plusieurs personnes."
Instruction Générale Relative à l'Etat Civil 1**: L'acte d'état civil tire sa force probante de son caractère authentique**.

L'Instruction Générale Relative à l'Etat Civil renvoie à la définition générale des actes authentiques de l'article 1317 du code civil: "*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.*"
"*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 D64 627)

En revanche, la véracité des faits qui ont été déclarés à l'officier de l'état civil fait foi jusqu'à preuve contraire.
Instruction Générale Relative à l'Etat Civil 93: "La présence de l'officier de l'état civil est nécessaire pour conférer à l'acte la force probante authentique; Il doit recevoir en personne les déclarations des comparants"

Discussion parlementaire: Madame le Garde des Sceaux:" *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.*"

2. RÈGLES GÉNÉRALES RELATIVES AUX ACTES DE L'ETAT CIVIL

1°) L'acte d'état civil nécessite le plus souvent l'intervention (actuellement la présence physique simultanée) d'un officier de l'état civil et de comparants.
Les comparants sont soit déclarants, soit parties, soit témoins.
Le déclarant est habilité par la loi à faire connaître à l'officier de l'état civil un fait ou un événement (naissance, décès).
Les parties sont des personnes dont l'expression de la volonté crée une situation juridique nouvelle que l'acte d'état civil va constater (reconnaissance, mariage).
Les témoins ne sont requis que pour le mariage.
L'Officier de l'état civil doit vérifier l'identité des comparants.
L'Officier de l'état civil peut déléguer ses fonctions d'Officier de l'état civil (art. 6 Déc. 3/8/62).
Sauf pour le mariage, les comparants peuvent se faire représenter par un "fondé de procuration spéciale et authentique (art. 36 du code civil).
L'acte d'état civil doit être reçu en mairie (sauf exception: prison, maternité, mariage in extremis..)
L'acte d'état civil doit être reçu sans délai (art. 3 Déc. 3/8/62)

2°) La rédaction des actes de l'état civil:
Instruction Générale Relative à l'Etat Civil 96 à 132; art. 34 et 39 du code civil
Les règles régissant la rédaction des actes de l'état civil sont strictes et entourées de solennité: l'acte doit obligatoirement être daté et comporter, notamment, un numéro d'ordre, une analyse marginale, les prénoms, nom et qualité de l'Officier de l'état civil rédacteur. Il doit être signé par les

comparants et les témoins ainsi que par l'Officier de l'état civil rédacteur.
La rédaction des actes doit être effectuée de façon manuelle ou informatisée sur feuillets mobiles en double original (double registre).
Les actes de l'état civil doivent toujours être dressés, mis à jour et conservés sur support papier.
L'acte doit être lu par l'Officier de l'état civil aux comparants et témoins. L'Officier de l'état civil doit inviter les comparants à prendre "directement" connaissance de l'acte avant d'y apposer leur signature. (art. 38 du code civil; Instruction Générale Relative à l'Etat Civil 94 72).

3°) L'importance des signatures Instruction Générale Relative à l'Etat Civil 130 à 132
Les signatures devant figurer sur l'acte établi sont obligatoires et limitatives: ce sont celles des comparants et de l'Officier de l'état civil.
C'est l'Officier de l'état civil qui clôt l'établissement de l'acte en y apposant sa signature et qui lui donne ainsi sa force authentique.
La machine à signer et la griffe sont exclues: la signature de l'Officier de l'état civil doit être manuscrite (art. 1 al. 2 Déc. 3/8/62); elle certifie la présence effective de l'Officier de l'état civil.
Mais l'absence de signature d'un comparant n'est pas de nature à enlever à l'acte l'autorité légale qui lui appartient (Cass. Civ. 1 23/6/1869) (Instruction Générale Relative à l'Etat Civil 166) car une régularisation a posteriori est possible.
En cas d'absence de signature de l'Officier de l'état civil, le Procureur de la République l'invite à signer s'il est encore en fonction. Dans le cas contraire, l'acte ne pourra se voir conférer force authentique que par jugement. (Instruction Générale Relative à l'Etat Civil 167)

<u>En cas d'établissement des actes d'état civil sur support électronique:</u>

- *La signature électronique consiste en un procédé fiable d'identification de celui qui l'appose; elle doit aussi garantir son lien avec l'acte auquel elle s'attache (identification formelle du signataire et garantie de l'intégrité de l'acte signé). Elle n'exige donc pas la visualisation, sur l'acte lui-même, d' un quelconque signe.*

-

- Il faudrait que chaque comparant possède une signature électronique propre qu'il appose sur l'acte <u>en présence et avant</u> celle de l'Officier de l'état civil (système de double clefs publique et privée).
Soit le comparant possède une telle signature qu'il appose sur l'acte pour certifier son identité et son approbation du contenu de l'acte dans la version qu'il visualise à l'écran, soit c'est l'Officier de l'état civil qui se charge de faire générer pour lui les clefs indispensables à sa signature électronique certifiée avant la rédaction de l'acte et pour les besoins de celle-ci.
On pourrait aussi concevoir que les comparants dépourvus de signature électronique (autres que l'Officier de l'état civil qui en serait systématiquement doté) signent au moyen d'un stylo électronique.
Après ces signatures, l'Officier de l'état civil apposerait sa signature électronique lui conférant le caractère authentique.
- Une autre solution consisterait à saisir les énonciations de l'acte en traitement de texte avant de l'imprimer afin qu'il puisse recevoir la signature manuscrite des comparants avant d'être scannerisé et de recevoir la signature électronique de l'Officier de l'état civil.
Dans les 2 cas, c'est la signature électronique de l'Officier de l'état civil qui aurait pour effet de "figer" l'acte dans sa formule définitive interdisant toute modification ultérieure. Une sécurité indispensable consisterait à prévoir un historique enregistrant toutes les versions du même acte (date et nature des modifications; nom de l'Officier de l'état civil qui a procédé à la modification).
- Toutes les énonciations de l'acte devraient figurer en clair afin d'être visualisées, lues, vérifiées et approuvées par les comparants avant qu'ils apposent leur signature (y compris l'identification de l'Officier de l'état civil et la date de l'acte).

3. RÈGLES GÉNÉRALES DE RÉDACTION DES ACTES DE L'ETAT CIVIL

Instruction Générale Relative à l'Etat Civil 96 et suivants:
Un acte de l'état civil signé ne peut être rectifié, modifié ou raturé par l'officier de l'état civil.
La tenue de l'état civil doit garantir la conservation et la pérennité de l'état civil. L'archivage n'est possible qu' après 100 ans.
Au début de chaque année, un exemplaire de chaque registre est transféré au greffe du tribunal de grande instance. (art. 53 du code civil).
L'informatisation de la tenue de l'état civil doit répondre à des règles de sécurité et de confidentialité sous la surveillance du procureur de la république.
La tenue en double des actes de l'état civil répond à ce souci de sécurité et de pérennité (art. 1 Déc. 3/8/62).

La conservation des pièces annexes est réglementée.

En cas d'établissement des actes d'état civil sur support électronique:

- *La règle de prohibition des ratures ne se pose pas jusqu'à la signature électronique de l'Officier de l'état civil. Après celle-ci, et tant que tous les comparants sont présents , la "réparation" prend la forme de rajouts en marge (en bas) de l'acte qui sont signés par tous les comparants avant de l'être par l'Officier de l'état civil de la même façon que lors du premier "dressé". Une "photo" du nouvel acte doit être réalisée et conservée dans l'historique joint à l'acte électronique.*
- *La tenue en double de l'état civil exige une sauvegarde systématique de l'acte et de son historique après le dressé de chaque acte et chaque mise à jour. La conservation de cette sauvegarde (double parfait) devrait être effectuée dans une base de donnée indépendante, et, à terme, sur un support inaltérable.*
- *L'accès à la base contenant les actes ou leur sauvegarde doit être sécurisé pour garantir la confidentialité.*

4. MISE A JOUR DES ACTES D'ETAT CIVIL

Instruction Générale Relative à l'Etat Civil 218 à 251; art. 7-1 Déc. 3/8/62; art. 49du code civil:
Cette mise à jour s'effectue par apposition de mentions "marginales". "Toute mention matginale énonce en outre, le lieu et la date de son apposition ainsi que la qualité de l'Officier de l'état civil qui a procédé à la mise à jour ou, lorsqu'elle est manuscrite, signé la mention."
Ces mentions sont provoquées par l'envoi d'avis de mention d'Officier de l'état civil à Officier de l'état civil, par réquisitions ou instructions du parquet, à la demande de certaines administrations, des juges d'instance, des greffiers en chef des tribunaux d'instance, à la requête des avocats, des notaires, ou des intéressés eux-mêmes.
Elles doivent être apposées dans un délai de 3 jours.
Elles ont la même force probante que l'acte lui-même.

En cas d'établissement des actes d'état civil sur support électronique:

- *Le décret de 1962 n'exige la signature de la mention par l'Officier de l'état civil qu'en cas d'apposition d'une mention manuscrite. La signature électronique de la mention ne pose donc aucun problème. Elle doit comporter, outre l'identification de l'Officier de l'état civil qui appose la mention, la date et le lieu d'apposition de celle-ci (horodatage).*
- *La mention apposée sur support électronique doit faire corps avec l'acte lui-même. La signature électronique de l'Officier de l'état civil et l'historique doivent garantir cette indissociabilité afin que, dorénavant, l'acte ne puisse plus être exploité que dans sa version mise à jour.*

5. DÉLIVRANCE DE COPIES OU D'EXTRAITS

Art. 13 Déc. 3/8/62; Instruction Générale Relative à l'Etat Civil 193 et suivants
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 .
Il est possible de réaliser une copie intégrale de tous les actes de l'état civil mais seuls les actes de naissance et de mariage peuvent faire l'objet d'extraits.
Art. 8 Déc. 3/8/62
Les Officier de l'état civil ne peuvent délivrer des copies et extraits que des actes qu'ils détiennent. Cependant, "au sein d'une même commune comprenant des divisions administratives où sont détenus les registres d'état civil de leur ressort, les Officier de l'état civil peuvent délivrer, chacun dans sa circonscription, des copies et extraits des actes dressés ou transcrits dans l'ensemble de la commune.
Les copies ou extraits sont délivrés sur place ou par correspondance avec possibilité de demandes par voie télématique.
COPIES:
Instruction Générale Relative à l'Etat Civil 194:
Principe: C'est la reproduction intègrale de l'acte original (mentions comprises).
Mais: cette reproduction doit être purgée des énonciations qui n'auraient pas dû figurer sur l'acte original en vertu d'une réglementation devenue obsolète ou d'une loi étrangère contraire à l'ordre public français (exemple: la mention de radiation du répertoire civil ne doit pas apparaître).
Instruction Générale Relative à l'Etat Civil 195: La loi ne prévoit ni procédé de délivrance des copies (rédaction manuelle ou reproduction), ni obligation de délivrance sur papier sécurisé.
Instruction Générale Relative à l'Etat Civil 196: La copie doit énoncer la date de délivrance, la qualité et le nom de l'Officier de l'état civil signataire, la signature et le sceau de cet Officier de l'état civil.
Les copies font foi jusqu'à inscription de faux (art. 13 Déc. 3/8/62).
Par souci de confidentialité, les copies ne sont délivrées QU' à certaines personnes et sous certaines conditions:

Exemple: La copie d'un acte de naissance ou de mariage n'est délivré qu'à
la personne concernée par l'acte,
ses ascendants ou descendants,
son conjoint,
son représentant légal
majeur ou émancipé
et sur indication des noms et prénoms usuels de ses parents.

Les personnes autorisées peuvent donner mandat exprès (mandat présumé pour les notaires ou avocats)(Instruction Générale Relative à l'Etat Civil 197-5)

EXTRAITS:
Instruction Générale Relative à l'Etat Civil 198 et suivants: Ils nécessitent une création spécifique car toutes les énonciations et mentions de l'acte original n'y figurent pas et certaines mentions figurant en marge de l'acte original doivent être intégrées dans le corps de l'extrait.
Par souci de confidentialité, les extraits ne sont délivrés qu'à certaines personnes.
Comme les copies, les extraits doivent énoncer la date de délivrance, la qualité et le nom de l'Officier de l'état civil signataire, la signature et le sceau de cet Officier de l'état civil. Ils doivent comporter l'énonciation "Extrait conforme au registre" ou, en cas de délivrance informatisée "Extrait délivré selon procédé informatisé." L'extrait ne comporte que la signature de l'officier de l'état civil qui le délivre et non pas celle des comparants à l'acte original.

En cas d'établissement des actes d'état civil sur support électronique:

- La délivrance informatisée des copies et extraits est le véritable enjeu de la tenue de l'état civil sur support électronique en raison du nombre très élevé des demandes d' extraits et de copies.

- Si l'acte original a été dressé et signé de façon électronique, l'Officier de l'état civil chargé de délivrer la copie intégrale doit créer un nouveau document électronique constitué par l'acte original sur lequel il appose la date de délivrance, sa qualité, son nom et son sceau avant de le signer de façon électronique et de l'envoyer. Les énonciations indispensables pour la délivrance (date de délivrance, nom, qualité et sceau de l'Officier de l'état civil) ne doivent pas être portées sur l'acte original qui doit demeurer inviolable durant le processus de délivrance. Par contre, ces énonciations doivent être indissociables de l'acte auxquelles se rapportent pour constituer un nouveau document électronique: la copie intégrale. Dans les cas où la copie intégrale nécessite que l'acte original soit expurgé, ce travail ne doit pas se faire sur l'acte lui-même ou sur sa sauvegarde (double) mais sur une copie de l'acte original. Dans ce cas, la version "copie intégrale" de l'acte original pourra figurer dans l'historique pour servir de base à une délivrance ultérieure. L'établissement de l'acte original sur support électronique permet de certifier la conformité de la copie à cet original et donc sa force probante puisque la visualisation de cet acte original par l'Officier de l'état civil chargé de la délivrance de la copie ne sera possible que si l'acte original n'a subi aucune modification depuis sa signature par l'Officier de l'état civil qui l'a établi. La seule obligation de l'Officier de l'état civil qui délivre est de s'assurer que l'acte qu'il délivre correspond bien à celui du demandeur.

La délivrance d'une copie intégrale ne requiert l'intervention que de l'Officier de l'état civil. La date de délivrance de la copie, le nom, la qualité et le sceau de l'Officier de l'état civil qui délivre n'ont pas à être approuvée par d'autres personnes. C'est pourquoi, la signature électronique de l'Officier de l'état civil qui délivre une copie intégrale peut inclure son identification et la date de délivrance (horodatage automatique) sans que ces éléments n'apparaissent explicitement à la lecture de la copie délivrée. Ces informations pourraient donc être "attachées" à la copie délivrée sous forme électronique et visualisées à la demande ou figurer automatiquement sur la copie en cas d'impression.

- Sur la copie intégrale électronique n'apparaîtrait donc aucune signature manuscrite puisque l'officier de l'état civil qui a dressé l'acte original, l'officier de l'état civil qui la délivre, et les comparants auront apposé leur signature électronique. Seules les signatures manuscrites des comparants qui auront pu être scannerisées apparaîtront sur la copie intégrale électronique. C'est le cas actuellement lorsque l'officier de l'état civil délivre une copie intégrale en recopiant à la main l'acte original.

- Le problème posé par la vérification nécessaire de la qualité du demandeur de la copie ou de l'extrait se posera de la même façon qu'actuellement lorsque l'acte sera dressé sur support électronique. Les demandes de copies actuellement formulées par lettre ou par voie télématique (minitel) ne peuvent être vérifiées. De même, il est aujourd'hui impossible de vérifier l'identité du réceptionnaire de l'acte adressé par voie postale. Par contre, la copie intégrale d'un acte de l'état civil revêtue de la signature électronique de l'Officier de l'état civil qui la délivre est transmise de façon parfaitement sécurisée à un destinataire disposant lui-même d'une signature électronique. Ainsi, dans l'attente de l'attribution d'une signature électronique à chaque personne concernée par un acte de l'état civil détenu sur les registres français, une transmission directe et sécurisée des copies ou extraits d'acte de l'état civil (ou de renseignements d'état civil) aux administrations ou aux officiers de l'état civil serait une amélioration considérable du service public de l'état civil. On pourrait concevoir que le demandeur formule sa demande de copie ou d'extrait auprès de l'Officier de l'état civil ou de l'administration de son choix qu'il mandaterait à cette fin et qui vérifierait sa qualité avant de transmettre sa demande de façon électronique sécurisée à l'Officier de l'état civil concerné. Le document serait ensuite transmis (instantanément) et remis après impression à son destinataire par l'Officier de l'état civil ou l'administration choisie par le demandeur.

6. ACCES AUX ACTES d'ETAT CIVIL: CONSULTATION DIRECTE DES REGISTRES
Instruction Générale Relative à l'Etat Civil 72 et suivants; article 8 al. 1 Déc. 3/8/62
Par souci de confidentialité et de bonne conservation des registres, la consultation directe des registres de l'état civil est en principe interdite sauf aux agents de l'Etat habilités, aux parquets et aux personnes autorisées par le parquet.

La consultation se fait sous le contrôle et la responsabilité de l'officier de l'état civil.
En cas d'établissement des actes d'état civil sur support électronique:
Il convient de sécuriser l'accès aux bases de données des actes (originale et sauvegarde).La consultation ne doit pas permettre la modification de l'acte consulté (ni son impression sauf autorisation du parquet).

Louis-Denis HUBERT

3. Contribution du sous-groupe «jugements»

-Note rédigée par M. Patrick HENRY-BONNIOT

GROUPE DE TRAVAIL SUR L'ACTE AUTHENTIQUE ÉLECTRONIQUE

NOTES DU SOUS-GROUPE "JUGEMENTS"

version finale

A l'issue des réunions du sous-groupe "jugements", tenues le 16 juin et le 11 juillet 2000, il est apparu utile de noter les questions et premières réflexions du groupe relatives aux actes authentiques émanant des juridictions, des huissiers de justice et des greffes de tribunaux de commerce.

Pour répondre à la question de savoir comment mettre en œuvre le principe de l'acte authentique électronique prévu par la loi du 13 mars 2000, il paraît inévitable de s'interroger à la fois sur des questions fondamentales relatives à l'acquisition de l'authenticité, et sur des questions plus terre à terre intéressant l'utilisation pratique de cette innovation juridique.

I - L'acquisition de l'authenticité.

Elle est conférée par la loi à des actes intervenus avec la participation ou émanant de certaines personnes dans des conditions précises.

L'article 1317 du code civil définit l'acte authentique comme ayant été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises. Cette formulation date de l'origine du code civil. Dans son traité des obligations, Pothier appelle actes authentiques ceux *qui sont reçus par un officier public, tel qu'est un notaire ou un greffier*.

La loi du 13 mars 2000 n'a rien changé à ces définitions, toutefois insuffisantes pour délimiter précisément l'objet de l'authentification et préciser l'autorité qui authentifie.

Ainsi sont, en principe, authentiques :

- les décisions judiciaires et les procès-verbaux dressés par un juge dans l'exercice de ses fonctions

- les actes d'huissiers accomplis dans l'exercice de leurs attributions légales

- des actes des greffiers de tribunaux de commerce

- les actes de l'état-civil dressés par les officiers de l'état-civil

- des procès-verbaux d'adjudication des commissaires-priseurs

- certains actes établis par les préfets (L76 code du domaine de l'Etat), les maires (L122-25 code des communes),

- des procès-verbaux dressés par les officiers de police judiciaire (OPJ) dans les cas prévus par des lois spéciales (433 du code de procédure pénale). Le procès-verbal d'OPJ n'a, sauf ces cas particuliers, de valeur probante que de ce que l'OPJ a vu, entendu ou constaté personnellement (cf 429 du code de procédure pénale) ; il ne fait foi que jusqu'à preuve contraire, celle-ci ne pouvant être rapportée que par écrit ou par témoins (537 du code de procédure pénale).

Certains textes confèrent l'authenticité à des actes en matière douanière (336 C des douanes), forestière (L342-4 C forestier) ou de pêche fluviale (L237-4 C rural). Quant aux procès-verbaux des agents de l'administration fiscale, ils ne peuvent être considérés comme authentiques puisqu'ils ne font foi que jusqu'à preuve contraire (L238 du livre des procédures fiscales).

A – L'objet de l'authenticité.

1/ Certainement le constat d'un fait. Mais quels faits ?

Dans le cas du constat d'huissier de justice l'authenticité ne s'attache pas à tout ce qui est mentionné, ni même à tout ce que l'huissier a constaté par lui-même. Toutes les mentions de l'acte authentique n'ont pas la même valeur probante. Il faut, semble-t-il, distinguer les mentions qui correspondent aux constatations personnelles de l'officier public ou ministériel - à condition que leur caractère technique soit limité- de celles qui relatent les déclarations des parties.

En ce sens, des arrêts excluent des procès-verbaux dressés à la requête de particuliers (Cour de Cassation 23 fev 1956 bulletin civil II 138)
ainsi que des procès-verbaux sur demande judiciaire pour constater certains faits
- par exemple un adultère (Ccass 12 déc 1904 Dalloz 1905, 1, 131 et encore cour d'appel de Nancy 8 nov 1972 - Dalloz 73, 94 : les déclarations recueillies par l'huissier ont la valeur d'attestations, s'agissant de faits dont la preuve est libre. Il a, par ailleurs, été jugé que les constatations de l'huissier ne font pas foi jusqu'à preuve contraire dans ce cas de l'adultère, mais qu'elles peuvent constituer une preuve directe)
- ou un constat de prix affichés dans un magasin (Ccass 22 nov 1971 bull civ IV 280 : les constatations matérielles de l'huissier ont une valeur probante souverainement retenue par la cour d'appel)

Ces décisions n'attribuent pas la valeur authentique aux seules constatations. En effet, l'acte demeure authentique dans ses indications concernant notamment la date, le nom de l'huissier

de justice, ainsi que le lieu où il s'est rendu, ou les circonstances d'obtention de ses constatations. Mais il est normal que ce caractère authentique (combattu par l'inscription de faux) ne soit pas accordé à des constatations matérielles qui demeurent de simples éléments de fait.

De même, l'authenticité du procès-verbal du juge d'instruction s'étend aux circonstances extérieures de l'acte ainsi qu'aux déclarations -X a dit ce qui est écrit- mais évidemment pas à la véracité de ce qui est écrit.

Assurément, l'acte fait foi des mentions formelles qu'il contient.

2/ Peut-être le constat d'un consentement ? Mais s'agit-il d'autre chose que du constat de l'expression du consentement qui est un fait comme un autre ?

L'exemple de l'acte notarié est celui que l'article 1319 du code civil a envisagé à titre principal.

Mais quelles sont les conséquences précises sur la validité de l'acte ?

Lorsque les énonciations de l'acte ont trait à des faits qui ne relèvent pas directement de la compétence de l'officier public ou ministériel, il n'est pas nécessaire de recourir à l'inscription de faux pour les combattre.

Les mentions de l'acte qui relatent ce que les parties ont déclaré à l'officier public ou ministériel ne font foi que jusqu'à preuve contraire.

Par ailleurs, le caractère authentique d'une convention n'a jamais mis une partie à l'abri d'une contestation des vices du consentement par une autre partie, qu'il s'agisse de l'erreur, du dol, de la lésion ou même de la violence (pour la violence : Ccass 13 janv 1999, JCP 99 I 143 - violences physiques et morales exercées par les membres d'une communauté sur une personne, l'ayant conduite à vendre sa maison en faveur de l'acquéreur afin que les membres de cette communauté y fussent hébergés).

3/ Le constat d'une décision lorsqu'il s'agit d'un acte juridictionnel

Une décision d'arbitrage n'a pas de caractère authentique. Elle a l'autorité de la chose jugée dès qu'elle est rendue (1476 du nouveau code de procédure civile) mais elle n'est susceptible d'exécution forcée qu'en vertu d'une décision judiciaire d'exequatur.

Inversement, tout acte juridictionnel n'est pas une décision. Le procès-verbal du juge d'instruction est authentique sans pour autant contenir de décision.

En conclusion, les éléments du contenu de l'acte auquel est conféré le caractère authentique varient selon la nature de l'acte et l'autorité qui le signe.

B - La personne conférant l'authenticité.

L'intervention d'un officier public ou ministériel est nécessaire ainsi que sa signature. Cette exigence fondamentale s'étend aux copies d'actes authentiques, ainsi qu'à l'approbation des ratures et surcharges, à peine de nullité (cass civ 20 juin 1968 bull civ II 188)

1/ L'acte d'huissier de justice

Les règles d'élaboration des actes d'huissiers de justice (cf la loi du 27 décembre 1923 - articles 6 et suivants- modifiée par la loi du 9 juillet 1991) établissent les cas dans lesquels un clerc peut instrumenter, l'acte étant de toute façon visé par l'huissier de justice. La jurisprudence décide, notamment dans le cas de la déclaration du tiers saisi dans la procédure de saisie-attribution, que l'acte reçu par un clerc est nul s'il résulte des textes que l'acte doit être établi par l'huissier de justice lui-même.

Par ailleurs, l'huissier de justice ne peut conférer le caractère authentique à son acte, que pour autant qu'il agisse dans le ressort de sa compétence territoriale.
Certains actes peuvent être faits par des clercs (assermentés ou habilités au constat). L'acte pour être authentique doit être fait par une personne "habilitée" et être, en outre, visé par l'huissier de justice, mais également être de ceux que ladite personne peut régulariser.

2/ La décision judiciaire

Le jugement, décision d'un tribunal, est signé du juge et du greffier (456 du nouveau code de procédure civile). L'absence de l'une des deux signatures -et plus généralement l'omission ou l'inexactitude d'une mention destinée à établir la régularité du jugement peut entraîner sa nullité (459 du nouveau code de procédure civile).

En cas d'empêchement du président le jugement d'une juridiction civile est signé par l'un des juges qui en ont délibéré (456 du nouveau code de procédure civile). La même règle, dans des termes identiques, a été introduite pour le jugement du tribunal correctionnel en 1989 (486 du code de procédure pénale).

L'empêchement du greffier ne pourrait entraîner la réouverture des débats que dans des cas particuliers. En effet, ce n'est pas le greffier de l'audience au cours de laquelle l'affaire a été plaidée qui signe le jugement, mais celui du prononcé de la décision. Cette règle montre que le rôle du greffier est d'authentifier la décision, la procédure et les déclarations éventuelles ayant été authentifiées par le registre et les notes d'audience.

Mais toute décision exécutoire n'est pas signée d'un greffier : l'ordonnance sur requête est une décision juridictionnelle non contentieuse exécutoire sur minute. Elle ne comporte que la signature du juge. Son caractère d'acte authentique est-il discutable ?

Une autre complication la concernant, ainsi que tous les jugements gracieux, vient de ce que la décision (jugement ou ordonnance) forme un tout indissociable avec la requête présentée par un avocat ou directement par une partie (466 du nouveau code de procédure civile).

3/ L'acte notarié

(déjà examiné ; voir, notamment les "*remarques préliminaires*" de M. Caprioli sur le site web de la mission droit et justice)

Le plus souvent l'intervention d'un notaire satisfait aux exigences légales. Exceptionnellement la loi en prévoit deux à moins qu'il y ait deux témoins (971 du code civil relatif au testament par acte public, ainsi que pour les actes contenant révocation de testament et pour les actes dans lesquels les parties ne pourraient pas signer).

Le défaut de signature par une des parties entraîne la nullité. En revanche, le recueil successif des signatures est admis et même fréquent. Un acte peut même être signé par le notaire après le décès d'un des signataires. En outre, le décret du 26 novembre 1971 a introduit la possibilité pour un clerc de recevoir les parties et de recueillir leur signature, le notaire devant signer après l'acte pour qu'il devienne authentique (voir l'article du professeur Jacques Flour, paru en 1972. Posant le postulat de la légalité du décret, il estime *"que la force probante d'un tel acte disparaît et que sa force exécutoire devient incertaine"*. Cette possibilité a été confirmée par la loi du 25 juin 1973 modifiant l'article 10 de la loi du 25 ventôse an XI contenant organisation du notariat).

C - Les conditions de l'authenticité.

1/ La présence physique.

* Dans l'acte notarié :

La présence physique est nécessaire mais, en revanche, il est admis que toutes les parties concernées ne soient pas présentes simultanément mais successivement. Cette présence ne concerne que les actes "reçus" par le notaire. Pour les actes "déposés" (par exemple un testament olographe), seul l'acte de dépôt est authentique, sauf cas particuliers.

* S'agissant des actes d'huissier de justice :

Il faut distinguer la présence physique du "significateur" de celle de la personne qui doit recevoir l'acte.

Pour les constatations, la présence physique d'une autre partie que l'huissier de justice ou du clerc habilité aux constats n'est pas requise pour la validité de celles-ci ;

- pour le significateur

La présence physique de l'huissier de justice n'est pas toujours requise, car l'acte peut être régularisé par un clerc qui doit bien entendu être présent.

- pour le signifié
La présence physique du destinataire est souhaitée, mais s'il n'est pas là, le code de procédure civile prévoit une hiérarchie des modes de remise de l'acte, à d'autres personnes (ses proches) ou dans un site (la mairie) où il est toujours possible de rencontrer quelqu'un (sauf fermeture de la mairie).

Il est donc possible que l'acte d'huissier de justice, bien qu'acte authentique, soit dressé hors la présence du signifié ou de l'un de ses proches. Il convient de préciser que le point de départ de l'authenticité de l'acte est la remise assortie des conditions de délivrance prévues par le code, ou le procès-verbal de recherches prévu par l'article 659 du nouveau code de procédure civile.

* Pour l'acte judiciaire

Le procès-verbal nécessite la présence concomitante des personnes entendues, du juge et d'un greffier.

Les décisions judiciaires peuvent être prononcée par défaut, par l'un des juges ayant participé à la décision, en présence d'un greffier pouvant ne pas être celui qui assistait à l'audience. La délivrance d'une expédition peut être faite par un troisième greffier.

2/ Les limites territoriales

Les conditions de l'article 1318 du code civil s'appliquent dans tous les cas d'actes authentiques, le ressort variant entre le territoire national (notaires, juges par exception, et l'arrondissement (huissiers de justice, juge d'instance).

3/ La régularité

Des pièces de procédure, notamment le registre d'audience qui est lui-même authentique, peuvent "sauver" la régularité d'un jugement et son authenticité (459 du nouveau code de procédure civile).

D - Les effets de l'authenticité

1/ sur le plan de la preuve

L'acte authentique fait foi jusqu'à inscription de faux (1319 du code civil) : sous réserve des limites du champ de l'authenticité.

2/ quant à l'exécution de l'acte

L'acte authentique peut être revêtu de la force exécutoire. C'est un des principaux effets qui distingue le contrat notarié du contrat sous seing privé.

Les actes d'huissier sont, pour la plupart des actes d'exécution des décisions de justice. Il faut souligner le cas particulier de l'apposition par l'huissier de justice de la formule exécutoire en matière de chèque.

S'agissant du jugement, l'autorité s'attache aux décisions contenues dans l'acte. Mais toute décision n'a pas force exécutoire. Elle doit n'être susceptible d'aucun recours ou bénéficier de l'exécution provisoire (504 du nouveau code de procédure civile).

3/ quant aux règles de conservation de l'acte et aux copies

Obligation de conserver l'acte pendant des délais variables selon la nature de l'acte
Particularité des règles de reconstitution (648 à 651 du code de procédure pénale et 1430 à 1434 du nouveau code de procédure civile)
Copies : 1435 à 1441 du nouveau code de procédure civile

4/ quant aux sanctions applicables

Le faux commis dans une écriture authentique est puni ... (441-4 du code pénal)

Conclusion : quelle serait la place et le rôle de la certification électronique de l'acte authentique ?

Rappelons que l'acte authentique électronique existe par la réunion de trois conditions nécessaires et suffisantes :

1 - condition organique : l'acte juridique émane d'un officier public ou ministériel, d'un officier d'état-civil ou d'un greffier (1317 du code civil)
2 - condition formelle : cet acte doit être signé de cet officier public (1316-4 du code civil)
3 - condition matérielle : cet acte ressort de l'activité réglementée de la profession concernée

Mais l'acte électronique suppose l'intervention d'un tiers pour la certification. L'autorité de certification intervient dans le processus de la signature électronique pour garantir l'identité et la qualité du signataire, lui-même certificateur de l'acte.

On constate à l'examen des conditions d'élaboration et d'opposabilité des différents actes authentiques que les signatures sont essentielles à leur validité même et que les règles varient selon les actes mais surtout, pour les mêmes actes, selon qu'il s'agit d'un original ou d'une copie.

Sur certains actes, il est possible de rencontrer plusieurs signatures (constat signé par le clerc habilité au constat et par l'huissier de justice ; jugement signé du juge et du greffier). En revanche les copies, authentiques et exécutoires, ne nécessitent plus qu'une seule signature.

Quel que soit le document authentique considéré et sa forme, il ne parait pas concevable aux membres du groupe que s'ajoutent aux contentieux qui peuvent naître avec les actes authentiques des litiges sur la certification.

Cette observation appelle des questions sur la place et le rôle de l'autorité de "certification".

La directive européenne place le certificateur dans une situation indépendante par rapport à celui qui délivre l'acte. Pour autant, il n'est nullement imposé qu'il s'agisse d'un organe privé, sauf à confondre ce certificateur et l'opérateur technique, certes incontournable pour créer les algorithmes et mettre en oeuvre les procédures de sécurité en fonction de l'évolution des techniques.

Il est apparu essentiel à tous les membres du groupe que le certificateur soit une autorité publique. S'agissant d'un acte authentique, expression de la puissance publique par les effets qui s'attachent à cet acte -forces probante et exécutoire- et le contrôle rigoureux sur son auteur, lui-même autorité ou officier public ou ministériel, on ne peut concevoir que des intérêts privés interfèrent.

La présence d'un opérateur technique–ne saurait déposséder la puissance publique du contrôle exclusif sur l'acte qui lui incombe.

II – L'utilisation de l'acte authentique électronique (AAE)

A – Intérêt pour les professions concernées

1/ pour les avocats

Les cas d'application concernent principalement les relations entre professionnels. La transmission d'actes authentiques sous signature électronique apportera 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 nouveau code de procédure civile).

La mise en état permanente est un exemple de gestion informatisée et de communication électronique entre avocats et le tribunal. Le plus souvent, il ne s'agit pas d'actes authentiques mais de "bulletins" de mise en état, lesquels ne sont pas des actes de procédure au sens strict, visés par le nouveau code de procédure civile. Cependant même ces "bulletins" prétoriens constituent sous forme électronique la matérialisation par un mandataire autorisé -héritier doit-on rappeler de l'officier ministériel qu'était l'avoué au tribunal- du mandat ad litem qu'il a reçu de son client. En outre, la transmission électronique pourrait porter sur les actes de procédure tels que l'assignation, la constitution, les conclusions des avocats.

Il apparaît ainsi essentiel de prévoir une "validation électronique de la signature des avocats", représentant leurs clients.

La transmission des jugements, qui serait l'aboutissement de cette communication électronique, n'est pas encore pratiquée, même pour de simples copies, sinon à titre expérimental.

Le tribunal de grande instance et le Barreau de Bordeaux ont été précurseurs dans le domaine de la mise en état permanente.

L'expérience de mise en état permanente à Bordeaux remonte aux années 80. Le système alors mis en place pour la chambre des accidents de la circulation (6ème chambre du tribunal) grâce au financement du Barreau de Bordeaux fonctionnait bien mais s'est heurté au faible équipement, à l'époque, des cabinets et aux transmissions de documents papiers. Chaque acte (constitution, dépôt de conclusions, demande d'incidents de mise en état, etc ...) générait une information de la, ou des parties adverses qui étaient invitées à répondre.

Dès réception de la réponse, la mise en état permanente permettait de prendre des décisions pouvant amener de la simple demande de précision aux parties, à la fixation avec clôture de l'audience, lorsque les parties étaient prêtes.
Bien évidemment, cela générait un gain de temps considérable puisqu'il n'était pas besoin d'attendre les mises en état périodiques pour faire avancer les dossiers.

Le Barreau de Bordeaux a repris, en collaboration avec les Barreaux de Versailles et de Rennes, il ya quelques mois de cela la même idée.

L'évolution des techniques et des équipements des avocats a permis l'élaboration d'un logiciel, en phase d'expérimentation, reprenant les schémas de la mise en état permanente. Le système est adaptable aux juridictions où il n'existe pas de mise en état mais simplement des contrats de procédure (pratique qui se généralise à l'instance, au commerce et aux prud'hommes).

Un autre projet, compatible avec celui du Barreau de Bordeaux, est en phase de validation par la structure dénommée Ediavocat et la Chancellerie. Il comporte un projet de communication avec certification de la qualité des intervenants avocats.

2/ pour les huissiers de justice

Pour la profession, l'acte authentique électronique est d'un grand intérêt, car il permet des relations plus rapides avec d'autres huissiers de justice ou des demandeurs (avocats ou autres) notamment dans des procédures aux délais courts (saisie attribution et dénonce, saisie conservatoire et dénonce, saisie des coffres -délai de 1 jour- notamment).

Il permet la conservation et la sécurisation de la signature de l'huissier de justice et facilite la conservation des minutes et leur archivage postérieur.

Il permet d'envisager un acte qui n'aurait pour support que des valeurs numériques, permettant ainsi des constatations de flux électroniques (constatations de flux circulant sur les réseaux).

3/ pour les tribunaux

Plusieurs juridictions s'équipent en moyens de gestion électronique de documents (GED).

L'expérience du tribunal de grande instance de Marseille dans ce domaine est appliquée aux minutes civiles. Elle se résume ainsi : 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.

Les minutes sont classées et constituent une garantie, outre une obligation légale en l'état, mais elles ne sont plus utilisées.
Cette situation qui prend en compte la dématérialisation désormais systématique de la décision judiciaire lors de sa dactylographie, du fait de son enregistrement sur un support électronique, tient compte d'un poids culturel fort en faveur du papier et des aléas des techniques informatiques, bien connus de l'institution judiciaire dans le passé.

En l'état de réticences qui subsistent face à un tout dématérialisé et aux questions de sécurité qui se posent, il apparaît que la pratique de la GED ne crée pas de risques excessifs : en cas d'échec technique la minute subsiste sous sa forme habituelle.

4/ pour les greffes de tribunaux de commerce

S'agissant de la tenue du registre du commerce et des sociétés, le souhait est exprimé de sa dématérialisation progressive.

En ce qui concerne les décisions judiciaires, la facilité de l'archivage électronique ne doit pas masquer les risques qu'il comporte, au moins pour les minutes. L'opinion émise rejoint les expérimentations de GED menées dans les services judiciaires. Le besoin de dématérialisation existe mais surtout au niveau de copies délivrées.

B - Quelques difficultés listées

Il est apparu utile de mentionner quelques unes des difficultés procédurales susceptibles de se poser dans le cadre de la dématérialisation des actes.

1/ en ce qui concerne les actes judiciaires

- le visa des conclusions dans le jugement prévu par l'article 455 du nouveau code de procédure civile dans sa version issue du décret du 28 décembre 1998

Faudra-t-il numériser les conclusions visées, au moins lorsque le juge précise que les conclusions sont jointes à sa décision ? Quelle garantie aura-t-on d'une identité entre les conclusions sur papier et leur version numérisée ?

- comment procéder pour la mention de la décision rectificative sur la minute et sur les expéditions du jugement, prévue par l'article 462 du nouveau code de procédure civile

- d'autres mentions en marge peuvent être rencontrées :

- le cas le plus fréquent parait être la mention d'un appel en cours ou jugé, en marge d'un jugement

- les lois d'amnistie imposent de porter en marge de l'expédition de jugement délivrée en matière pénale la mention de l'amnistie (articles 21 et 23 de la loi du 3 août 1995 par exemple)
- la quittance et les pièces justificatives sont expédiées à la suite du jugement d'adjudication immobilière (721 et 713 de l'ancien code de procédure civile)

- le cas de l'article 465-1 du NCPC ne parait pas faire difficulté : lorsqu'un jugement fixe une pension alimentaire ..., les parties sont informées par un document joint à l'expédition du jugement des modalités de recouvrement ...

* il ressort de ces cas examinés que la question des mentions marginales nécessite un double examen, selon que le document initial est ou non numérique.

- la pratique de l'ordonnance sur requête (du tribunal de grande instance, du tribunal d'instance) peut rendre difficile la signature électronique.
D'une part on sait que les avocats présentent presque toujours 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'elle recevra la formule exécutoire si dans le délai d'un mois de sa signification il n'y a pas eu d'opposition (1410 nouveau code de procédure civile).

2/ en ce qui concerne les actes d'huissier de justice

La seule difficulté pourrait provenir des documents reçus (par exemple un jugement ou des pièces) qui ne seraient pas sous forme électronique. A ce jour, le scanner pourrait permettre de résoudre ces difficultés et ce serait l'image du document qui serait jointe à l'acte électronique.

Le visa des mentions de signification faites par le clerc assermenté, au retour de l'acte signifié, ne pose aucune difficulté, l'acte authentique électronique étant signé par l'huissier de justice en son office.

Les mentions de délivrance de l'acte sont intégrées à celui-ci, et font partie intégrante de l'acte authentique électronique et ne posent donc aucune difficulté.

Le destinataire de l'acte n'a aucunement besoin de posséder la signature électronique pour recevoir l'acte, et sa situation ne change rien à la validité de l'acte authentique électronique.

L'acte sur support électronique pourra être facilement reproduit et délivré à toute réquisition de l'autorité judiciaire.

La conservation de l'acte authentique électronique ne pose aucune difficulté spécifique pour l'huissier de justice, qui conservera l'acte et donc son contenu au rang de ses minutes.

En conclusion, il n'est pas inventorié de réelles difficultés pour l'acte authentique électronique chez l'huissier de justice.

CONCLUSIONS PROVISOIRES DU SOUS-GROUPE DE TRAVAIL

1 - La certification de la signature des actes authentiques, prévue par la loi du 13 mars 2000, parait devoir être effectuée sous la responsabilité juridique d'une autorité publique habilitée à certifier l'identité de la personne signataire dans l'exercice de sa fonction.

Pour les huissiers de justice, cette fonction pourrait être confiée à la chambre nationale. Celle-ci certifierait que telle personne est huissier de justice dans tel arrondissement. A ses côtés, un prestataire technique fournirait la clef technique de certification, laquelle ne serait renouvelée qu'en fonction de questions techniques ou de sécurité.

Pour les greffiers de tribunaux de commerce, l'autorité de certification est nécessairement le greffier lui-même, seul titulaire de la délégation de puissance publique. Toutefois, cette autorité s'exerce sous le contrôle du ministère de tutelle lequel, par ailleurs, agrée l'opérateur technique appelé à intervenir et les choix techniques mis en oeuvre.

Pour les juridictions, la Chancellerie.

Pour les avocats, ce sont les ordres locaux qui sont maîtres du Tableau. Si l'indépendance des ordres appelle qu'ils soient les seuls au plan local à valider la qualité d'avocat, il apparaîtrait souhaitable, au plan de la rationalité et de l'efficacité, qu'une structure nationale, qui pourrait être le Conseil national des barreaux, rassemble et valide aux yeux des pouvoirs publics ces certifications.

Il est bien précisé qu'en toute hypothèse le technicien n'aurait pas accès à l'acte à authentifier.

2 - La signature électronique doit demeurer une possibilité et ne doit pas être imposée.

3 - La signature électronique parait plus aisée à mettre en oeuvre pour les copies des décisions judiciaires ; les minutes seraient conservées sur support papier en raison Des problèmes importants que posent leur complète dématérialisation.

4. La réflexion préparatoire au décret d'application de la loi du 13 mars 2000 et à l'acte authentique électronique

-Contribution de la profession d'huissier de justice-

Contribution de la profession d'huissier de justice à La réflexion préparatoire au décret d'application de la loi du 13 mars 2000 et à l'acte authentique électronique.

« Un huissier de justice agissant en vertu d'une délégation de la loi pour l'exécution d'un acte entrant dans ses attributions imprime à son acte un caractère authentique ».

L'article 1317 du Code de Procédure Civile édicte :

« L'acte authentique est celui qui a été reçu par officier public ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé avec les solennités requises ».

La profession d'huissier de justice dont les études utilisent des moyens informatiques depuis de nombreuses années est favorable à l'instauration de l'acte authentique électronique tout en gardant la possibilité de solutions mixtes, associant électronique et papier dans la chaîne d'établissement, d'exploitation et de conservation des actes authentiques, en n'imposant pas le tout-électronique, mais en laissant à ses membres la possibilité de choisir.

Pour aborder les solutions proposées par la profession, nous allons suivre le parcours d'un acte d'huissier de justice et envisager les possibilités de dématérialisation dans :

Sa conception, l'envoi à l'étude, la signification de l'acte à son destinataire (transformation du projet en acte authentique), sa conservation.

LA CONCEPTION

Le taux d'équipement informatique des études d'huissier de justice est proche de 100%. Les matériels et 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.

Faut-il une norme pour cette rédaction ?

En théorie, il paraîtrait souhaitable d'imposer une normalisation, c'est à dire un format d'encodage identique pour la conception de tous les actes authentiques électroniques. Mais, est-ce possible ?

Avec la diversité des systèmes, il faut sans doute préserver la liberté du choix notamment pour les officiers publics et ministériels, professionnels libéraux.

De plus, en considérant l'évolution permanente des techniques est-ce possible ?

Si l'on admet la diversité des formats d'encodage, il sera nécessaire d'édicter des prescriptions précises pour la conservation.

Pour respecter les textes sur les actes d'huissier de justice, l'acte une fois conçu électroniquement est édité et matérialisé en trois exemplaires :

1 exemplaire destiné à être délivré au signifié : la copie
1 exemplaire conservé à l'étude : la minute
1 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).

Si l'acte n'est pas établi depuis un dossier géré à l'étude de l'huissier de justice, il peut provenir de tiers (Cabinet d'avocat, étude d'avoué à la cour, étude de notaire, tout correspondant de l'étude, service juridique de la clientèle, contentieux etc.)

Dans ce cas, ces actes établis par des tiers peuvent être adressés aux études d'huissier de justice sous forme électronique.

Se pose alors la question de l'identité de l'expéditeur : elle sera alors garantie par la signature électronique. Il faudra assurer la sécurisation du réseau de transmission utilisé d'où mise en place de réseaux protégés, type intranet, extranet ou très sécurisés comme Atlas 400 etc. Certaines administrations ou professions utilisent déjà des réseaux fermés sécurisés et protégés et il conviendra d'organiser l'inter communicabilité (définition des modalités des conventions d'inter change) et créée les conditions assurant l'interopérabilité des diverses organisations de certification.

❖❖❖

Le projet d'acte établi électroniquement devra être remis à son destinataire, c'est la signification.

LA SIGNIFICATION

C'est l'activité première de l'huissier de justice énoncée dans l'ordonnance du 2 novembre 1945 :

« Les huissiers de justice sont les officiers ministériels qui ont seuls qualité pour signifier les actes et les exploits ... »

Il est donc nécessaire d'éditer sur papier l'acte pour qu'il soit remis au destinataire.

Cet acte doit être **signifié** à son destinataire en appliquant les articles 653, 654 et 655 du Code de Procédure Cicile qui édicte notamment que la signification d'un acte doit être faite à personne et si elle s'avère impossible l'acte peut être délivré soit à domicile soit à défaut de domicile connu à résidence.

La loi s'est donc attachée à réglementer le coté physique de la remise.

Cette remise ne peut donc pas être électronique.

La remise de la copie d'un acte d'huissier de justice à son destinataire exige donc une rencontre physique.

En effet, le vœu du législateur en la matière est que l'huissier de justice, personne qualifiée, officier ministériel, explique lors de cette remise les droits et obligations du destinataire bien souvent peu familiarisé avec les pratiques du monde judiciaire et les termes juridiques.

Il est donc **indispensable** que le contact demeure avec le signifié pour que l'oralité prévue par de nombreux textes puisse être exercée par le rappel verbal de certains articles.

L'acte d'huissier de justice ne peut être **banalisé**, par le simple envoi vers une boîte à lettres électronique.

De plus, la loi impose la confidentialité et à ce titre le destinataire possédant une simple boîte à lettres électroniques est exposé à tous les dangers bien connus d'Internet. Il faudrait aussi imposer à tous de manière égalitaire un réseau spécialement protégé pour permettre la transmission électronique, mais cela ne résoudrait pas la nécessité de la rencontre avec le destinataire indispensable pour attester qu'il a eu connaissance du fait judiciaire.

LA SIGNATURE

L'acte doit être signé :

- Sur la copie papier remise au destinataire la signature sera manuscrite
- Sur la minute et le second original la signature pourra être électronique.

Les technologies connues à ce jour doivent faire appel à des prestataires techniques très qualifiés et réglementées par le premier décret sur la signature électronique.

Cependant, la signature électronique de l'officier public et ministériel doit dépendre d'une autorité de certification légitime et propre à sa qualité.

C'est pourquoi la profession d'huissier de justice estime qu'à coté du prestataire technique, doit être instituée une autorité d'enregistrement et de certification qui pourrait être la Chambre Nationale des Huissiers de Justice qui, en raison de sa connaissance des différents installations et mouvements de ses membres, représente l'organisme légitimement habilité.

L'acte d'huissier, une fois sa copie remise au destinataire (la signification), le second original et la minute comportant toutes les mentions relatives aux modalités des significations sont signés électroniquement et sont devenus des actes authentiques.

LA CONSERVATION

Le second original : il va suivre la vie d'un dossier électronique qu'il soit géré par l'étude d'huissier de justice, par une juridiction ou par des tiers requérants ou correspondants.

Son mode de gestion électronique sera donc celui du dossier dans lequel il est déposé suivant un processus informatique propre à chaque partenaire et sous sa responsabilité.

La durée de conservation des archives et actes d'huissier de justice est fixée par le décret du 29 février 1956 modifié par la loi du 3 janvier 1979 et le décret du 3 décembre 1979 qui indique que les actes, exploits et procès verbaux établis en double original doivent être conservés par l'huissier de justice pour une durée d'au moins trente années. C'est le délai maximum visé par les textes pour toutes les pièces et documents produits ou détenus par une étude d'huissier de justice.

Après un certain temps de conservation de la minute dans le système électronique de l'huissier de justice que l'on peut estimer à six mois, un an, (durée raisonnable de bonne conservation « locale ») il y a lieu d'envisager les moyens d'archivage dans le respect de certaines recommandations, telles que celles contenues dans la norme Afnor NT Z42 013 qui décrit notamment les principes permettant de s'assurer que les systèmes sont bien conçus et que leur exploitation respecte des procédures répertoriées et sécurisées afin d'assurer l'intégrité et la fidélité des documents électroniques stockés ou restitués ainsi que la pérennité de l'archivage dans le cadre de la durée de conservation légale.

Il faudra mettre en œuvre un système d'archive interne ou externe en utilisant des techniques appropriées pour assurer toutes ces garanties.

S'il est externe, la prise en charge par un tiers spécialisé devra comprendre, outre les documents électroniques eux-mêmes, tous les éléments qui ont contribués à leur établissement : les formats d'encodage, logiciel de lecture, l'indication des périphériques de visualisation et d'impression et du matériel nécessaire etc..

Il appartiendra à ce prestataire spécialisé d'analyser l'ensemble des données transmises pour maintenir et restituer le document à tout moment. Les mêmes éléments devront être fournis en ce qui concerne la signature électronique pour permettre sa constante identification.

5. Dispositions applicables aux modalités de collecte et de diffusion pour les actes électroniques des tribunaux de commerce

-Contribution du Conseil national des greffiers des tribunaux de commerce-

CNG

Paris, le 22 janvier 2001

LES GREFFES DES TRIBUNAUX DE COMMERCE

LES REGISTRES DE PUBLICITES LEGALES
COLLECTE et DIFFUSION

DIFFUSION ELECTRONIQUE

- Article R 821-2-1 COJ (Décret n° 98-550 du 2 juillet 1998)

« Les copies délivrées par les Greffiers à titre de simple renseignement et relatives aux inscriptions portées aux registres de publicité légale dont ils ont la charge peuvent être diffusées par voie électronique dans les conditions suivantes :

- *Les informations sont diffusées directement par le greffe compétent. Toutefois, les greffiers peuvent s'associer au sein d'un groupement ayant soit l'une des formes autorisées par l'article L.821-1 du présent code, soit une forme associative. Ce groupement est chargé de centraliser les appels et de les orienter vers le greffe concerné. Les greffiers peuvent, dans les mêmes conditions, conclure aux mêmes fins des accords avec l'Institut national de la propriété industrielle pour les attributions de celui-ci ;*

- *Les informations ne portent que sur les inscriptions figurant, en application des textes législatifs et réglementaires, aux registres dont les greffiers assurent la tenue ;*

- *Les informations sont délivrées telles qu'inscrites aux registres ou sur les actes annexés, sans subir de traitement quelconque, sous réserve des dispositions prévues par l'acte réglementaire pris en application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. »*

Il ne fait pas de doute que la loi du 13 mars 2000 modifie considérablement la portée de ce texte puisque la diffusion par voie électronique ne pouvait porter, avant la promulgation de cette loi, que sur des copies à titre de simple renseignement dans la mesure où l'authenticité et l'intégrité desdites copies ne pouvaient être assurées.

Dès lors que suite à la loi du 13 mars 2000, la dématérialisation des actes garantira l'authenticité et l'intégrité des renseignements diffusées par les greffes, les copies délivrées ne le seront plus à titre de simple renseignement mais seront purement et simplement équivalentes aux documents papiers actuellement délivrés.

- **L'arrêté du 6 novembre 1981** relatif à l'automatisation de la gestion des greffes des tribunaux de commerce et des TGI statuant en matière commerciale (J.O.NC.21/11/1981) énumère, parmi les différents registres tenus par les greffiers, les REGISTRES PUBLICS suivants :

«- Le registre de commerce et des sociétés,

- *Le registre des agents commerciaux,*
- *Le répertoire des décisions en matière de règlement judiciaire, de liquidation des biens et de suspension provisoire des poursuites,*
- *Le registre relatif au privilège du vendeur et de nantissement sur le fonds de commerce,*
- *Le registre relatif au nantissement sur l'outillage et le matériel d'équipement,*
- *Les registres des nantissements des parts sociales,*
- *Les registres du privilège du Trésor et de la sécurité sociale,*
- *Le registre des warrants, de la publicité des contrats de crédit-bail, des protêts,*
- *Les registres d'immatriculation et d'inscription d'hypothèque sur les bateaux de rivière. »*

COLLECTE/DIFFUSION ELECTRONIQUE

R.C.S.	
COLLECTE	DIFFUSION
Décret n° 78-704 du 3 juillet 1978 relatif à l'application de la loi n° 78-9 du 4 janvier 1978 modifiant le titre IX du livre III du Code Civil. → Article 19 → Article 21 → Article 52 → Article 53 Décret (modifié) n° 84-406 du 30 mai 1984 relatif au registre du commerce et des sociétés.	Décret (modifié) n° 84-406 du 30 mai 1984 relatif au registre du commerce et des sociétés. → Article 67 et suivants Arrêté du 9 février 1988 relatif au RCS, Titre IV : la publicité du registre → Article 29 et suivants L'article 32 dispose, depuis 1984, que la publicité du RCS peut également s'effectuer sous forme de surveillance d'événements futurs par application de l'article 68 du décret.

PROCEDURES COLLECTIVES

COLLECTE	DIFFUSION
Loi n° 85-98 du 25 janvier 1985 (modifiée) relative au redressement et à la liquidation judiciaires.	Loi n° 85-98 du 25 janvier 1985 Décret n° 85-1388 du 27 décembre 1985 Décret 30 mai 1984 (Articles 35 à 39, 42, 71) Arrêté 9 février 1988 (Article 18) (MENTIONS D'OFFICE)

REGISTRES DES PRIVILEGES, NANTISSEMENTS et PUBLICITES DIVERSES

LOI DU 17 MARS 1909 RELATIVE A LA VENTE ET EN NANTISSEMENT DES FONDS DE COMMERCE : PRIVILEGE DU VENDEUR ET DU NANTISSEMENT DES FONDS DE COMMERCE ET FONDS ARTISANAUX.

COLLECTE	DIFFUSION
→ Article 24 et suivants (L 143-16 Code de Commerce et suivants)	Article 32 et suivants (L 143-23 Code Commerce et suivants)
Décret du 28 août 1909 portant règlement d'administration publique pour l'exécution des lois des 17 mars et 1er avril 1909 sur la vente et le nantissement des fonds de commerce.	

LOI N° 51-59 DU 18 JANVIER 1951 RELATIVE AU NANTISSEMENT DE L'OUTILLAGE ET DU MATERIEL D'EQUIPEMENT

COLLECTE	DIFFUSION
→ Article 10 et suivants (L 525-10 Code de Commerce et suivants	Article 12 et suivants (L 525-12 Code Commerce et suivants)
Décret n°51-194 du 17 février 1951 portant, en ce qui concerne les formalités d'inscription des privilèges, règlement d'administration publique pour l'application de la loi du 18 février 1951 relative au nantissement de l'outillage et du matériel d'équipement.	

NANTISSEMENT DE PARTS DE SOCIETES CIVILES

ARTICLE 1866 CODE CIVIL

COLLECTE	DIFFUSION
→ Article 53 du décret n° 78-704 du 3 juillet 1978.	Article 57 du décret n° 78-704 du 3 juillet 1978.

NANTISSEMENT JUDICIAIRE

Loi n° 91-650 du 9 juillet 1991 portant réforme des procédures civiles d'exécution.

Décret n° 92-755 du 31 juillet 1992 pris pour l'application de la loi du 9 juillet 1991.

PRIVILEGE de la SECURITE SOCIALE

Article L 243-4 du Code la Sécurité Sociale Article L 243-5 du Code la Sécurité Sociale
Articles R 243-46 à 58 et, Article R 612-5 du Code la Sécurité Sociale

PRIVILEGE du TRESOR

Articles 1920 à 1929 du code général des impôts Annexe II Article 396 bis

INSCRIPTIONS de CREDIT-BAIL

DECRET N° 72-665 DU 4 JUILLET 1972	
COLLECTE	DIFFUSION
→ Articles 1 à 6	→ Article 7

INSCRIPTIONS des CONTRATS de LOCATION Et des CONTRATS de VENTE ASSORTIS d'une CLAUSE de RESERVE de PROPRIETE

Article 115-1 de la loi n°94-475 du 10 juin 1994 relative au traitement des difficultés des entreprises modifiant la loi du 25 janvier 1985 relative au RJ et à la L.J. (Article L 621-116 du Code de Commerce)
Article 85-5 décret n°94-910 du 21 octobre 1994 modifiant le décret du 27 décembre 1985.

INSCRIPTIONS des PRETS et DELAIS de PAIEMENT AUTORISES par le JUGE-COMMISSAIRE

Article 40 de la loi n° 85-98 du 25 janvier 1985 Article 60 du décret 85-1388 du 27 décembre 1985.

TRANSCRIPTION des PROTETS de CHEQUES Et CERTIFICATS de NON-PAIEMENT des CHEQUES

Cf. Anciens articles 159 à 162 du Code de Commerce. (L 511-52 à L 511-55)

COLLECTE

→ Article 57 Décret-loi du 30 octobre 1935 unifiant le droit en matière de chèques et relatif aux cartes de paiement.

Décret n° 50-737 du 24 juin 1950 portant réglementation d'administration publique pour l'application de la loi n° 49 1093 du 2 août 1949.

COLLECTE	DIFFUSION
→ Articles 1 à 5 Décret 50-737	→ Article 6 et suivants D. 50-737

WARRANTS

WARRANT HOTELIER
LOI DU 8 AOUT 1913 MODIFIEE PAR LA LOI DU 17 MARS 1915

COLLECTE	DIFFUSION
→ Articles 1 à 4 (L 523-1 à L 523-5 Code de Commerce)	→ Article 6 et suivants (L 523-6 et suivants Code de Commerce)

WARRANT PETROLIER
LOI DU 21 AVRIL 1932 MODIFIEE PAR LA LOI DU 16 DECEMBRE 1992

COLLECTE	DIFFUSION
→ Articles 1 à 3 (L 524-1 à L 524-3 Code de Commerce)	→ Article 4 et suivants (L 524-4 et suivants Code de Commerce)

WARRANT INDUSTRIEL
LOI DU 12 SEPTEMBRE 1940 ; PROROGATION PAR LA LOI DU 31 DECEMBRE 1953

COLLECTE	DIFFUSION
→ Article 3	→ Article 5

B. CONTRIBUTIONS RELATIVES A L'ARCHIVAGE ET A LA CONSERVATION DES ACTES AUTHENTIQUES ELECTRONIQUES

1. Remarques de la Direction des archives de France sur la dématérialisation des actes authentiques

Remarques de la Direction des Archives de France sur la dématérialisation des actes authentiques

Rosine Cleyet-Michaud , chef du Service technique
Catherine Dhérent, chargée de mission pour les TIC
Gérard Ermisse, chef de l'Inspection générale

Le ministère de la Justice a mis en place divers groupes de travail en vue de la préparation des décrets d'application 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. La Direction des Archives de France est particulièrement sensibilisée et attentive aux sujets qui y sont évoqués car ils ont une importance considérable pour l'évolution de la collecte, de la conservation et de la communication des archives du pays.

Les sujets qui y sont traités soulèvent ainsi de sa part des remarques et questions.

Sur le plan strictement juridique, tout d'abord, l'un des deux décrets prévus est pris en application de l'alinéa 2 de l'article 1317 modifié du Code civil, prévoyant que l'acte authentique peut être dressé sur support électronique moyennant certaines conditions d'utilisation et de conservation.

Or, l'article 1317 du code civil est inscrit dans la section première « de la preuve littérale » du chapitre VI « de la preuve des obligations et de celle du paiement » du titre III « des contrats ou des obligations conventionnelles en général » du livre III « des différentes manières dont on acquiert la propriété » de ce code.

Il semble qu'il y ait consensus au sein du groupe préparant le rapport pour la préparation du décret « Actes authentiques », pour considérer que l'article 1317-1 concerne tous les types d'actes authentiques (procès-verbal de l'état d'avancement des travaux du groupe plénier au 12/12/2000). Cependant la Direction des Archives de France continue de s'interroger sur le point de savoir si l'article 1317 modifié s'applique de façon restrictive aux seuls actes authentiques portant sur les matières mentionnées au paragraphe précédent, c'est-à-dire essentiellement aux actes relatifs aux transferts de propriété et notamment aux actes notariés, ou, au contraire, de façon extensive à l'ensemble des actes authentiques visés par le droit civil ou la jurisprudence, par exemple aux actes d'état civil et aux minutes de jugement. Dans ce dernier cas, il semble **qu'il conviendrait que soit dressée la liste précise des actes authentiques concernés**.

L'interprétation de la volonté du législateur emporte en effet d'importantes conséquences quant à la mission réglementaire dévolue au Gouvernement : si la loi a entendu ouvrir la possibilité d'une dématérialisation limitée à une catégorie précise d'actes authentiques, seule

la réglementation relative à cette catégorie d'actes devra être modifiée, ainsi le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires. Si, en revanche, l'interprétation extensive de la modification de l'article 1317 du code civil doit être retenue, la tâche réglementaire sera de beaucoup plus grande ampleur et ne pourra notamment éviter de porter sur les responsabilités respectives de l'Etat et des collectivités territoriales en matière de conservation des actes authentiques dématérialisés.

En effet, **la conservation** de la majorité des actes authentiques **est aujourd'hui assurée pour le compte de l'Etat par les services d'archives des collectivités territoriales qui en assument le coût**. C'est ainsi que le premier original de l'état civil est à l'heure actuelle conservé définitivement par les communes de plus de 2 000 habitants (sauf dépôt volontaire aux Archives départementales) et versé aux mêmes Archives départementales obligatoirement au bout de 100 ans par les communes de moins de 2000 habitants. Le second original confié aux greffes des tribunaux, est versé par ceux-ci aux Archives départementales également à l'issue d'un délai de 100 ans. Les actes notariés, les minutes de jugements, sont eux aussi conservés aux archives départementales à l'issue du délai d'utilité administrative, dit « DUA ».

Dans le cas des documents électroniques, la référence à un lieu de conservation précis perd toute signification, puisqu'ils peuvent être transmis pour communication à l'administration, aux administrés ou aux chercheurs, selon des conditions déterminées dans leurs métadonnées. Il sera désormais possible d'envisager des lieux différents pour la conservation et la communication.

La dématérialisation des documents, de leur forme de conservation à long terme et celle à venir de leur communication, **est** donc **susceptible de remettre profondément en cause la structure institutionnelle de la politique d'archivage** en France, avec des conséquences directes sur l'équilibre existant actuellement dans ce domaine entre l'Etat et les collectivités territoriales : quelle que soit la solution retenue, **une concertation étroite avec ces dernières, à travers leurs organes respectifs, s'imposera en préalable à tout choix définitif**.

Le décret sur les actes authentiques ne peut rester au niveau des principes puisque ces modalités de conservation figurent dans les décrets d'application de la loi de 1979 qui deviendraient techniquement inapplicables. Le décret à venir devrait donc tenir compte de ces nouvelles réalités et envisager une nouvelle répartition des charges de conservation.

Cela paraît d'autant plus nécessaire **que l'archivage à long terme des documents électroniques pose, sans doute encore pour quelques années, des problèmes techniques et financiers importants**.

Chaque transfert de support, nécessaire en raison de l'obsolescence rapide de ceux-ci et des matériels de lecture, fait courir au document le risque, aujourd'hui encore inévitable, de perte de qualité et de données.

De plus, le coût de chaque migration est important. La migration des 4500 fichiers nationaux produits par l'INSEE ainsi que par les ministères de l'agriculture et des transports et qui sont archivés aux Archives nationales, a coûté 3 MF en 1996.

On doit donc se demander si les collectivités départementales et communales accepteront ou pourront toutes assumer dans des conditions optimales pour la garantie des données et de l'authenticité des documents d'Etat, le coût de leur archivage électronique, qui suppose notamment l'acquisition de matériels performants, le recrutement d'agents dotés des compétences spécifiques aujourd'hui encore quasi inexistantes, et le maintien d'un état de veille technologique permanente.

Afin de ne pas introduire une inégalité de traitement de la forme des documents, inégalité préjudiciable d'une part à l'accès du citoyen à l'information, d'autre part à la viabilité même du système de gestion électronique de ces documents, deux solutions pourraient être envisagées.

La première serait pour l'Etat d'apporter une assistance aux collectivités chargées de la conservation, assistance financière pour compenser le transfert de charge, et assistance technique pour assurer l'homogénéité du système.

La seconde solution, certainement la plus logique et la plus fiable, serait d'établir un **système national d'archivage** à long terme de ces données. La structure d'archivage est aujourd'hui communale ou départementale parce que la commune et le département sont les institutions les plus proches du citoyen. L'acte dématérialisé rend caduc ce critère puisque ce document peut être accessible rapidement de partout à tous.

En revanche, services d'archives communales et départementales sont depuis deux siècles des lieux de médiation pour les administrés et les citoyens. Nombreux sont ceux qui s'y rendent pour obtenir preuve de droits dans des démarches administratives ou pour des recherches scientifiques ou personnelles. **Quelque soit à l'avenir le lieu de conservation, elles demeurent des lieux idoines de communication** et **peuvent permettre aux citoyens qui ne seraient pas eux-mêmes équipés de matériel informatique, d'accéder à l'information**. Même s'ils ne devaient plus à terme conserver certains documents du fait de leur dématérialisation, **ces services d'archives** communales et départementales **peuvent aussi continuer à délivrer des certifications** lorsque le citoyen, au titre des lois de 1978 et 1979, le demande sur forme papier ou numérique, comme ils le font aujourd'hui. Pour les administrés intéressés, la communication ne se ferait qu'après délivrance d'une autorisation d'accès par l'autorité en ayant le pouvoir (par exemple les notaires pour les minutes notariales).

Maître Lambert a évoqué la création d'un Minutier national qui pourrait éventuellement accueillir les minutes notariales certes mais aussi des actes authentiques autres que celles-ci.

Une telle institution peut être un excellent site de gestion et de conservation sur le long terme. Toutefois, si elle était destinée à la préservation d'autres actes que les minutes, il ne faudrait pas lui donner le nom de Minutier trop connoté « notariat ». De plus, il serait indispensable que ce service national soit sous la tutelle des Archives de France. Il ne devrait en aucun cas être administré directement et uniquement par les notaires. Les Archives de France ont lutté pour faire reconnaître dans la loi de 1979 et ses décrets d'application, le fait que les minutes notariales sont des *documents publics* ayant leur place à terme dans les « dépôts publics », ce qui n'a pas été facile à faire accepter par les notaires. Depuis la loi de 1928, en effet, ils avaient obtenu que ces minutes soient considérées comme des actes semi-publics, ce qui a été constamment et violemment critiqué par le grand public, les historiens professionnels, les généalogistes, car les versements aux Archives départementales n'étaient faits que de haute lutte, certains notaires refusant l'accès de leurs études aux archivistes et aux chercheurs, d'autres même ayant dilapidé ce patrimoine national, voire l'ayant vendu.

Dans le cadre d'une dématérialisation, le moment et le temps de l'archivage doivent être différents de ceux de la gestion papier. **Les délais d'utilité administrative**, définis conjointement par le producteur et l'administration des Archives, **n'ont plus de raison d'être**. Ces délais n'ont en effet été fixés que pour éviter d'incessants aller et retour des documents entre le producteur qui peut recourir fréquemment à ses documents, voire les annoter, les compléter, pendant un temps plus ou moins long, et le service d'archivage définitif. Ce n'est qu'à expiration du délai que les actes authentiques sont, pour l'heure, versés aux Archives départementales.

Un acte dématérialisé peut être « archivé » dès qu'il est finalisé, c'est-à-dire immédiatement après validation pour un acte d'état civil, une minute notariale ou de jugement..

Il peut être communiqué au demandeur immédiatement si celui-ci est l'officier public producteur du document ou selon la loi en vigueur sur la communicabilité des documents s'il s'agit d'une autre personne. La copie pourrait ne plus être délivrée par le notaire producteur de l'acte, mais bien par ce service d'archivage national. En ce cas, le coût de la délivrance au public peut et devrait être très faible. Ce ne serait sans doute pas le cas si un Minutier central était géré par les notaires.

Ce système de service d'archivage national serait aussi intéressant pour celles parmi les études notariales, les juridictions dont les moyens sont peu importants. Il créerait une égalité de traitement, s'il était un service gratuit, comme ce serait raisonnable qu'il le soit puisque ce serait l'Etat qui archiverait la production qu'il considère comme régalienne. Il pourrait éventuellement même, sous certaines conditions, accepter l'archivage de documents dématérialisés produits par les collectivités territoriales.

Le Centre des archives contemporaines de Fontainebleau reçoit déjà les documents électroniques produits par les administrations centrales. On pourrait donc imaginer que ce service accueille des documents produits pour l'Etat dans les services déconcentrés de celui-ci ou par les officiers publics ministériels. Mais le statut actuel de ce centre semble peu compatible avec une telle mission. En effet, un tel service nécessite des moyens conséquents et souples : humains (le service devra être assuré 24h/24h) et financiers (veille technologique permanente et dynamique pour les supports de conservation et de sauvegarde). Il vaudrait donc mieux **envisager la création d'un établissement spécifique (établissement public ou autre) sous tutelle de la Direction des Archives de France**.

Il semble aussi souhaitable qu'avant la mise en application de la loi, soient **définies au plan national, les conditions d'élaboration de chaque type documentaire**. Une fois la dématérialisation envisagée à grande échelle, il est nécessaire que les solutions techniques retenues par types d'actes soient compatibles, voire uniques. L'Etat a toujours diffusé, voire imposé des modèles et formulaires. Il est d'autant plus nécessaire qu'il continue à le faire pour la forme électronique des documents et qu'il ne laisse pas les producteurs de GEIDE diffuser leurs propres solutions pour les documents d'Etat. Il est indispensable que ces modèles soient indépendants des plates-formes matériels et logiciels. Des « Definition Type Document » (DTD) ou des « schema » sous le format « Extended Markup Language » (XML) pourraient être diffusés au niveau national afin que chaque commune, chaque notaire ou chaque tribunal n'adopte pas une structure documentaire propre et afin que soient respectées des procédures précises d'archivage et le respect des conditions de communication.

En revanche, cela n'impose pas à tous les officiers publics de dématérialiser au même rythme et en même temps.

Enfin, il conviendra aussi de se pencher sur les processus et les conditions techniques dans lesquels pourront être dématérialisés les documents existant sous forme papier dans le cas où un producteur souhaiterait traiter sous forme numérique l'ensemble de sa production présente mais aussi passée. Cette numérisation a posteriori devra assurer l'authenticité et la fiabilité du document tout en en améliorant l'accès.

2. L'établissement et la conservation des actes authentiques dématérialisés : problématiques

-Note rédigée par
Mme Françoise BANAT-BERGER et
M. Yves RABINEAU-

L'établissement et la conservation des actes authentiques dématérialisés : problématiques[1]

Etat de la réflexion du sous-groupe sécurité et conservation, janvier 2001

Le sous-groupe de travail relatif aux aspects techniques de la dématérialisation des actes authentiques s'est réuni les 7 et 21 juin 2000. Lors de la première séance, le sous-groupe a entendu en qualité d'experts Jean-Pierre Teil (Archives Nationales) et Jean-Louis Pascon (Ministère de la Culture). Il s'est également déplacé sur divers sites pour apprécier l'état actuel des réalisations dans le domaine du stockage et de la conservation à long terme des documents électronique (CNES à Toulouse, service central de l'état civil de Nantes, service de l'état civil de Strasbourg, conseil des greffiers des tribunaux de commerce, INSEE –*voir en annexe à ce document, les différents comptes rendus de visite rédigés par Françoise Banat-Berger*)

Le sous-groupe a tenté de procéder au recensement des difficultés soulevées, en retenant une distinction entre la phase de conception des actes, de celle de leur exploitation et de leur conservation.

Sur ces deux grandes catégories de difficultés, le sous-groupe s'est ensuite efforcé de dresser un premier état des solutions techniques disponibles ou susceptibles de le devenir à brève échéance.[2]

1- L'établissement des actes authentiques

Le sous-groupe a estimé que son étude devait envisager l'hypothèse de l'acte électronique au sens strict du terme, c'est à dire un acte entièrement élaboré par voie électronique et non par une simple numérisation d'un acte établi sur support papier.

Dans cette hypothèse, l'établissement d'un acte authentique devrait logiquement obéir au schéma suivant

Phase 1 : saisie du document par le biais d'un logiciel de traitement de texte

A ce stade, les modalités de production du document sont sans incidence sur son traitement ultérieur ; il n'est donc pas nécessaire de retenir une norme ou des procédures particulières. Il importe peu que cette production soit générée par un progiciel ou qu'elle soit le simple fruit d'une frappe « au kilomètre »

Phase 2 : transfert du document dans un format d'échanges

A cet égard, il sera essentiel de retenir un format standardisé (non-propriétaire) et transparent, aussi ouvert que possible pour faciliter les échanges. La transparence du format est indispensable pour garantir au futur signataire qu'il n'existe aucune donnée ou instruction cachées dans le fichier qu'il valide.

C'est le format XML qui, bien qu'encore non stabilisé[3], semble pour l'instant présenter le plus d'avantages ; retenu par la plupart des experts comme le format qui devrait s'imposer dans les dix prochaines années, il est d'ailleurs préconisé par les instances interministérielles de veille

---

[1] *Ont participé à ce groupe de travail : Françoise Banat-Berger, Jean Berbineau, Jean-François Blanchette, Laurent Perdiolat, Yves Rabineau.. Cette note a été rédigée par Françoise Banat-Berger et Yves Rabineau*

[2] Voir également la note de I. Guyon-Renard et de L-D Hubert : « *Eléments pour une pré-synthèse* », dans laquelle la réflexion est menée sur l'établissement, l'exploitation et la conservation des actes de l'état civil.

[3] Voir l'étude parue dans le cadre du groupe de travail sur les actes authentiques de Jean-François Blanchette : « *Matérialité de l'acte authentique électronique : encodage, signature, archivage* », 11 décembre 2000.

technologique, telle que la MTIC Sur l'émergence du format d'échanges de données XLM, voir http://www.mtic.pm.gouv.fr/XML/, ainsi que ainsi que les travaux du groupe LEGAL XML

* il permet de distinguer le contenu de la forme et de la présentation.

* il se présente sous la forme d'un texte brut encadré par des balises ordonnées hiérarchiquement suivant les spécifications de DTD (définition type de document) ou un schéma XML [ensemble de règles pour définir la structure et l'articulation des informations d'un document XML] : les actes authentiques se prêteraient particulièrement bien à cette logique dans la mesure où ils obéissent eux-mêmes à des règles d'élaboration structurées et prédéfinies.

* il est directement lisible par l'homme au prix d'un certain effort. Sa représentation est très simple dans la mesure où il contient uniquement un texte et des balises, à l'exclusion de toute macro-commande dans laquelle pourrait être dissimulée un virus ou des données cachées qui viendraient modifier le document après archivage.

* enfin, il peut être obtenu à partir d'un traitement de texte standard.

Certains intervenants ont exprimé leurs réserves vis à vis de ce format, considéré comme trop complexe et ne permettant pas de garantir une restitution visuelle unique des données conservées. Certes, l'utilisation d'un format « image » tel que les formats Jpeg, Tiff ou Pdf ne présente pas cet inconvénient. Mais de tels formats correspondent à une approche réductrice de la notion d'acte électronique :

- il s'agit en pratique de la numérisation d'un document « papier » et non de la création d'un document électronique dématérialisé.
- Les formats considérés sont pour la plupart des formats « propriétaire »
- De tels formats présentent des inconvénients au stade de l'archivage, dans la mesure où ils sont très consommateurs en espace- disque
- Ils sont plus compliqués à interroger et ne permettent pas la délivrance automatique de simples extraits

A l'inverse, le choix d'un format « image » présente l'avantage de permettre, dans une phase intermédiaire qui durera nécessairement longtemps, de préserver, à côté d'une production « tout électronique », la possibilité d'une élaboration « tout papier » des actes authentiques, tout en unifiant les modes de stockage, de conservation et de délivrance ultérieure des actes. Il suffirait en effet de procéder à la numérisation par scanner des actes établis selon un mode traditionnel pour les convertir dans un format image, identique à celui des actes élaborés par voie électronique et convertis directement en mode image.

Phase 3 : Intervention des signatures électroniques exprimant l'accord des parties lorsque ces dernières ne sont pas physiquement présentes lors de l'élaboration de l'acte authentique :

- En règle générale, chaque signature du document (que ce soit au moment de son établissement ou de son exploitation –voir ci-dessous) devra être complétée par un horodatage (qualité du tiers qui assurera ce service ?), permettant d'une part, notamment lorsque le consentement des parties n'est pas exprimé par une présence physique devant l'officier public, de s'assurer de la validité de la signature au moment où elle aura été utilisée et, d'autre part, de reconstituer l' « historique » du document.

Le futur décret d'application de la loi du 13 mars 2000 portant transposition de la directive européenne du 13 décembre 1999 s'appuie sur les technologies liées aux infrastructures à clé publique. On partira par conséquent de cette hypothèse là, même si on peut s'interroger sur l'absence de prise en compte d'autres procédés (signature biométrique, signature-tatouage), alors même que, s'il semble bien que « la signature cryptographique soit idéale pour s'assurer de l'intégrité d'un document qui transite au sein d'un réseau

ouvert[...], elle impose une infrastructure de gestion de clés très lourde »[4], *notamment s'il s'agit de permettre la pérennité dans le très long terme de ces clés*[5].

Il appartiendra à l'officier public de s'assurer auprès des prestataires de service de certificats que ces signatures sont toujours valables, avant d'apposer lui-même sa signature. C'est une mission nouvelle pour lui, mais qui s'apparente à celle qui lui incombe déjà en matière de contrôle de l'identité des parties à l'acte.

Dans l'hypothèse où les parties sont présentes lors de l'élaboration de l'acte, leur signature électronique ne semble pas indispensable. C'est en effet le rôle de l'officier public de s'assurer de leur identité et de leur consentement à l'acte.

Phase 4 Intervention de la signature électronique de l'officier public, qui donne à l'acte son caractère authentique

Le prestataire de service auquel s'adressera l'officier public pour se faire délivrer un certificat doit être, du point de vue du sous-groupe de travail, un organisme d'Etat, dans la mesure où, par essence, l'officier public ou ministériel agit au nom de l'Etat.

Phase 5 : délivrance d'une copie aux parties : les parties devront pouvoir obtenir alors un support électronique (disquette, Cd-Rom) sur lequel sera enregistré le document au format XML (ou tout autre format électronique) avec ses signatures électroniques. Au besoin, une copie papier portant la signature manuscrite de l'officier avec son sceau, pourra également leur être délivrée.

Phase 6 Les modifications ultérieures (voir la partie suivante) pouvant affecter par la suite l'acte d'origine ne devront pas altérer celui-ci : il faudra donc utiliser une méthode permettant de générer des liens entre la modification et le document originel , ce qui implique des modes de conservation nouveaux (voir plus loin). Chaque modification devra faire l'objet d'un horodatage.

2- L'exploitation des actes authentiques

2.1 Quelques éléments de réflexion sur lesquels s'appuyer en matière d'archivage à long terme de documents électroniques

Le passage d'un support papier à un support électronique pour la conservation des actes authentiques génère des risques importants de déperdition que seuls des moyens techniques lourds et coûteux permettront d'écarter. Certes le support papier est fragile et se dégrade avec le temps, mais la reproduction et la lecture des données qu'il contient ne demande aucune technologie particulière, ce qui nous permet de continuer à exploiter des documents édités il y a plusieurs centaines d'années.

En revanche, la survie d'un document dématérialisée est conditionnée par une maintenance et une veille technologique permanentes. Régulièrement, le document doit migrer d'un support à un autre, voire d'un format à un autre, et ce dans le respect de procédures lourdes et contraignantes s'appuyant notamment sur des exigences de sécurité importantes (sauvegardes...), sur l'obligation de conserver une traçabilité complète de toutes les opérations techniques effectuées sur un document (élaboration et maintien d'une méta-documentation aussi complète que possible), sur l'importance des audits et des tiers archiveurs. Pour n'avoir pas pris en considération ces contraintes, de nombreuses organisations, parmi les plus performantes (Cf la NASA) ont déjà pu déplorer la perte irrémédiable de données en raison d'une évolution technologique non anticipée ou d'un choix erroné dans le type de support utilisé.

De nombreux travaux ont été déjà publiés sur la question de l'archivage électronique et des démarches de normalisation sont en cours :

---

[4] *Idem*, chapitre 3 sur la signature.

[5] On remarquera d'ailleurs que le groupe travaillant sur la dématérialisation de l'état civil prend à l'inverse comme hypothèse de travail non une signature électronique mais une simple signature numérisée.

Voir pour une présentation synthétique des problématiques de l'archivage électronique, l'article d'Alison Bullock (bibliothèque nationale du Canada) sur la conservation de l'information numérique, 22 avril 1999 (http:/www.nlc-bnc.ca/pubs/netnotes/fnotes60.htm)

- Les expériences menées depuis une vingtaine d'années en matière d'archivage de fichiers statistiques par l'équipe Constance du centre des archives nationales de Fontainebleau (à ce jour, 6000 fichiers statistiques sont conservés et ont déjà subi deux migrations sur deux nouveaux supports). Voir également les fiches pratiques élaborées par le centre sur le traitement et la conservation des archives nouvelles constituées par l'électronique (version de 1999).

- ***La norme NF Z 42-013*** : une nouvelle version est actuellement étudiée et elle est proposée à l'ISO. L'ensemble des prescriptions qu'elle contient « *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* » (introduction). Elle se décompose en plusieurs parties, la plus longue consacrée aux moyens matériels et logiciels à mettre en œuvre, les autres traitant de la sécurité des systèmes, des procédures d'exploitation, du suivi des procédures, des audits, des tiers archiveurs et des prestataires de services. Des options sont prévues pour ceux qui veulent s'assurer d'un niveau de sécurité optimal.

  La norme traite uniquement des systèmes utilisant des disques optiques de type WORM (Write Once Read Many) dans la mesure où il est quasi-impossible sur ces supports d'effacer une information une fois qu'elle est enregistrée ou de la modifier de quelque manière que ce soit, sans que cette altération ne soit aisément détectable (entrelacement des écritures). Le choix d'un support minéral (disques en verre) garantit une durée de vie sensiblement supérieure aux solutions de type CD ou DVD (support plastifié).

  L'AFNOR devrait se pencher dans les mois à venir sur de nouveaux projets de normes intéressant directement nos travaux, puisqu'ils concernent notamment l'identification des supports et la traçabilité des modifications et des transferts de supports. Voir l'ouvrage paru en 2000 dans les collections de l'Afnor pratique : « Archivage électronique » par Jean-Louis Pascon et Isabelle Pottier.

- Les travaux menés sur le sujet par le DLM Forum : voir les actes du DLM Forum qui se sont tenus à Bruxelles les 18 et 19 octobre dernier (http://www.dlmforum.eu.org)

- Le modèle de référence d'un système d'archivage ouvert (O.A.I.S.) qui a fait l'objet d'une norme ISO, élaboré par le comité consultatif pour les systèmes de données spatiales et qui s'applique principalement pour les organisations chargées de rendre l'information disponible à long terme

- L'appel à commentaires lancé par la MTIC au sujet de la conservation à moyen et long terme des documents et des informations électroniques (un guide est en préparation)[6]
  http://www.mtic.pm.gouv.fr/teleprocedures/

2.2 Pistes de réflexion pour l'archivage des actes authentiques dématérialisés

Les réflexions menées au sein du sous-groupe l'ont conduit à considérer que les contraintes techniques liées à la conservation et au stockage des actes électroniques auront certainement des conséquences importantes sur les attributions des officiers publics en matière de conservation des actes authentiques, même dans la phase où ces documents ne sont pas librement communicables (au-delà de ce délai, 30 ans pour les jugements, 100 ans pour les actes notariés et les actes d'état- civil, les documents sont versés dans les services publics d'archives départementales). De la même façon, il semble indispensable de s'interroger sur la règle qui prévoit le dépôt

[6] Ce guide a été présenté lors d'un séminaire organisé par la MTIC le 25 janvier 2001. Les exposés présentés confirment les orientations de ce présent rapport.

d'un double des actes d'état- civil au greffe du tribunal [7], ou encore sur celle qui prévoit que les notaires déposent un double de leur répertoire au greffe du tribunal.

En effet, la conservation et la mise à jour sur des délais pouvant être très longs (des mentions portées sur un acte de naissance papier peuvent s'étaler sur 100 ans voire plus) et la dématérialisation des actes imposant une technicité très poussée en matière de maintenance et de veille technologiques ainsi que de la conservation impérative des méta-données accompagnant le document, il semble réaliste de centraliser le stockage des documents au sein d'organismes publics qui assureront les fonctions d'exploitation des données et des méta-données. On peut alors imaginer des services centraux propres aux principales catégories d'actes authentiques :

Un service central de l'état civil
(sur le modèle de l'actuel service central de l'état civil des étrangers de Nantes)
Un minutier central pour les minutes notariales
Un minutier central pour les minutes des jugements.

On peut aussi imaginer des services de ce type à l'échelon régional (cadre des régions, des cours d'appel).

L'officier public externaliserait en quelque sorte cette fonction de stockage, ce qui ne ferait éventuellement pas échec à ce qu'il conserve un monopole dans la délivrance des copies, les nouvelles technologies de la communication permettant de lui garantir un accès permanent aux données conservées à distance, qu'il s'agisse des actes « bruts » ou des méta-données permettant de recenser les événements postérieurs à son établissement qui affectent son contenu.

Cette organisation présenterait l'avantage de simplifier le travail des officiers publics dans ses aspects techniques et permettrait à des producteurs disposant de moyens modestes (par exemple les mairies rurales en matière d'état civil) et ne possédant pas d'une capacité technique élevée de faire face aux contraintes et aux coûts induits par une dématérialisation des supports et les transferts technologiques imposés régulièrement par l'évolution des modes de conservation.

L'ensemble des officiers publics devra par conséquent pouvoir avoir accès aux bases de données des services centraux compétents, les accès étant sécurisés et la gestion de ces accès étant assurée par les services centraux (afin de s'assurer de l'origine des demandes, de l'authentification du demandeur, des habilitations et radiations).

Le schéma serait alors le suivant :

- Transfert immédiat de l'acte muni de la signature de l'officier public par réseau informatique sécurisé aux services centraux chargés de l'exploitation de l'acte. Sont alors garanties l'origine et l'intégrité du document durant le transfert. La reproduction de la signature électronique des parties n'est plus indispensable à ce stade, puisque l'officier public est le garant de leur intervention . Au plus, il pourrait lui être imposé une obligation de représenter les signatures en cas de litige ultérieur

- La solution qui semble ensuite la plus raisonnable consiste pour le service central, afin de n'avoir pas à assurer la pérennité des clés provenant de plusieurs centaines de propriétaires (officiers publics concernés et éventuellement parties), à re-signer l'acte reçu immédiatement avec *sa propre clé*, la gestion des clés de ces services étant assurée, comme pour les officiers publics, par un organisme de l' Etat . Ce sera donc à ces services centraux de s'assurer de la pérennité de leur système de signature en révisant périodiquement leurs clés.

- Cette méthode suppose que la signature électronique ne soit pas accompagnée par un processus de chiffrement, dont l'intérêt est limité s'agissant généralement d'actes ne présentant pas un niveau de confidentialité imposant un cryptage, surtout si la liaison entre les officiers publics et les organismes centralisateurs est assurée par le biais d'un réseau sécurisé. L'existence d'un tel réseau, ainsi que le caractère fermé des transmissions entre officiers publics et services centralisateurs permet de s'affranchir par ailleurs d'une mise en place d'infrastructures à clés publiques,

- L'organisme récepteur assurerait alors une triple sauvegarde du document (méthode 2 + 1)

[7] La mise à jour des actes dans les greffes n'étant plus effectuées depuis 1987, en raison notamment de la centralisation du casier judiciaire à Nantes.

* Gravure d'un original et d'une sauvegarde sur un support de type Worm[8]. On peut imaginer un disque par producteur et par année qui serait clôturé annuellement.

* Une copie supplémentaire utiliserait la technologie dite COM (computer output microfilm) peu coûteuse, indépendante de tout matériel, d'une longue durée de vie, pour réaliser une image du document électronique et le stocker sur un film.

- Parallèlement, l'organisme aura la charge de la conservation des méta- données des documents, base de données qui, par les informations qui y seraient stockées, permettraient d'assurer la traçabilité de tous les événements pouvant affecter un acte : par exemple, les migrations, les délivrances d'une copie, les enregistrements de nouveaux événements affectant cet acte (« mentions marginales ») avec la création de liens entre l'événement, sa date et l'acte et l'enregistrement du numéro et de la cote des supports où cet événement sera gravé...

- Un partage des tâches reste à déterminer entre les officiers publics auxquels s'adressent les parties et les services centraux.

  Ainsi, l'officier qui aura reçu un acte portant modification d'un acte source, le transmettra au service central compétent qui l'enregistrera dans la base de données, procédera à son décryptage, à sa nouvelle signature, à sa gravure et à sa copie et mentionnera dans la base la localisation et la cote (sur le disque et sur le microfilm).

  En cas de délivrance d'une copie, plusieurs hypothèses peuvent être envisagées :

* Soit les parties s'adressent à l'officier public le plus accessible pour elles (proche de leur domicile[9], ou encore chargé de dresser un nouvel acte consécutif au premier) qui consultera alors la base de données du service central compétent (chaque demande devra être horodatée) qui lui permettra de connaître précisément la localisation de l'acte et de l'ensemble des événements ayant éventuellement affecté cet acte ; il aura alors la responsabilité d'en délivrer alors une copie conforme et exhaustive à partir des éléments dont il aura demandé le transfert au service central.

* Deux cas de figure se présentent alors : soit l'expédition sera faite sur un support papier et elle portera la signature manuscrite et le sceau de l'officier qui délivre l'acte, soit l'expédition est sur support numérique et elle portera la signature électronique de l'officier qui délivre l'acte. Dans ce cas, il faudra mettre en œuvre une infrastructure à clés publiques permettant aux usagers de s'assurer de l'origine et de l'authenticité des copies d'actes qui lui sont délivrées.

* Soit les parties s'adressent à l'officier public qui a établi initialement l'acte et c'est la même procédure qui est mise en œuvre.

- Au delà du délai légal actuel de conservation par les services centraux (30 ans pour les minutes des jugements, 100 pour les minutes notariales et les actes d'état civil) se pose le problème de la conservation à long terme des actes. Actuellement, c'est l'administration des Archives (direction des Archives de France du ministère de la Culture) qui assure, au terme de la loi du 3 janvier 1979, la conservation des archives publiques[10]. Toute la question sera de savoir s'il continuera à y avoir transfert de compétences entre des services centralisateurs et l'administration des archives, un problème supplémentaire étant posé par le délai de libre communicabilité de ces archives : 100 ans pour les minutes notariales et les actes de l'état civil (accès ouvert aux bases de données pour les actes de plus de

[8] Hormis les supports type CD-Rom et bientôt DVD-Rom en matière plastique, ont été mis au point des DVD longue conservation à substrat en verre et couches minérales sans polymères, dont les avantages tiennent moins à sa pérennité (des supports pouvant subsister sans altération plus de 100 ans sont inutilisables si on ne peut plus les lire) qu'à leur solidité et leur fiabilité. Ces supports ne sont pas encore commercialisés.

[9] Voir la note de I. Guyon-Renard et de L-D Hubert : « *Eléments pour une pré-synthèse* ».

[10] Voir note de Françoise Banat-Berger sur *les actes authentiques dématérialisés et leur conservation*, décembre 2000.

cent ans à tous les particuliers et gestion de ces demandes et satisfaction de ces demandes (délivrance de copies certifiées conformes).

- Les minutes des jugements posent un problème spécifique plus immédiat pour le service central compétent dans la mesure où une minute d'un jugement prononcé en audience publique est communicable immédiatement à quiconque en fait la demande (au terme d'un délai de 100 ans pour les audiences non publiques du moins pour les attendus du jugement).

Trois schémas d'organisation peuvent être envisagés à ce stade :

1- Confier la responsabilité de la conservation des actes dès leur établissement aux Archives de France, qui seraient responsables des services centralisateurs spécialisés selon les types d'actes et éventuellement déconcentrés

2- Prévoir des services centralisateurs relevant de la compétence de chaque département ministériel concerné (ministères de la justice, de l'intérieur, des finances) avec transfert des données aux Archives de France au terme des délais fixés par la loi du 3 janvier 1979

3- Faire définitivement assurer par les services centralisateurs la conservation à long terme des actes authentiques dématérialisés en écartant les Archives de France de cette mission.

Quel que soit le schéma finalement retenu, la dématérialisation des actes authentiques aura pour probable conséquence un bouleversement complet de la doctrine relative à l'archivage des papiers publics. Les contraintes techniques considérables qu'elle implique obligera en effet à revoir la répartition des responsabilités actuellement partagées entre producteurs et archivistes, selon la théorie des trois temps : le temps de la production (archives vivantes), le temps de l'exploitation (archives intermédiaires), le temps de la conservation à long terme (archives définitives). Avec les documents électroniques, la question de la conservation se pose dès la phase de création et l'intervention des autorités chargées de la conservation à long terme doit être anticipée.

En conclusion, il convient de bien mesurer les défis très importants posés par la pérennisation dans le temps de documents électroniques munis de signatures électroniques, qui émanent de producteurs variés ayant différents statuts (Etat, officiers publics ministériels, personnes privées --cas des documents déposés par les entreprises au greffe du tribunal de commerce qui sont eux-mêmes munis de signatures électroniques).

La conservation à très long terme de documents électroniques, sans aborder la question de la signature électronique, pose déjà un certain nombre de problèmes portant notamment sur la diversité des formats et des architectures qui rend complexe la portabilité des systèmes : en effet, on part en général d'une situation où l'informatisation a été mise en place à partir de formats « propriétaire » qui ne permettront pas toujours d'être exploités directement par d'autres applications. De plus, la signature électronique introduit une nouvel enjeu qui est celui de la pérennité des signatures.

Même si les problèmes techniques sont complexes, ils ne constituent pas l'essentiel des difficultés. Les enjeux sont avant tout d'ordre organisationnel. Or, il faut constater qu'aujourd'hui personne n'a la maîtrise des coûts (on sait seulement que ces coûts, si l'on veut assurer une prestation d'une qualité maximum en matière de sécurité des systèmes d'information, ce qui sera le cas pour les actes authentiques que l'on doit conserver pour une durée illimitée, seront extrêmement élevés).

Si une réflexion a été engagée chez certains acteurs du privé (experts comptables, greffiers des tribunaux de commerce, notaires, huissiers, avocats d'affaires...) visant à mettre en place une organisation permettant d'aller vers une standardisation des produits, une meilleure opérabilité, à ré-inventer des relations de confiance entre partenaires (mise en place d'une fédération nationale des tiers de service, de certifications croisées, d'annuaires communs...), cette réflexion est encore embryonnaire.

Enfin, si les services de l' Etat concernés par la mise en place de ces dispositifs savent que le vrai défi se situe bien au niveau de l'organisation, d'une harmonisation entre les formats, les différentes infrastructures de gestion de clés entre les ministères et leurs partenaires, rien n'a encore véritablement commencé pour la définition d'une politique commune de certification.

Yves Rabineau et Françoise Banat-Berger
Janvier 2001

C. COMPTES RENDUS DE VISITES

1 : - L'informatisation du service de l'état civil de Nantes (Ministère des affaires étrangères)

(compte rendu de visite)

- Note sur l'informatisation du service central d'état civil (SCEC)

(note de synthèse n° 256/DIR/EC))

L'informatisation du service de l'état -civil de Nantes

Un groupe de travail constitué par le GIP mission de recherche droit et justice à la demande de la directrice des affaires civiles et du sceau du ministère de la Justice, a été chargé d'élaborer un rapport sur la dématérialisation des actes authentiques (actes d'état civil, minutes notariales, minutes des jugements) à la suite de la loi du 13 mars 2000 sur l'adaptation du droit de la preuve et sur la signature électronique.

Cette loi prévoit en effet que la dématérialisation des actes soit étendu aux actes authentiques, dans certaines conditions devant être fixées par décret. Le rapport préparé par la mission droit et justice servira par conséquent de base à la réflexion accompagnant l'élaboration du décret. Il doit en effet donner des éléments de réponse autour de deux thèmes : l'adaptation à l'électronique du formalisme inhérent aux actes authentiques, les conditions de stockage et de conservation des actes authentiques.

Dans le cadre de ce groupe, une visite a été organisée au service central de l'état civil de Nantes dans la mesure où il s'agit du seul service d'état civil en France à avoir mené une réflexion très poussée sur la dématérialisation des registres et à avoir mis en œuvre cette dématérialisation.

Présentation sommaire[1]

Le service de l'état civil de Nantes (ministère des Affaires étrangères) créé par décret du 1er juin 1965[2] possède, outre des compétences propres liées à son statut de sous-direction d'administration centrale (diffusion de la réglementation, inspection auprès des postes consulaires ; rôle dans la réflexion sur l'évolution de l'état civil, notamment par le biais de la commission internationale de l'état civil (C.I.E.C.)[3] ; actions ponctuelles en direction de l'étranger), a un rôle spécifique en tant que service central de l'état civil proprement dit, pour tous les évènements d'état civil intervenus à l'étranger et concernant des ressortissants français.

C'est ainsi qu'il assume d'une part, un rôle en matière de délivrance et de mise à jour des actes transmis par les postes consulaires[4] : les actes dressés ou transcrits dans un registre dans le poste consulaire sont établis comme dans les communes en deux exemplaires et c'est le second exemplaire qui, chaque année, est transmis au S.C.E.C. (ainsi que le support magnétique, les actes étant de plus en plus majoritairement --entre 80 et 90% des postes- établis informatiquement par les postes consulaires). Les données sont alors récupérées et intégrées dans les bases du S.C.E.C.

Il assume, d'autre part, un rôle en matière d'établissement et de délivrance d'actes :

- le S.C.E.C. crée les actes de naissance et de mariage des étrangers devenus français par décret (naturalisés) ou par déclaration (notamment par mariage)
- pour les reconstitutions d'état civil : ressortissants des anciennes colonies ainsi que des anciens protectorats français, ainsi que pour l'Algérie[5], dont les actes ne seraient pas conservés au SCEC depuis l'accession à l'indépendance de ces pays.

---

[1] Pour un panorama complet des attributions du service central de l'état civil, voir le numéro 520 et suivants de l'instruction générale relative à l'état civil.

[2] Il a pris la suite de l'ancien bureau d'état civil consulaire.

[3] A initié notamment la réflexion sur les mentions marginales apposées par un outil informatique, qui ne reçoivent plus de signature , pratique fondée sur les dispositions de l'article 7-1 du décret du 3 août 1962.

[4] Ces actes sont dressés ou transcrits : pour les actes qui sont transcrits (sous une forme structurée au consulat après établissement par l'autorité locale), la transcription, qui n'est pas obligatoire, peut intervenir plusieurs années après l'événement (art. 7 du décret du 3 août 1962).

[5] Le S.C.E.C. a récupéré les microfilms des actes d'état- civil dressés en Algérie avant 1963, à l'issue de campagnes, l'une en 1964 et l'autre en 1971. En 1964, tous les actes des registres pris en compte dans la campagne ont été microfilmés ; dans la seconde, sous le contrôle des autorités algériennes, les actes concernant les personnes dont le nom avait une résonance arabe, ont été écartés. Il devait y avoir une troisième campagne qui n'a jamais eu lieu. Sur 5 millions d'actes dressés depuis 1830, 3,5 ont été microfilmés (avec une indexation par nom de commune, nature d'acte et année). A partir de cette production, le S.C.E.C. tire, à la demande, des

Informatisation du service

En raison des volumes considérables traités (6000 courriers qui arrivent en moyenne journellement, plus de 87000 actes établis par le S.C.E.C. en 2000, plus de 900 000 actes délivrés en 2000, plus de 110 000 mentions apposées en 2000...), leservice s'est lancé dès 1990 dans une opération massive d'informatisation, en commençant par l'informatisation des fichiers papier donnant accès aux actes provenant des postes consulaires.

Parallèlement, dès 1992, était implicitement acquis le principe que dès lors qu'un acte faisait l'objet d'une dématérialisation, seul l'acte dématérialisé faisait foi, ce qui entraînait comme conséquence que les registres papier étaient considérés comme définitivement clos et n'étaient plus tenus à jour. Les mentions sont par conséquent apposées (incrustées) sur l'acte « image » ou placées à la fin de l'acte « texte ».[6]

S'agissant de l'établissement des actes par le S.C.E.C, celui-ci reste conforme à la législation en vigueur dans les communes. En effet, est maintenue la pratique consistant à éditer les actes qu'il établit sur support papier pour y porter une signature manuscrite : après validation du projet par le demandeur, l'acte est validé informatiquement, immédiatement mis en ligne tandis qu'une sortie papier est réalisée, qui reçoit dans les jours qui suivent une signature manuscrite de la main d'un officier d'état civil. L'original ainsi réalisé est classé mais n'est plus exploité et mis à jour.

En revanche, pour les délivrances de copies et d'extraits d'actes conservés au SCEC de matière informatisée, c'est la signature manuscrite numérisée de l'officier d'état civil délivrant l'acte, qui est apposée, depuis le début de l'année 2000 sur l'acte dématérialisée, la sécurité du système reposant sur l'emploi de mots de passe propres à chaque officier, conservés non sur les postes de travail mais sur l'ordinateur central : le stylo a été remplacé par l'outil informatique sécurisé.

S'agissant de la numérisation des actes déjà conservés et exploités au SCEC sous forme de registres, la récente informatisation au SCEC a concerné majoritairement les registres des postes consulaires et a connu une très forte accélération avec une opération de numérisation de masse des anciens registres papier des postes consulaires, qui a démarré en 1999 : durant 16 mois, une société a travaillé dans les locaux du S.C.E.C. Environ 10 000 actes étaient numérisés quotidiennement, soit au final la numérisation de 3 millions d'actes en mode image. L'opération s'est faite en 3 étapes : numérisation des actes à partir des registres, découpe des actes et indexation par rapprochement avec la base de données réalisée à partir des anciens fichiers manuel[7]. Tout ce travail a été accompli par la société, sous le contrôle des titulaires du S.C.E.C., un contrôle a posteriori est effectué au flux par un système de déverrouillage des actes ainsi numérisés. C'est seulement à l'occasion d'une demande ultérieure sur cet acte que l'officier d'état civil en charge de la demande accède à l'acte verrouillé, vérifie son aspect, procède au « nettoyage » de l'acte (enlèvement des tâches, des scories diverses, repositionnement de l'acte qui gêneraient l'apposition ultérieure de mention)[8], valide l'acte qui est à ce moment là apte à la délivrance ou à la mise à jour[9].

---

photostats avec, si nécessaire, des mentions marginales qui y sont alors apposées, sur la base de pièces annexes que le S.C.E.C. archive également. Le S.C.E.C. conserve également les actes d'état civil des « optants » soit des français de droit local qui ont eu la possibilité d'opter pour la nationalité française durant plusieurs années après la guerre. Des reconstitutions d'état civil sont réalisés à la demande, pour ceux dont les actes n'ont pas été conservés, sur la base de pièces justificatives fournies par ces derniers (notamment des actes de notoriété).

[6] Les mentions les plus utilisées (une cinquantaine sur 175 structurées et standardisées dans l'instruction générale relative à l'état civil du ministère de la justice) ont fait l'objet de développement de logiciels adaptés pour faciliter leur apposition.

[7] Cette opération a coûté en totalité environ 10 millions de francs dont 7 donnés à la société (Ever), le ministère des affaires étrangères ayant entre autres acquis les droits du progiciel développé par la société.

[8] Toute trace est considérée par le système informatique comme du texte, sur lequel ou à côté duquel aucun autre texte ne peut être apposé. Cette sécurité sert à empêcher de frapper du texte par exemple sur une mention déjà existante.

[9] Actuellement, 900 actes environ sont déverrouillés par jour.

Actuellement, la quasi-totalité des registres des postes consulaire est numérisée. La numérisation est moins importante pour les actes provenant des anciennes colonies et de l'Algérie, en raison du manque de fichiers des références permettant un accès aux actes eux-mêmes et en raison de la plus grande complexité de l'état civil notamment pour l'Afrique : on compte 500 000 actes numérisés pour le fonds colonial (pays anciennement DPM-TOM avant 1960) et un nombre sensiblement équivalent pour l'Algérie (notamment les 85 000 actes des « optants »).

Pour la numérisation de ces actes (numérisation des flux, soit environ 600 actes par jour), la préparation par les services de l'état civil est beaucoup plus importante que pour les actes des postes consulaires numérisés en masse : la numérisation se fait soit, à partir des photocopies des pages des registres, c'est-à -dire à partir des photostats tirés des microfilms (ensuite photocopiés). Les termes à indexer sont indiqués au bas de la photocopie. Le travail de numérisation proprement dit puis d'indexation est réalisé par des vacataires sous le contrôle d'un officier d'état civil, soit un travail de nettoyage de l'acte numérisé et le « raccrochement » de l'image et de la fiche. La saisie de la fiche de référence[10] est réalisée par les officiers d'état civil des bureaux qui préparent les dossiers de numérisation.

Quant aux actes établis informatiquement quotidiennement, ils sont en mode « texte ».

Au total, on comptabilise 3,9 millions d'actes sous forme image et 1,6 sous forme texte, ainsi que 825 000 extraits sur un total de 15 millions d'actes conservés par le S.C.E.C. (6,5 millions possédant une référence informatique).

L'informatisation couvre ainsi :

- **la dématérialisation des actes de l'état civil**
- **la dématérialisation de la mise à jour des actes**
- **la dématérialisation du traitement de la demande d'actes de l'état civil [11]**
- **la dématérialisation de la signature des officiers sur les copies et les extraits**
- **la dématérialisation de l'accès aux fichiers (pour le parquet de Nantes, pour la cellule état civil consulaire d'Algérie), accès bridé uniquement pour la consultation.**

Configuration technique

Le SCEC fonctionne avec 2 ordinateurs centraux : un Bull DPS7000 GCOS7 pour le fichier des références d'actes (7 millions) et le fichier d'actes et d'extraits d'actes texte ; un serveur NT pour les images d'actes ; 300 P.C.

Toutes les données sont en ligne.

Des migrations des données n'ayant entraîné que des pertes minimes (auxquelles on a pu remédier en se reportant d'une part aux registres papier et, d'autre part, à l'historique de l'image), ont été effectuées, assurant le passage du support optique au support magnétique.

Le S.C.E.C. a réussi à avoir une parfaite maîtrise des logiciels et des fichiers, après quelques difficultés de départ, la société prestataire utilisant un format TIF qualifié par le chef de projet informatique de « trafiqué » : les formats choisis sont normalisés et ouverts (format TIFF normalisé CITT groupe IV pour les actes « image » et mode caractère pour les actes « texte ») ; l'indexation des fiches a été faite sur TAURUS.

De même, l'application permet de suivre la traçabilité d'un acte et de ses corrections, tandis qu'est constitué un fichier des mentions marginales (avec un historique sur une année).

---

[10] Portant les indications suivantes : nom et prénom, autres noms et prénoms, nature, date et lieu de l'événement, référence à partir de la référence du registre papier, lieu de naissance.

[11] Depuis 1997 a été développé d'une part le dépôt de demandes d'actes par minitel et, d'autre part, depuis 1999 a été introduit un procédé de lecture automatique (qui nécessite de nombreuses corrections manuelles, mais qui constitue néanmoins un gain de 50% du temps de traitement) des formulaires de demande 116/Ec . Des projets sont en cours pour utiliser le réseau intranet (pour les notaires notamment) et internet.

Chaque fois qu'une image est mise à jour, le programme relit image et sa fiche associée et avertit en cas de problème, la version de l'image –1 étant conservée en ligne.

En matière de sécurité, une sauvegarde partielle des images a lieu chaque nuit tandis qu'une sauvegarde totale est réalisée hebdomadairement et conservée dans un emplacement proche. Une réflexion a été engagée afin de pouvoir dupliquer le système entre Paris et Nantes[12] : le projet est très cher.

Le S.C.E.C. n'a toutefois pas obtenu de réponse aux questions posées aux archivistes sur les problèmes de l'archivage proprement dit des données qu'il gère. En effet, il est tenu par la réglementation de verser ses archives centenaires soit à la direction des Archives du ministère des Affaires étrangères à Paris (pour les actes des postes consulaires[13] ainsi que pour les actes provenant des anciens protectorats du Maroc et de la Tunisie), soit au Centre des archives d'Outre-Mer (Archives nationales) pour les actes dits coloniaux (Algérie comprise). C'est pourquoi, le S.C.E.C. a saisi la direction des Archives de son ministère pour organiser le transfert des documents numérisés ayant plus de 100 ans. Deux questions se posent à ce sujet : d'une part, jusqu'alors étaient envoyés aux Archives les registres dont la date de clôture avait atteint 100 ans. Dorénavant, le transfert s'effectuerait non plus en fonction des registres mais des événements (événements de plus de 100 ans). D'autre part, les modalités matérielles sont à définir : base qui reste à Nantes avec seulement un accès limité aux actes de plus de 100 ans pour la direction des Archives, ou, au contraire, site dédié aux évènements archivés où ces derniers seraient stockés ? A ce jour, la direction des Archives n'a pas répondu à cette saisine.

Conclusion

Les membres du groupe travaillant sur la préparation du décret d'application de la loi du 13 mars 2000 sur les actes authentiques, présents à cette visite, se sont émus d'une des conséquences de cette dématérialisation d'actes authentiques, à savoir que l'officier d'état civil qui délivre une copie d'acte, appose une signature numérique censée signifier l'adéquation entre l'acte qu'il voit à l'écran et l'acte original (notamment le registre papier). Or, il ne peut pas matériellement opérer cette vérification et il est ainsi amené à signer pour un acte qui a été « retouché » : détouré, nettoyé... en ignorant si ces manipulations ont par exemple pu entraîner par inadvertance la suppression d'une mention marginale.

Les responsables du S.C.E.C. rétorquent qu'il s'agit d'un faux problème, compte tenu des précautions prises lors de la numérisation des actes et du fait que le papier n'étant plus en lui-même un gage de sécurité puisqu'il n'est plus mis à jour après numérisation. De plus, des erreurs peuvent intervenir tout autant lors de la délivrance de copie sous forme de photocopies d'actes. Et finalement, depuis que l'informatisation est mise en place, les problèmes posés ont tous trouvé des solutions tandis que les usagers n'ont jamais émis de protestations quant à la qualité des prestations fournies.

Effectivement, le S.C.E.C., devant les demandes de plus en plus massives (+ 100% entre 1993 et 1999) auxquelles il ne pouvait plus faire face dans des délais satisfaisants, ne pouvait que se lancer dans l'automatisation de ses procédures, automatisation qui, certes, permet un traitement infiniment plus rapide, augmente la sécurité dans certains cas (des contrôles ayant été mis en place par les programmes informatiques, qui constituent un réel progrès) mais peut ne pas se concilier toujours pleinement avec le formalisme qui est censé accompagner l'exploitation d'actes authentiques.

Le service a mené cette informatisation avec prudence et en remplissant les conditions techniques qui pourront permettre à ces applications d'évoluer dans le temps et d'être pérennes. Le service a également été le promoteur d'une évolution dans le domaine de l'adaptabilité du formalisme entourant les actes authentiques aux nouvelles technologies : ainsi toute la réflexion juridique menée sur les mentions marginales apposées par un outil informatique et la signature numérisée.

Il était impossible de s'opposer à ces évolutions, de la même manière qu'il semble bien aujourd'hui que le seul verrou de la signature manuscrite des actes pour la délivrance est bien faible et devient absurde dans

[12] Afin de pouvoir, en cas de sinistre sur un des sites, re-démarrer le système sous les 48 heures.
[13] L'exemplaire conservé dans les postes est transféré après un délai de 100 ans au service des archives diplomatiques de Nantes.

le fonctionnement global de l'institution, pire peut conduire à des aberrations : on a vu que les actes validés informatiquement sont imprimés et signés dans les jours qui suivent. On peut imaginer que l'officier d'état civil ayant commis une erreur opère une modification sur l'acte en ligne et que la copie de l'acte papier qui serait envoyée ne soit plus la bonne... Toutefois, l'apposition de la signature numérique sur l'acte, si l'on considère qu'elle est une signature électronique au sens de la loi du 13 mars 2000, pourrait permettre de surmonter ces difficultés.

Bref, la loi du 13 mars 2000 et ses décrets d'application viendront à point pour le S.C.E.C. qui a les capacités pour achever son évolution. Ceci étant, ce qui vaut pour un important service à compétence nationale, assumant des missions centralisées et disposant d'importants moyens matériels et logistiques, ne vaudra certainement pas pour des services éparpillés dans tout le territoire : là encore, les solutions ne peuvent que provenir de la mutualisation des moyens, voire d'une certaine centralisation accompagnée de l'élaboration d'outils standards et ouverts communs à l'ensemble des services assumant les mêmes fonctions.

En effet, l'informatisation de l'état civil des mairies (voir les numéros 98-1 et suivants de l'instruction générale) est déjà très avancée, notamment pour les 600 mairies[14] avec lesquelles l'INSEE a mis en place des échanges dématérialisées des informations d'état civil[15]. Elle a été conduite par différentes sociétés sans que des normes à respecter pour permettre la pérennisation des données informatisées ne semblent préconisées par l'Etat[16]. Aujourd'hui, le décret d'application de la loi du 13 mars 2000 sur la signature électronique qui va sortir et dont les sociétés ont connaissance, a entraîné une effervescence de ces dernières proposant des produits basées sur les technologies à clés publique ainsi que, grâce à des portails internet, des mises en réseau des mairies qui utilisent le même produit, les transferts de données étant assurés par ces sociétés privées. Dans ces conditions, il semble urgent de prendre en compte cette situation en mettant en place des préconisations tendant à la sécurité des systèmes ainsi qu'à leur interopérabilité et à la pérennité des données et parallèlement, mettre en place des systèmes de contrôles et d'audit.

Françoise BANAT-BERGER

[14] Communes comptabilisant le plus d'actes de naissance.
[15] Décrets du 18 février 1998.
[16] En effet, les officiers d'état civil n'ayant pas eu l'autorisation de substituer la tenue automatisée de l'état civil à la tenue traditionnelle, les préconisations concernent uniquement la pérennité de l'édition des actes qu'ils ont établis de manière informatique.

MINISTERE DES AFFAIRES ETRANGERES — REPUBLIQUE FRANCAISE
Nantes le 26 juin 2000

DIRECTION DES FRANCAIS A L'ETRANGER ET DES ETRANGERS EN FRANCE
SERVICE CENTRAL D'ETAT CIVIL

NOTE DE SYNTHESE

N° 256 / DIR / EC

A/s : l'informatisation du Service Central d'Etat Civil

Le Service Central d'Etat Civil est engagé depuis une vingtaine d'années dans un processus d'informatisation. Le volume des archives à gérer et des affaires à traiter a orienté les choix en matière d'informatisation au cours de ces dernières années.

L'investissement du SCEC dans le domaine informatique se traduit par les chiffres suivants :

* 15 millions d'actes sont conservés et exploités par le Service Central d'Etat civil
  - 6,3 millions d'entre eux possèdent une référence informatique et
  - 5 millions d'actes sont informatisés
    - 3,5 millions sous forme d'image
    - 1,5 million sous forme de texte
  - 800 000 extraits d'actes sont mémorisés

* chaque année sont injectés dans le système informatique :
  - 80 000 actes dressés ou transcrits dans les postes à l'étranger
  - 100 000 actes établis ou reconstitués par le SCEC

* au cours de l'année 1999:
  - 204 000 mentions ont été apposées (dont 151 000 de façon informatique)
  - 1,4 million d'actes ont été délivrés (dont 75% de façon informatisée)
  - 2,3 millions de correspondances ont été expédiées

Cet effort d'informatisation a connu une très forte accélération avec l'opération AGATE de numérisation de masse des actes d'état civil :

cette opération a commencée au mois de mars 1999 et s'achèvera au mois de juillet 2000. Pendant cette période 3,5 millions d'actes de l'état civil auront été numérisés (3 200 000 en masse par la société prestataire de service SAFIG et 300 000 au flux par le SCEC), ce qui permettra d'atteindre un taux de délivrance informatisé de 85% .

L'une des conséquences de cette opération est l'abandon massif de l'exploitation des registres concernés au profit exclusif de l'informatique, que ce soit pour la délivrance ou la mise à jour des actes.

Ces quelques chiffres permettront de mieux appréhender le volume des tâches que le SCEC doit accomplir au quotidien et expliquent la recherche systématique de solutions informatiques pour pouvoir assurer la mission de service public dans un contexte d'augmentation constante des charges de travail depuis 1993 (doublement en 5 ans de 1993 à 1998 et poursuite de la forte tendance à la hausse depuis ces deux dernières années) conjuguée avec une réduction des effectifs au cours de ces dernières années.

C'est la raison pour laquelle la dématérialisation a pris plusieurs formes :

* la dématérialisation des actes de l'état civil

* la dématérialisation de la mise à jour des actes de l'état civil

* la dématérialisation du traitement de la demande d'actes de l'état civil

* la dématérialisation de la signature des officiers de l'état civil sur les copies et les extraits

* la dématérialisation de l'accès aux fichiers du Service Central de l'Etat Civil

Des fiches, jointes en annexe, décrivent de façon détaillée les différentes réalisations entreprises par le Service Central d'Etat Civil dans le cadre de sa modernisation ainsi que les pistes suivies pour ouvrir l'accès total ou partiel des informations qu'il détient aux organismes autorisés.

Le Service Central d'Etat Civil a privilégié la dématérialisation des supports pour mener à bien son informatisation : c'est ainsi que le traitement du papier est de plus en plus remplacé par des traitements informatiques depuis l'origine jusqu'à la délivrance proprement dite qui, elle, continue à se faire de façon traditionnelle sur un support papier qui est par la suite acheminé vers les usagers par voie postale.

Il n'est pas toutefois pas interdit de penser que la pratique actuelle pouvant paraître paradoxale du "tout dématérialisé" débouchant ... sur la production "classique" de papier évolue et qu'un jour la délivrance puisse être également totalement dématérialisée dans un contexte respectant à la fois la sécurité des informations transmises et les droits fondamentaux des usagers à la confidentialité (expédition d'une copie d'acte par internet par exemple)./.

Claude FAY
Sous-Directeur,
Chef du Service Central d'Etat Civil

LA DEMATERIALISATION DES ACTES DE L'ETAT CIVIL

Le Service Central d'Etat Civil conserve et exploite environ 15 millions d'actes. Parmi ceux-ci 5 millions sont informatisés. La dématérialisation des actes, initiée en 1985, peut se faire à deux moments différents : au moment de la création de l'acte (informatisation "directe") ou au moment choisit par le SCEC (informatisation "différée"), et relève de deux techniques différentes : conservation de l'acte sous forme de texte (récupération des données utilisées lors de l'établissement de l'acte via une application informatique spécifique) ou conservation de l'acte sous forme d'image (après numérisation de celui-ci à partir du registre).

Les actes informatisés du SCEC sont conservés de la façon suivante : 1,5 million d'actes sous forme de "texte" et 3,5 millions d'actes sous forme "d'image".

Les actes "texte" sont des actes dressés ou transcrits par les postes diplomatiques et consulaires dits "informatisés" et des actes établis ou reconstitués par le Service Central d'Etat Civil.
Sur les 262 registres d'état civil ouverts à l'étranger en 1999, 156 étaient tenus au moyen d'une application informatique développée par le Ministère des Affaires Etrangères et qui ont générés près de 90% des 80 000 actes dressés ou transcrits.
Les 100 000 actes établis ou reconstitués chaque année par le Service Central d'Etat Civil le sont tous au moyen d'applications informatiques spécifiques.
Dès que les actes "texte" sont intégrés dans le système informatique (versement annuel "millésimé" à partir du mois de janvier suivant pour les actes diplomatique et consulaires, et en temps réel pour les actes du Service Central d'Etat Civil) ils ne sont plus exploités que sur support informatique, le registre "papier" étant considéré comme une archive morte.

Les actes "image" sont des actes qui ont été numérisés au Service Central d'Etat Civil au moyen de scanners ou de caméras.
Il peut s'agir d'actes "isolés" dans un registre suivant la méthode dite du *flux*, c'est à dire l'informatisation d'un acte au coup par coup à l'occasion d'une délivrance ou d'une mise à jour afin de pouvoir l'exploiter plus rapidement la fois suivante.
Il peut s'agir de tous les actes d'un registre (sous réserve que chaque acte ne dépasse pas 3 pages en raison d'une contrainte technique de l'application informatique) soit à l'occasion de la numérisation systématique (depuis 1990) des registres diplomatiques et consulaires des postes non informatisés, soit lors d'opérations spécifiques en *masse* (projet AGATE notamment, qui devrait totaliser fin juillet 2000 près de 3 millions de nouveaux actes numérisés).
Dès que les actes "image" sont intégrés dans le système informatique (numérisation au flux ou en masse) ils ne sont plus exploités que sur support informatique, la version "papier" de l'acte n'étant plus utilisée ou mise à jour.

QUESTIONS JURIDIQUES :

- Valeur juridique de l'acte informatisé (voir § 2.1 de la note de la Conseillère juridique du SCEC)
- Conservation d'un second exemplaire sous forme de sauvegarde pour les actes informatisés (à l'exception des actes consulaires dont le premier exemplaire est conservé par les officiers de l'état civil en poste à l'étranger)

LA DEMATERIALISATION DE LA MISE A JOUR DES ACTES DE L'ETAT CIVIL

Depuis le début de l'année 1992, la pratique du Service Central d'Etat Civil en matière de mise à jour des actes "informatisés" a été la suivante : seule la version informatique (acte "texte" ou acte "image" avec, le cas échéant, l'extrait qui y est associé) est mise à jour au moyen des applications développées par le Ministère des Affaires Etrangères, la version "papier" de l'acte n'étant pour sa part plus mise à jour. Lorsqu'il existe seulement un extrait informatisé, le SCEC procède à une double mise à jour : de l'acte dans le registre *puis* de l'extrait informatisé).

Compte tenu du nombre important de mentions à apposer (204 000 en 1999) une application spécifique a été développée à cet effet en 1998/1999 de façon à standardiser et faciliter l'apposition des mentions les plus fréquemment utilisées. C'est ainsi qu'une cinquantaine d'entre elles, sur les 175 répertoriées dans le tableau des mentions, ont été structurées afin de n'avoir plus à saisir que les éléments variables du texte, le programme se chargeant de la mise en forme du texte intégral à apposer soit sur l'acte "image", soit à la fin de l'acte "texte".

Les mentions informatisées comportent, après le texte prescrit, les indications suivantes qui sont mises automatiquement : Nantes, le (date du jour de l'apposition). L'officier de l'état civil, (Prénom NOM). Elles sont donc "signées" de façon informatique, en effet le Prénom et le NOM correspondent à l'utilisateur, et à lui seul, ayant accédé à l'application en introduisant son mot de passe personnel et confidentiel.

Au début de chaque mois, un listing de toutes les mentions apposées le mois précédent est édité (présentation : classement par référence de l'acte sur lequel elles ont été apposées). Cette pratique étant à la fois lourde pour les services informatiques et pour les bureaux chargés d'archiver ces documents par ailleurs difficiles à exploiter, une nouvelle application sera prochainement développée et permettra un stockage informatique des mentions apposées (avec des possibilités de consultation par date d'apposition ou par référence), autorisant ainsi le "chaînage" des différentes mentions apposées successivement sur un même acte.

P.J. copie d'écran d'apposition de mention structurée et mention correspondante sur un acte "texte", sur un acte "image" et sur un extrait

QUESTIONS JURIDIQUES :

- L'absence de signature des mentions informatisées est autorisée par l'article 7.1 du décret du 3 août 1962

LA DEMATERIALISATION DU TRAITEMENT DE LA DEMANDE D'ACTE DE L'ETAT CIVIL

Compte tenu du nombre toujours croissant de demandes d'actes de l'état civil depuis l'année 1993 (1,4 million d'actes délivrés en 1999), le Service Central d'Etat Civil a exploré

différentes pistes pour faciliter et accélérer leur traitement, le fil conducteur étant de limiter autant que possible la saisie des informations nécessaires pour interroger la base de données.

C'est ainsi que fin 1996 / début 1997 le dépôt de demande d'actes via le Minitel a été rendu possible pour les usagers (3615 code SCEC). De quelques dizaines de demandes par jour au début, la progression de ce mode de saisine a été spectaculaire pour atteindre aujourd'hui plus de 1200 demandes par jour ouvré (25 402 demandes reçues au mois de mai 2000).

Depuis le début de l'année 1999, un procédé de traitement par lecture optique a été développé (sous forme de prototype) pour permettre la transformation des imprimés de demande 116/Ec en fichiers informatiques afin de pouvoir les injecter directement dans les applications de délivrance (traitement identique à celui effectué pour les demandes parvenues par le Minitel). Le nombre de demandes ainsi traité est en moyenne de 800 par jour ouvré depuis le début de l'année 2000.

Les demandes dématérialisées (à l'arrivée - Minitel - ou dès l'arrivée - Lecture optique) représente aujourd'hui un peu plus de 46% des demandes traitées au Service Central d'Etat Civil. Des projets sont en cours pour permettre dans un avenir très proche le dépôt des demandes par le réseau Intranet (celui des notaires notamment) et, sans doute vers la fin de l'année, par Internet. L'augmentation des capacités de traitement des imprimés 116/EC est programmée pour le 1er semestre 2001.

L'objectif du Service Central d'Etat Civil est de parvenir, à terme, à traiter de façon dématérialisée l'essentiel sinon la totalité des demandes d'actes qu'il reçoit dans une organisation où ne circuleraient plus que des données informatiques. Il serait alors tout à fait envisageable de généraliser les opérations de délivrance sur l'ensemble des officiers de l'état civil (soit une vingtaine de demandes par jour et par personne, compte tenu du niveau actuel de la demande et du nombre d'agents) : une fois la demande satisfaite, l'acte serait signé de façon informatique avant d'être l'imprimé sur un site centralisé lui même couplé avec un processus de mise sous pli automatique. Ainsi il n'y aurait plus aucune manipulation de papier par les officiers de l'état civil qui ne verraient même pas physiquement les actes qu'ils expédient.

J. imprimé 116/EC + copie des écrans de travail après traitement de la demande par lecture optique

UESTIONS JURIDIQUES :

- Mise à jour du dossier détenu par la CNIL contenant le détail des applications utilisées par le SCEC .

- Déclaration d'un fichier particulier en cas de création de fichiers de traitement sur la base de critères précis (par exemple, nature et motifs de la demande, adresse)

LA DEMATERIALISATION DE LA SIGNATURE DES OFFICIERS DE L'ETAT CIVIL

L'application informatique permettant d'apposer un tampon informatique comportant la signature numérisée de l'officier de l'état civil sur les copies et les extraits délivrés selon un procédé informatisé - ce qui revient à signer un document sans avoir recours à un stylo - est testée, à titre expérimental, par une vingtaine d'officiers de l'état civil du SCEC depuis le 1er décembre 1999. Les premiers résultats étant positifs, la généralisation à tous les officiers de l'état civil des bureaux de délivrance (130) a été entreprise au mois de mars 2000.

L'officier de l'état civil, après avoir accédé à l'application SAGA en introduisant son mot de passe personnel et confidentiel, peut désormais signer de façon informatique la copie intégrale ou l'extrait d'acte lorsque ceux ci figurent dans les fichiers informatiques soit sous forme d'image, soit sous forme de texte. Les informations suivantes sont contenues dans le tampon informatique qui est apposé :

* acte image (copie intégrale) :
- *cachet* "COPIE D'ACTE DELIVREE SELON PROCEDE INFORMATISE NANTES, LE ..... L'OFFICIER DE L'ETAT CIVIL"
- *signature numérisée de l'officier de l'état civil*
- *Prénom NOM*
- *sceau*

* acte texte (copie intégrale) et extrait :
- *signature numérisée de l'officier de l'état civil*
- *Prénom NOM*
- *sceau*

La sécurisation de l'application , de son accès et de son l'utilisation sont garantis par :

- la numérisation du spécimen de signature (signature identique à celle déposée au parquet général de Rennes) qui est effectuée par la Division PSI;
- la gestion des mots de passe individuels et des autorisations d'accès (détermination du profil de l'utilisateur) aux différentes applications qui est assurée par un bureau spécialisé du SCEC;
- le tampon informatique, qui ne peut contenir que l'identité d'un officier de l'état civil, n'est pas conservé sur le poste de travail en local mais sur l'ordinateur central afin de ne pas permettre à une autre personne de l'utiliser;
- les consignes strictes qui sont données aux agents en matière de protection de l'accès aux applications lorsqu'ils sont amenés à quitter leur bureau;
- l'officier de l'état civil qui s'assure du positionnement correct du tampon sur l'image de l'acte à délivrer par deux opérations de validation distinctes.

Cette dématérialisation de la signature autorise maintenant le SCEC à s'orienter vers une centralisation de tous les travaux d'impressions liés à la délivrance des actes, déchargeant ainsi les officiers de l'état civil des tâches fastidieuses préalables à la mise sous pli des courriers générés (vérification, signature, classement, adjonction d'imprimés, agrafage,...), leur permettant ainsi de pouvoir consacrer plus de temps à l'exercice de leur métier.

J. acte "texte" , acte "image" et extrait signés de façon informatique

UESTIONS JURIDIQUES :

- Voir contenu de la discussion avec le ministère de la justice sur la signature numérisée (§1.3 de la note de la Conseillère juridique du SCEC)

A DEMATERIALISATION DE L'ACCES AUX FICHIERS DU SERVICE CENTRAL DE L'ETAT CIVIL

Le Service Central d'Etat Civil a été conduit, dans le cadre de ses bonnes relations de travail avec des interlocuteurs institutionnels, à mener une expérience "d'ouverture sur l'extérieur " de ses fichiers (références + actes).

C'est ainsi que le Parquet de Nantes et la CECA (Cellule Etat-civil Consulaire Algérie), qui relève tout comme le SCEC de la Direction des Français à l'Etranger et des Etrangers en France, disposent d'un terminal dédié qui peut accéder au système informatique. Une application "bridée" ne permettant que la recherche, la consultation et l'édition des actes (sur papier "normal"), sans possibilité de modifier quoi que ce soit, a été développée et installée dans des conditions de sécurité maximum.

Cet accès "direct" permet à ces utilisateurs de pouvoir raccourcir de façon considérable les délais de traitement de leurs dossiers puisque l'information recherchée est disponible en temps réel. Il diminue d'autant le nombre de demandes que le SCEC doit traiter.

Le SCEC envisage d'autres pistes pour "partager" ses fichiers avec ses utilisateurs institutionnels :

* avec le Projet ESPOIR (Echange Sécurisé POur Inscription au Rnipp) qui permettrait à l'INSEE (et à la CNAV de Tours qui vient de reprendre le suivi du dossier), avec un transfert annuel du contenu des fiches relatives aux actes de naissances dressés ou transcrits dans les postes diplomatiques et consulaires au cours de l'année écoulée, de préaffecter des numéros d'identification aux ressortissants français nés à l'étranger..

* avec le projet BISES (Base Informative Structurée en Extraits Simples) qui permettrait de mettre à la disposition des utilisateurs institutionnels une base de données extraites des fichiers du SCEC correspondant, sauf exception qui serait précisée, aux informations contenues dans les extraits sans filiation.

Le but affiché du partage des fichiers ou des autorisations d'accès à ceux-ci (on pourrait imaginer la consultation, dans un futur "proche", des fichiers du SCEC par toutes les Préfectures et les postes consulaires) est de faire diminuer la demande d'actes et d'échanger des informations sur les dossiers en cours d'instruction. Ainsi, l'usagers verrait diminuer les délais de satisfaction à ses démarches administratives et la sécurité des documents délivrés s'en trouverait améliorée en raison d'une procédure réduisant les risques de fraude.

ESTIONS JURIDIQUES :

- S'agissant des recherches pour le RNIPP, l'autorisation du Parquet devrait être sollicitée

- Autorisations de la CNIL pour l'accès au fichier des références et des actes (voir §2.2 de la note de la Conseillère juridique du SCEC).

2. L'informatisation de l'état civil de Strasbourg

(compte rendu de visite)

L'informatisation de l'état civil de Strasbourg (visite du 3 janvier 2001)

Le contexte

Depuis une dizaine d'années, les services en charge de l'état civil[1] ont accentué leur action 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 : si la tenue de l'état civil est restée centralisée au sein de la mairie centrale, les mairies de quartier fournissent aux usagers des renseignements sur l'état civil, délivrent des copies et des extraits d'actes...).

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.

C'est dans ce cadre là qu'on peut replacer et comprendre l'informatisation de l'état civil à Strasbourg. Cette informatisation, comme dans la plupart de toutes les municipalités importantes (dans lesquelles on compte notamment des naissances) est également à mettre en corrélation avec l'incitation forte de l'INSEE qui, demande une transmission des données de l'état civil[2] aux mairies afin, d'une part de pouvoir réaliser des statistiques démographiques et, d'autre part de tenir à jour un certain nombre de répertoires (répertoire national d'identification des personnes physiques, fichier électoral, répertoire national inter- régimes des bénéficiaires de l'assurance maladie). C'est ainsi que l'INSEE peut attribuer des subventions[3] aux communes ayant dressé au moins 100 actes de naissance en 1996, qui auront réalisé des investissements nécessaires pour mettre en œuvre un logiciel de traitement de l'état civil agréé.

La coexistence support électronique/support papier

L'informatisation de l'état civil de Strasbourg remonte au début des années 1990 : a été choisi un logiciel spécifique élaboré par la société LOGITUDE, société de la région ayant d'autres références en matière d'état civil, le parti pris de départ ayant été de choisir le mode texte (et non le mode image grand consommateur en espace-disque). Les actes sont par conséquent saisis dans la base tandis que les actes des anciens registres papier sont re-saisis. Le logiciel respecte l'instruction générale de l'état civil (ainsi il est impossible d'introduire un nouveau numéro entre deux actes).

L'objectif est d'opérer la re-saisie totale de l'arriéré, les premières reprises ayant concerné les actes qui allaient être le plus demandés dans les années à venir. Cette 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 passé avec la même société depuis plusieurs années, la reprise étant également effectuée en interne dès lors que les agents en ont la possibilité. 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. Aucun acte ayant une valeur juridique ne vient sanctionner cette saisie et la conformité de l'acte saisi avec l'acte original sur papier.

Tout acte établi aujourd'hui est produit par le logiciel et fait l'objet de trois sorties sur papier sécurisé[4] qui sont alors signées d'une façon manuscrite. Pour les actes de mariage, le projet est établi au vu des

---

[1] Le service de l'état civil de Strasbourg est organisé autour des sections naissance / mariage / décès / registres (stockage des registres). Par délégation du Maire et de ses adjoints (le maire peut également déléguer cette fonction à certains conseillers municipaux ; la délégation ne peut concerner la célébration des mariages réservée au maire et à ses adjoints), les officiers publics d'état civil au sein du service ayant une délégation complète sont au nombre de 10 tandis que 80 ont reçu une délégation partielle (pour la délivrance des actes) notamment dans les mairies de quartier.

[2] Bulletins 1 et 1bis (transcription et mention en marge), 2 (mariage), 4 (reconnaissance), 5 (naissance), 6 (enfant sans vie), 7 et 7bis (décès). Les transmissions sont quotidiennes (bulletins 5 et 7 –avec certificat de décès), hebdomadaires (4 et 7bis), mensuelles (1,1bis, 2 et 6).

[3] Décret n° 98-92 du 18 février 1998 et arrêté du 2 mars 1998.

[4] Une pour la partie, l'autre pour le tribunal de grande instance, l'autre enfin qui sera intégré dans un registre et qui formera la collection originale des actes de l'état civil.

pièces fournies par les parties[5], enregistré puis édité[6]. Enfin, l'acte lui-même est établi la veille ou l'avant-veille du mariage et authentifié par les parties et l'officier d'état civil (maire ou adjoint).[7] Au retour de l'acte, les notifications sont faites dans les communes des lieux de naissance des époux ainsi que des enfants (en cas de légitimation pour des enfants nés hors mariage).[8] 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.[9]

Toutes les mentions marginales sont saisies dans la base (sans signature avec seulement la mention « officier de l'état civil délégué ») et, parallèlement, pratiquement simultanément la mention est apposée d'une façon manuscrite sur le registre contenant l'acte source et est signée par l'officier apposant cette mention (qui n'est pas le même que celui ayant entré la mention dans la base)[10].

Enfin toute délivrance (copie intégrale, extrait, extrait simplifié[11]) se fait sur support papier et est signé 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. Les erreurs sont rares : elles sont détectées par l'intéressé et une vérification se fait alors à partir du registre papier.

Difficultés liées à l'informatisation

La maintenance et l'évolution du produit sont assurées par la société Logitude, la mairie ne s' étant pas rendue propriétaire du produit.

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). Le passage d'une version à une autre est complexe, notamment lorsque l'évolution du produit entraîne un changement dans la structure des fichiers (correspondances malaisées à mettre en œuvre)[12]. Toutefois, ces problèmes ont été résolus et le service n'a pas encore constaté d'altérations ou de pertes des données.

L'expérience de Besançon est similaire : un premier logiciel élaboré en 1988 racheté par la Ville, sans aucune reprise d'antériorité. Le logiciel ne pouvant plus évoluer, le service a acheté en 1998 un produit de la société Arpège. Il y a eu par conséquent un gros travail de reprise des données nécessitant de nombreux contrôles ainsi que des vérifications à partir des registres papier, qui ont permis de déceler un certain nombre d'erreurs provenant de la première informatisation. Le prochain chantier du service de l'état civil de Besançon est la reprise de l'antériorité (documents antérieurs à 1988) et le choix entre le mode image (qui ne permet pas d'établir des copies mais uniquement des extraits) et le mode texte (plus fiable mais beaucoup plus long à mettre en place). Concernant l'arriéré, le service a pour l'instant uniquement informatisé les tables décennales.

En fait, les deux systèmes mis en place à Strasbourg et à Besançon ne peuvent pas communiquer entre eux (pas de compatibilité directe).

Ce problème est général à l'ensemble des mairies : les stockages des données[13] 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). Il semble **qu'une des priorités pour l'état civil consisterait à uniformiser l'architecture des bases de données spécialisées pour le traitement de l'état civil afin de permettre la portabilité entre les différents logiciels.**

---

[5] 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).

[6] Parallèlement à la publication des bans.

[7] Le jour du mariage sont remis aux parties le livret de famille ainsi que les extraits.

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

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

[10] Les récépissés sont établis une fois les deux enregistrements (informatique, manuel) effectués.

[11] Sans filiation

[12] 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.

[13] 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).

Conclusions

Les agents en charge de l'état civil sont réservés vis-à-vis du passage au tout « électronique », malgré la souplesse et la facilité apparentes liées au fait qu'il n'y aurait plus de rupture de charge. Ce passage impliquerait d'introduire une signature électronique des actes afin de donner une valeur légale aux actes enregistrés informatiquement et aurait pour corollaire en toute logique de faire disparaître la collection papier.

L'obligation notamment d'enregistrer deux fois les mentions marginales est ressentie durement en terme de charge de travail et de lourdeur de la procédure. Toutefois, la solution consistant à sortir sur papier les mentions marginales, à les signer et à les classer à part sans faire le lien manuellement avec l'acte source n'est pas réellement satisfaisante (solution adoptée pour les mentions marginales qui ne sont plus apposées dans les greffes des tribunaux de grande instance et que tous s'accordent à trouver mauvaise : quasi impossibilité dans une grande commune de reconstituer si besoin l'acte étant donné le nombre très important de documents et classement souvent médiocre).

Le problème des signatures électroniques des parties et des déclarants n'a pas réellement été étudié, ni sous son aspect technique[14] ni sous son aspect organisationnel (mise en place d'une infrastructure de gestion de clés)[15] . C'est là en effet une des difficultés principales de la dématérialisation des actes de l'état civil dans la mesure où on ne peut imaginer un système dans lequel on aurait à la fois des signatures manuscrites (si ce n'est pour la délivrance des actes) et des signatures électroniques[16]. S'engager dans la dématérialisation au sens de la loi du 13 mars 2000 et de son premier décret d'application sur la signature électronique implique de généraliser la signature électronique à tous les officiers et à toutes les parties.

Ceci étant, il est proposé d'opérer une distinction entre les signatures des parties (mariage) et celles des simples déclarants (naissance, décès). La signature des déclarants est-elle à ce point indispensable, la signature de l'officier public pouvant, seule, authentifier la déclaration qui lui est faite ?

En outre, ne doit-on pas considérer la dématérialisation comme avant tout, une possibilité d'améliorer le service et de simplifier les formalités administratives et imaginer, notamment pour les actes de naissance, que ce serait l'officier public qui se déplacerait dans les maternités et recueillerait la déclaration non plus d'une sage-femme mais de la mère elle-même, ceci afin d'améliorer la qualité de la vérification par l'officier public de ce qui lui est rapporté ? Dans ce cas, devrait être résolu un problème d'organisation (attribution concomitante de numéros si plusieurs officiers accomplissent simultanément la même démarche).

Dans cet état d'esprit, ne doit-on pas développer un maximum les relations administration à administration (par réseau sécurisé) pour l'échange des actes[17], les demandes émanant de particuliers pour avoir des copies ou extraits, étant généralement justifiées elles-mêmes par une demande d'une administration. Ceci étant, ces échanges qui « éviteraient » le particulier posent d'autres problèmes : impossibilité pour la personne de se rendre compte d'une erreur éventuelle, atteintes éventuelles aux droits de la personne, toutes les informations le concernant n'ayant pas forcément à être vues par une autre administration sans sa médiation.

Le fait de renoncer à l'édition des actes sur papier[18] (hormis pour les parties si elles le désirent) suscite une inquiétude assez grande causée notamment par la difficulté technique soit de passer d'une version à une autre d'un logiciel, voire d'une application à une application, par les inconvénients des formats propriétaires (« soumission » à une société[19] et à ses aléas –faillite..., difficultés éventuellement de récupérer les codes sources, absence de compatibilité entre une application et une autre et par conséquent entre une mairie et une

---

[14] En attendant une carte d'identité avec une carte à puce contenant la signature électronique de l'individu ?

[15] D'ailleurs le service central de l'état civil de Nantes qui est déjà allé très loin dans l'informatisation de ses actes (le registre papier n'étant plus tenu à jour) n'utilise pas une infrastructure de gestion de clés au sens du projet de décret d'application de la loi du 13 mars 2000 sur la signature électronique, mais un système de signature numérisée. Le service serait aujourd'hui dans l'incapacité, selon ses dires, de passer à la signature électronique au sens du projet de décret.

[16] Sauf à imaginer qu'on recueille des actes papier signés à la main par les parties (conservés à part pour faire preuve) et que la transcription de ces actes sur la base de données comporte simplement mention de ces signatures et soit authentifiée par la seule signature électronique de l'officier.

[17] Ce qui repose le problème de la compatibilité des produits !

[18] L'avantage du gain de place papier n'a pas été évoqué par les différents participants.

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

autre qui n'est pas équipée avec le même système), par les craintes habituelles suscitées par l'électronique (et son obsolescence très rapide) dans une perspective de conservation pour une durée illimitée.

Pour la conservation à très long terme des actes, on pourrait imaginer[20] que de même que certains actes sont, dès leur établissement envoyés automatiquement à l'INSEE, ils soient également envoyés systématiquement à un service central de l'état civil qui assureraient le stockage et la conservation de ces actes pour l'ensemble des municipalités, ce qui permettrait de reporter sur ce seul service les problèmes de compatibilité entre les différents systèmes (logiciels à faire agréer par ce service, qui imposerait un certain nombre de recommandations quant à l'architecture des systèmes et le format des actes).

Françoise BANAT-BERGER

[20] Voir note sur l'établissement et la conservation des actes authentiques dématérialisés, par Yves Rabineau et Françoise Banat-Berger.

3. L'I N S E E

(compte rendu de visite)

Compte-rendu de visite à l'INSEE (Département démographie de la direction des statistiques démographiques et sociales), 9 janvier 2001

Transmissions des données des actes de l'état civil à l'INSEE

Cette visite a été effectuée par le groupe de travail sur la dématérialisation des actes authentiques dans la mesure où l'INSEE est devenu un partenaire essentiel des services de l'état civil des communes dans le cadre du transfert de bulletins statistiques.
Elle devra être complétée, notamment pour les problèmes de stockage, d'exploitation et de conservation des archives électroniques, par la visite de la cellule mise à disposition et archivage (direction de la diffusion et de l'action régionale) ainsi que du centre informatique de Nantes.

Les communes (les 600 plus importantes dans lesquelles se trouvent notamment des maternités) envoient un certain nombre de bulletins statistiques à l'INSEE (bulletins 1 et 1bis (transcription et mention en marge), 2 (mariage), 4 (reconnaissance), 5 (naissance), 6 (enfant sans vie), 7 et 7bis (décès). Les transmissions sont quotidiennes (bulletins 5 et 7 –avec certificat de décès), hebdomadaires (4 et 7bis), mensuelles (1,1bis, 2 et 6).

Les données proviennent des renseignements qui sont portés sur les actes de l'état civil auxquelles se rajoutent quelques indications spécifiques demandées par l'INSEE dans un but statistique[1]. Ces bulletins permettent en effet de réaliser des statistiques démographiques et, d'autre part, ce qui intéresse particulièrement notre propos, de tenir à jour un certain nombre de répertoires (répertoire national d'identification des personnes physiques, fichier électoral, répertoire national inter- régimes des bénéficiaires de l'assurance maladie).

Les transmissions à l'INSEE des données de l'état civil des personnes se sont peu à peu automatisées[2] en prenant en compte l'informatisation croissante de la gestion de l'état civil dans les grosses communes : envoi de disquettes qui posent de gros problèmes de compatibilité de formats, de lecture et, parallèlement lorsque les communes l'acceptaient, transfert par Tedeco, ce type de transfert permettant des transmissions de meilleure qualité dans la mesure où une norme de transfert est respectée. Les délais initiaux en matière d'alimentation du répertoire restaient assez longs (deux à trois mois).

C'est depuis 4 ans que l'INSEE a décidé d'améliorer les modalités de ces transferts en raison des nécessités d'alimentation quotidienne du répertoire national interrégimes des bénéficiaires de l'assurance maladie (RNIAM)[3]. L'INSEE a entrepris un action forte vers les 600 communes dans lesquelles on comptabilise des naissances en vue de développer l'informatisation de la gestion de l'état civil et les transferts par voie télématique (abandon progressif des disquettes). Elle a par conséquent mis en place une politique d'homologation des logiciels sur la base d'un cahier des charges. Cette politique concernait les sociétés développant des outils pour la gestion de l'état civil ou des communes qui développaient eux-mêmes leurs propres produits. Ceux-ci ont dû modifier si nécessaire leurs applications pour les rendre conformes. L'opération a réussi dans la mesure où l'INSEE en contrepartie accordait une subvention aux communes qui avaient mis en place leur informatisation avant une date fixe. Le coût total des subventions attribuées s'est élevé à 7 à 8 millions de francs. Cette opération s'est accompagnée de campagnes de formation et d'information de la part de l'INSEE, ceci afin de permettre une meilleure prise en compte par les communes des impératifs de l'INSEE (mise à jour du répertoire national dans les trois jours pour les actes de naissance). Aujourd'hui, sur ces 600 communes, le taux d'informatisation pour la transmission des actes de naissance est de 90 à 95%[4]. Ceci étant, le suivi de cette politique d'homologation n'est actuellement pas assuré.

Un projet est en cours pour les petites communes qui leur permettraient d'utiliser Internet pour transmettre leurs bulletins statistiques, le transfert Tedeco étant lourd en terme de procédure et en terme de coûts (abonnement) pour des communes qui n'envoient que peu de bulletins à la fois. Ce projet ne sera finalisé que lorsque la sécurité du réseau mis en place sera parfaitement assurée. Ce projet s'inscrit à son tour dans le cadre d'un projet plus global de l'INSEE portant sur la certification des postes de travail et le cryptage des données.

---

[1] Situation familiale, activité professionnelle des intéressés, poids des nouveaux-nés...
[2] Durant une longue période, l'INSEE saisissait les bulletins papier et il arrivait qu'il s'agisse d'une re-saisie dans la mesure où les communes étaient déjà elles-mêmes informatisées.
[3] Attribution immédiate d'une carte Vitale aux nouveaux nés.
[4] 60% pour les décès mais la mise à jour du répertoire national est plus lente (délai d'un mois qui devrait être réduit à une semaine), pourcentage encore moindre pour les mariages (mais les impératifs de délai sont bien moindres dans la mesure où le bulletins mariage servent exclusivement aux statistiques).

Fonctionnement du répertoire national

Le répertoire physique créé en 1945 (on y trouve mention de personnes nées en 1891) a été informatisé et centralisé (jusqu'alors les données étaient déconcentrées entre les différentes directions régionales) en 1972. C'est ainsi que les données concernant l'état civil des personnes nées en France et dans les DOM-TOM[5] sont conservées sous une forme électronique dans ce répertoire, sans aucune suppression des données, dans une base vivante[6] depuis plus de 30 ans.

Figurent dans le répertoire les données concernant la naissance d'un individu (numéro de l'acte, nom, prénom, date et lieu de naissance) ainsi que son décès. Aucun élément ne figure sur la filiation, le mariage. Les mentions marginales ne sont utilisées que dans la mesure où elles « affectent » les données concernant la naissance (notamment les incidences sur le nom). Le répertoire ne gère en outre aucun historique des enregistrements.

L'INSEE a mis au point un algorithme d'identification (mécanisme de recherche) permettant de vérifier que les données fournies sont suffisamment fiables pour être automatiquement implémentées dans la base de données. Dans le cas contraire (« les litiges »), il y aura une intervention humaine permettant de cerner le problème et allant jusqu'à contacter la commune en cas de problème. Ces « litiges » peuvent atteindre 2%. Ce sont ces coûts humains qui sont les plus lourds à supporter pour l'INSEE, bien loin devant les coûts de maintenance technique de la base. Cette méthodologie permet à l'INSEE de repérer éventuellement des erreurs qui n'auraient pas été décelées par les communes (problèmes liés à l'exhaustivité des données fournies, confusion entre la date d'enregistrement et la date de naissance, doublons, problèmes de conformité...).

Conclusion

La politique menée par l'INSEE en matière de transmission de données provenant des actes de l'état civil est intéressante dans la mesure où cet organisme s'est trouvé confronté à des problèmes d'hétérogénéité des applications étant donné le nombre particulièrement élevé des communes.

Dès lors qu'il a voulu obtenir des résultats significatifs, il a dû adopter une politique très volontariste en réussissant à imposer des normes (par le respect d'un cahier des charges qu'il a imposé aux communes) contre l'obtention de subventions, ces subventions n'étant pas attribuées (à un jour près) si la date fixée pour l'informatisation du service ou son évolution était dépassée. Ceci étant cette méthode a ses limites si son suivi n'a pas été pris en compte dès l'origine.

On remarque également que l'action de l'INSEE en direction des communes autres que les 600 plus grandes est restée très limitée, ne serait-ce que parce que son intérêt à agir est moindre (les impératifs de délai ne sont pas comparables) et certainement aussi en raison de l'impossibilité d'entreprendre une action efficace face à autant de partenaires.

En matière d'établissement et de conservation des actes de l'état civil, soit les plus petites communes conservent l'édition papier des actes établis ainsi que de leur mise à jour en gardant également les signatures manuscrites, même si elles disposent d'un outil permettant la gestion informatisée de l'état civil, soit, si elles décident pour certaines d'entre elles, d'abandonner le support papier, il semble indispensable alors de mettre en place une procédure de transfert, cette fois non des données mais des actes eux-mêmes à un service central chargé de l'exploitation à long terme de ces actes. Si ce service central (national ou régional) est mis en place, il serait préférable que toutes les communes quel que soit leur taille, y transfèrent leurs actes. On peut alors imaginer que les transferts de bulletins à l'INSEE soit, continueraient à être assurés par les communes, soit par ces services centraux, l'INSEE ayant tout intérêt à avoir un petit nombre d'interlocuteurs avec qui négocier et pouvant alors tisser des liens privilégiés avec ces services centraux.

En tout état de cause, l'exemple de l'INSEE semble prouver que si l'Etat veut mener à bien la dématérialisation des actes de l'état civil, il devra mettre en œuvre une politique très volontariste basée sur le respect de cahiers des charges et de normes, la formation, le contrôle ainsi que sur des incitations financières fortes.

Françoise Banat-Berger
Service des archives, ministère de la Justice

[5] C'est la caisse nationale d'assurance vieillesse qui gère le répertoire des personnes nées à l'étranger (quelle que soit leur nationalité), leur inscription se faisant généralement par le biais d'un organisme social.
Un fichier miroir du répertoire général est géré par cette caisse, toute mise à jour sur le répertoire lui étant transmise immédiatement

[6] SGBD Adabase.

4. Conseil national des greffiers des tribunaux de commerce

(compte rendu de visite)

Visite au Conseil national des greffiers des tribunaux de commerce le 4 janvier 2001

Les tribunaux de commerce ont déjà une longue expérience en matière d'échanges dématérialisées : premières expériences télématiques dès les années 1984-1986 et depuis le début des années 1990, dans le domaine des transmissions inter-admininistrations : 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[1].

Actuellement, au tribunal de commerce de Bobigny, est mis en place à titre expérimental, l'établissement des assignations sur support électronique[2] : 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[3] 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[4].

Si les officiers publics d'état civil ou les greffiers des tribunaux sont mitigés, les greffiers des tribunaux de commerce qui travaillent avec des entreprises, des organismes financiers qui ont largement développé les échanges dématérialisés, attendent avec impatience les décrets d'application de la loi du 13 mars 2000, y voyant enfin la possibilité d'éliminer dans la chaîne toute rupture de charge ainsi que les gains à réaliser en mettant fin à la conservation papier des documents.

La définition d'actes authentiques[5] pour les documents conservés dans les greffes des tribunaux de commerce, au-delà des minutes des décisions rendues par la juridiction avec les plumitifs d'audience (avec enregistrement des incidents par le greffier), les états de nantissement et les inscriptions de privilèges ainsi que le registre du commerce, pose problème pour les actes déposés qui comportent eux-mêmes des signatures électroniques, ceci devant se décliner suivant le type d'acte (que le greffier doit contrôler, contrôler partiellement, ne pas contrôler) et les restitutions qui doivent en être faites. Une sur –signature apposée par un greffier accompagnée d'un horodatage sur les actes déposés conférerait l'authenticité à ces actes en ce que cette signature signifierait bien que les actes ont bien été reçus tel jour par tel greffier après vérification par ce dernier de l'identité des signataires ainsi que de leur qualité à signer et que leur contenu n'a pas été modifié, cette sur-signature s'accompagnant de l'émission d'un certificat électronique de dépôt (valant récépissé opposable à tiers).

Pour les minutes des décisions signées par le juge puis par le greffier[6], on pourrait envisager soit une première signature électronique du juge que sur-signerait le greffier (sa sur-signature signifiant alors qu'il se

[1] Cette opération est possible aujourd'hui car elle ne nécessite aucune pièce justificative : il s'agit uniquement d'un simple bordereau qui est dématérialisé, puis qui fait l'objet d'une sortie papier pour archivage.
[2] Une sortie papier est tout de même encore produite, conformément à la législation.
[3] En attente de regroupement et de standardisation des centres informatiques des URSSAFF.
[4] 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.
[5] A la différence des actes de l'état civil, des minutes notariales, des minutes des décisions des juridictions, tous les actes authentiques conservés par les tribunaux de commerce n'ont pas vocation à être conservés pour une durée illimitée (voir circulaire conjointe Culture/Justice AD 88-7 et CIV 88/3 du 27 juillet 1988 sur le règlement des archives des tribunaux de commerce et des tribunaux de l'ordre judiciaire à compétence commerciale).
[6] Les greffiers des tribunaux de commerce participent à la mise en forme des décisions.

porte garant que le juge qui a signé est bien celui qui a assisté à l'audience durant laquelle l'affaire a été jugée[7]), soit une double signature parallèle, le tout étant lié dans une enveloppe –qui vaudrait accusé de réception- sur laquelle serait portée une troisième signature (simple cette fois, au sens de la directive européenne du 13 décembre 1999) d'un greffier.

Les greffiers des tribunaux de commerce ainsi que les professionnels concernés (experts comptables, huissiers, avocats..) ont bien conscience qu'il s'agit non seulement de mettre en place une signature électronique mais également de mettre en place des procédures dans lesquelles s'inscrirait cette signature.

De nombreuses questions se posent concernant la qualité des prestataires de service, la constitution, au sein des ordres et professions réglementées, d'autorités d'enregistrement garantissant au certificateur qu'un tel a bien la qualité de greffier dans tel tribunal. Les acteurs concernés ressentent fortement le besoin de re-découvrir de nouvelles relations de confiance entre partenaires, allant de la création (en projet) d'une fédération nationale de tiers de service, à la certification croisée[8], permettant une garantie des systèmes mis en place, un contrôle permanent de la qualité des prestations et finalement de la mise en place de politiques de certification type.

En conclusion, il apparaît bien que les professionnels attendent impatiemment les décrets d'application de la loi du 13 mars 2000, en raison des gains de productivité et des économies qu'ils permettront en supprimant les circuits papier, tout en étant conscients des difficultés et des enjeux qui seront alors en jeu. Ils sont encore au début de leurs réflexions visant à mettre en place une nouvelle éthique permettant de certifier la qualité des nouvelles prestations qui seront fournies et sont désireux de travailler avec les pouvoirs publics sur les politiques à mettre en place dans ce cadre-là.

Françoise BANAT-BERGER

[7] Un des intervenants lors de la visite au conseil national des greffiers des tribunaux de commerce a toutefois émis l'idée que cette sur-signature serait impossible dans la mesure où elle signifierait bien plus, à savoir que le greffier se porterait garant en quelque sorte du fonds et de la forme de la décision.

[8] Concept déjà très pensé et appliqué dans des pays comme l'Allemagne.

5. Le service de transfert et d'archivage des fichiers (Centre national d'études spatiales)

(compte rendu de visite)

Compte-rendu de la visite effectuée au C.N.E.S. le 17 octobre 2000[1]

Contexte de création du département de valorisation et de gestion des données ainsi que du premier centre de données de la physique des plasmas

De 1960 à 1990, les données produites par les différentes équipes de recherches sont récupérées et alimentent une bandothèque. En 1990, un groupe sur la gestion des données spatiales se monte avec la nécessité de récupérer les données enregistrées sur les bandes dans la mesure où celles-ci deviendront obsolètes à compter de 1998. Tout un travail de rétro- conversion a dû être mené pour les données sous format propriétaire : il s'agissait d'une opération beaucoup plus délicate qu'une simple migration de supports. Dans certains cas, la réversibilité a pu être préservée, qui a permis de vérifier que les données n'avaient pas subi d'altération.

La principale difficulté rencontrée provenait de l'information de représentation - à savoir les informations qui établissent une correspondance entre les données d'une part et, d'autre part des concepts plus compréhensibles- qui, soit n'existaient plus, soit étaient incomplètes, soit comportaient des erreurs, soit ne résistaient pas aux changements de formats. En 1995, sont ainsi comptabilisées 64 000 bandes dont les données proviennent de 295 propriétaires différents.

A partir de ce groupe de travail, ont été créés d'une part un service de gestion des données spatiales et d'autre part, un service de transfert et d'archivage des fichiers (STAF).

En 1998, la direction de CNES accepte de créer le département de valorisation et de gestion des données tandis qu'en 1999 est créé le premier centre de données (celui de la physique des plasmas), résultat d'une collaboration CNES/CNRS.

Le centre participe à deux groupe de normalisation : celui du comité consultatif pour la consultation des données spatiales, qui met au point le modèle O.A.I.S., ainsi que celui du comité d'observation des satellites, qui se préoccupe de l'interopérabilité des produits résultants du spatial. Le département développe quant à lui des actions de recherche dans le domaine de la gestion des données numériques.

Le service de transfert et d'archivage des fichiers[2]

C'est en 1993 que le CNES a décidé d'implémenter dans le centre informatique un système d'archivage pour la préservation des données et la gestion de leur stockage. Le STAF fonctionne depuis 1995 et est dédié aux projets spatiaux qui exigent un archivage à long terme.

Le STAF se base sur les grands principes suivants :

---

[1] Cette visite devra être complétée par celle du centre d'archivage de la société de service EDS qui exploite pour le compte de la carte Vitale, les feuilles de soins établies sur tout le territoire. La société a acquis une progiciel du marché « Object Archive » de la société Synstar, lié au logiciel d'archivage « Net-backup » de chez Veritas. Le principe est que chaque producteur de feuille poste quotidiennement depuis son poste, les feuilles de soins dressées qu'un logiciel spécifique de messagerie asynchrone va chercher automatiquement et archive via le logiciel Object Archive. Cette problématique pourrait rejoindre celle de la récupération éventuelle des actes authentiques par des services centraux, d'autant que le problème de la confidentialité et de la sécurité de la transmission se posent également. Enfin, le système archive les feuilles sur des Cd-Rom non-réinscriptibles (les volumes n'étant pas très élevés) et obligation lui est faite de ne pas mélanger sur un même CD-Rom des feuilles provenant de plusieurs mutuelles (de la même façon qu'il ne s'agirait pas de stocker sur un même support des actes provenant de plusieurs études notariales, ou greffes ou encore communes).

[2] Outre les explications fournies lors de la visite par Claude Huc, des compléments m'ont été très obligeamment fourni par Anne Jean-Antoine, informaticienne travaillant au service projets du STAF.

- Transparence pour les utilisateurs vis à vis des supports : l'utilisateur ne manipule plus les média et ne se préoccupe plus de leur pérénnité physique,
-
- Stockage structuré des données sous forme d'arborescence de fichiers,

- Indépendance par rapport aux systèmes d'exploitation producteur de données par :

la restitution en monde hétérogène permettant de récupérer des données depuis des moyens de traitement différents des moyens qui ont archivé initialement les données,

la mise à disposition d'une ligne de commande unique quel que soient les moyens de traitement depuis lesquels sont archivées / restituées les données

- Confidentialité et sécurité des données.

Plusieurs types de données sont archivées :

- Données provenant des missions spatiales (soit des données d'observation, soit des mesures).

- Données provenant d'expériences (mesures, résultats de calculs pour la mise au point de modèles mathématiques que les scientifiques veulent préserver pour les comparer aux données réellement observées ...)

- Données d'observation de la terre (les images provenant de satellites d'observation de la terre comme SPOT).

Intégration des données

Lorsqu'un administrateur de projet souhaite archiver, il rencontre les agents du STAF, passe un contrat de service dans lequel il donne quelques éléments sur le projet (volume, éléments descriptifs).

L'archivage des projets comprend généralement les données elles-mêmes ainsi que les fichiers descriptifs de ces données. Le STAF peut gérer un lien sémantique entre les données et leur description mais bien souvent, ce sont les utilisateurs eux-mêmes qui préfèrent gérer dans des bases qui leur sont propres, ces liens.

L'admininistrateur système qui a une vue horizontale sur tous les projets crée une racine et c'est l'administrateur du projet qui reprend alors la main pour nommer le projet, créer des profils d'utilisateurs. C'est ainsi que chaque projet a son arborescence (racine, répertoires, fichiers) alimente le catalogue, sorte de "directory" enrichi. Ceci étant, il n'existe pas une racine unique pour l'ensemble des projets.

Un profil d'accès combine des droits d'accès (droit d'écrire, de lire, projet pouvant être consulté par tous --et par conséquent sans gestion de mot de passe) et des privilèges soit des droits d'action (droits de créer des utilisateurs, des répertoires, de consulter les statistiques). Les droits d'accès et les privilèges sont automatiquement récupérés par les niveaux inférieurs.

Après avoir défini les profils, l'administrateur du projet peut relier un utilisateur physique sur un moyen de traitement (client du système STAF) à un profil.

L'utilisateur manipule les noms logiques des dossiers pendant que le système de stockage gère des noms physiques et uniques à chaque fichier ; un lien est créé entre ce nom logique et ce nom physique du fichier, lien qui est contenu dans la base de donnée qui renferme également le catalogue des projets.

Lorqu'un utilisateur archive un fichier, il lui donne des attributs (nom, format des données, classe de service) tandis que le système calcule certains attributs (taille, date d'archivage...), les utilisateurs ayant la possibilité de donner des attributs complémentaires s'ils le souhaitent., tous ces attributs et meta-données étant conservés dans la base.

Stockage et restitution des données

Les classes de service définies par les utilisateurs permettent de déterminer le niveau de performance en matière de restitution des données archivées ainsi que la garantie de pérennité par la duplication ou pas des fichiers physiques (opération de backup) : ainsi le support pour obtenir la meilleure performance au STAF sont aujourd'hui les disques magnétiques. Les disques sont automatiquement "redondés", un pour un (système RAID 1) en cas de défaillance ; les supports de deuxième niveau sont des cartouches de la gamme Storagetek et IBM .

Ceci est transparent pour l'utilisateur qui ignore quel est le système de stockage pour les données qu'il a archivées et le type de support. Les cartouches sont stockées dans des librairies automatisées. Le STAF gère automatiquement la migration des données des disques vers les cartouches (la migration est paramétrée aujourd'hui un jour après la mise sur disque via l'opération d'archivage) mais le retour des cartouches sur disques est déclenché systématiquement quand l'utilisateur veut une restitution des données. Le système gère également le recyclage des supports : un support qui est détérioré est repéré par le système qui le recycle. Les cartouches sont aussi recyclées systématiquement tous les 5 ans via ce même procédé.

C'est ainsi que pour le stockage, le STAF propose :

- des supports en ligne (les disques magnétiques)
- des supports "presque en ligne" soit les cartouches de petite ou grande contenance : le délai de restitution est un peu plus long .

Il n'existe pas de média "off-line" ce qui équivaudrait à déstocker des cartouches des librairies automatisées pour les stocker sur des rayonnages.

Le stockage est binaire : ainsi le STAF restitue à l'utilisateur exactement ce que celui-ci a archivé. Il ne touche pas au contenu des fichiers. Les utilisateurs prennent ainsi la responsabilité de faire en sorte de pouvoir relire les données avec leurs propres outils quand celles-ci sont restituées (ainsi les images SPOT ont leur propre format). Ceci étant, des formats sont recommandés par le STAF (norme IEEE qui permet de relire des flottants dans le domaine du calcul, norme ASCII, format texte..).

En ce qui concerne les formats de description de données, d'autres services du CNES ont créé des formats normalisés de description spécifiques pour les données spatiales (format EAST, un logiciel pour le mettre en valeur –OASIS- ayant notamment été adopté pour la description des images SPOT)[3].

Equipements et volumétries

Le STAF fonctionne en majorité sur les équipements IBM : c'est IBM qui a développé l'application STAF et qui s'occupe de la maintenance de l'ensemble. Les librairies robotisées et cartouches sont de la gamme STK. Une librairie robotisée est dédiée aux cartouches de 50 gigaoctets pour assurer les backups des cartouches primaires.

Trois serveurs sont actuellement en service : un serveur qui manipule les petites cartouches (Timberlines) dont le volume total représente 2-3 teraoctets ; un serveur pour les grosses cartouches (9840) de 20 gigaoctects et dont la volumétrie globale représente 30 Teraoctets (1 à 2 tera d'augmentation par mois avec les images SPOT) et un serveur récemment installé. Ces trois serveurs peuvent communiquer avec 15 systèmes clients. Chaque système client dispose d'une ligne de commande unique alors même que l'utilisateur archive à partir d'un système (HP) et se voit restituer les données à partir d'un autre système

[3] Ce travail de normalisation n'a pas concerné les formats relevant déjà d'un langage commun type XML. Le problème reste entier pour les documents textuels, les solution d'attente reposant sur le format d'échanges XML même s'il existe encore très peu de ponts entre les logiciels de traitements de texte et les représentations XML. En outre, il est impossible que ce soit les services d'archives qui se chargent de reprendre les données en XML (le travail serait trop long et trop dangereux). La solution serait de donner aux équipes la possibilité d'utiliser une D.T.D. qui serait appliquée au niveau de la production. Cette solution pourrait certainement s'appliquer aux actes authentiques.

(Sun). Certains projets ont, en outre, constitué leur propre serveur Web ou leur propre application qui s'interconnecte avec le STAF, ceci afin de masquer la ligne de commande très peu interactive.

Coût du système

Le coût du STAF est bien évidemment relativement élevé (si le coût du giga a tendance à diminuer, cette baisse est largement compensée par le nombre de plus en plus important d'utilisateurs) : coût du développement initial de l'opération avec l'intégration des logiciels, des équipements (librairies automatisées, processeurs, lecteurs de bande...) et des consommables (disques, cartouches), coûts de maintenance. Coûts auxquels il faut ajouter le coût humain, à savoir un service exploitation (un administrateur système, un support externe, un exploitant), et un service projet (un informaticien, un support externe employé à 4/5 qui va passer à 2/5) .

Ceci étant, le STAF fonctionne : c'est un système fiable pour lequel les responsables n'ont eu à déplorer aucune perte de données depuis sa mise en service. Il constitue à cet égard un exemple intéressant pour nous dans la mesure où il assure toute la chaîne de traitement depuis l'intégration des données jusqu'à leur restitution.

Françoise BANAT-BERGER

6. Audition par la commission des Lois du Sénat

(compte rendu d'audition)

//LOIS CONSTITUTIONNELLES, LEGISLATION, SUFFRAGE UNIVERSEL, REGLEMENT ET ADMINISTRATION GENERALE//

##Mercredi 6 juin 2001## - Présidence de M. Jacques Larché, président.

La commission a tout d'abord procédé à **l'audition** de **M. Jean-Paul Jean**, **président**, et de **Mme Isabelle de Lamberterie, rapporteur**, accompagnés d'une délégation de membres du groupe de travail sur les **actes authentiques** sur support électronique.

M. Jean-Paul Jean, directeur de la mission de recherche droit et justice, a rappelé l'engagement pris par Mme Guigou, alors ministre de la Justice, lors de la discussion de la loi du 13 mars 2000 portant adaptation du droit de la preuve et relative à la signature électronique, d'associer les parlementaires à l'élaboration des décrets d'application. Il a noté que le groupement d'intérêt public « Mission de recherche droit et justice », constitué de membres du ministère de la Justice et du CNRS, avait remis dès 1997 un rapport sur l'écrit et les moyens technologiques à l'épreuve du droit. Il a indiqué que les membres du groupe de travail chargé d'une réflexion sur les actes authentiques sur support électronique tendaient à raisonner en juristes et avaient cherché à appliquer les principes juridiques à la technologie, et non l'inverse. Puis il a souligné le pragmatisme du projet de rapport du groupe de travail et les comparaisons internationales effectuées.

M. Jacques Larché, président, a approuvé le fait que les principes juridiques ne cèdent pas à la technologie.

Mme Isabelle de Lamberterie, directeur de recherches au CNRS-CECOJI, a rappelé que l'introduction dans la loi de la possibilité d'établir les actes authentiques sur support électronique résultait d'une initiative de la commission des lois du Sénat, le projet de loi initial ne visant que les actes sous seing privé. Elle a souligné que les membres du groupe de travail constitué au sein du GIP étaient non seulement

des juristes mais pratiquaient les actes authentiques et étaient confrontés au passage au support électronique dans les mairies, les greffes des tribunaux ou les études notariales. Elle a ajouté que les acteurs du monde de la technique étaient présents pour expliquer les contraintes inhérentes aux supports papier et électronique.

Malgré la spécificité de chaque catégorie d'actes authentiques, elle a fait savoir que le groupe de travail avait souhaité affirmer leurs points communs en proposant un décret général, ayant une fonction pédagogique. Elle a indiqué que celui-ci devrait poser les critères permettant l'harmonisation des systèmes techniques et régler les questions générales communes à l'ensemble des actes authentiques, en particulier le respect des solennités requises, en premier lieu la nécessaire présence physique de l'officier public. Elle a estimé que la signature électronique de l'acte devait s'inscrire dans le cadre de la procédure de création, de vérification et de certification des signatures électroniques sécurisées décrite dans le décret du 31 mars 2001, pris pour l'application de l'article 4 de la loi, relatif à la présomption de fiabilité. Elle a toutefois souligné la complexité d'une telle démarche, dans la mesure où la directive communautaire du 13 juin 1999 sur les signatures électroniques, comme le décret du 31 mars 2001 la transposant, utilisaient deux notions distinctes, la signature électronique et la signature électronique sécurisée (ou « avancée »), la seconde seule garantissant l'intégrité de l'acte.

Mme Isabelle de Lamberterie, directeur de recherches au CNRS-CECOJI, a mis en évidence les difficultés techniques de la conservation des signatures électroniques sécurisées, dans la mesure où les migrations successives ne permettaient pas la vérification de l'intégrité des données. Elle a écarté la solution tendant à signer les actes lors de la migration, en faisant valoir que la seule signature importante pour la définition de l'acte authentique était celle de l'officier public ayant établi l'acte. En conséquence, le groupe de travail a conclu à la nécessité de prévoir une signature électronique liée indissociablement aux données de l'acte mais ne pouvant être altérée lors des migrations successives.

Enfin, elle a noté que le statut des originaux et des copies ne dépendait pas du support utilisé (papier ou électronique) mais des conditions dans lesquelles étaient établis les actes.

M. Jean-Dominique Mathias, administrateur au Conseil supérieur du notariat, a estimé que l'introduction par le Sénat de la possibilité de dresser les actes authentiques sur support électronique avait rétabli la cohérence de la réforme du droit de la preuve, dans la mesure où l'acte authentique était placé au sommet de la hiérarchie des modes de preuve littérale. Il a fait part de sa préférence pour l'adoption de plusieurs décrets d'application, un pour chaque type d'acte authentique.

Appelant à la prudence, il a mis en garde contre le risque de confusion entre authentification et certification, entretenu par la terminologie employée par les professionnels de l'informatique. Il a insisté sur le rôle de conseil et de contrôle dévolu au notaire, chargé de vérifier l'identité des parties, de contrôler le contenu de la convention, de s'assurer de la sincérité du consentement et de l'équilibre du contrat ou encore de l'opportunité du montage juridique retenu ; pour toutes ces raisons, il a jugé que la présence physique du notaire constituait l'essence même de l'authenticité.

M. Jean-Dominique Mathias, administrateur au Conseil supérieur du notariat, a fait savoir que l'établissement des actes notariés sur support électronique était d'ores et déjà possible, grâce au réseau intranet sécurisé Réal, dont étaient équipés deux tiers des offices, et à la carte Réal à microprocesseur détenue par 3000 notaires soit la moitié de la profession. Rappelant que la loi du 13 mars 2000 ne remettait en cause ni le droit de la preuve, ni la hiérarchie des actes, ni les solennités requises pour les actes authentiques, il a annoncé que le notariat était favorable à une modification du décret du 26 novembre 1971 relatif à la compétence d'instrumentation des notaires afin de consacrer la forme électronique de l'authenticité. Enfin il a précisé que la signature des parties n'était pas nécessairement une signature électronique sécurisée, puisque la présence du notaire garantissait l'identité des parties.

M. Jean-Luc Iffrig, directeur du service population de la ville de Strasbourg, a illustré les enjeux de la loi du 13 mars 2000 pour les services d'état civil, en soulignant que ceux-ci étaient sans cesse partagés entre le nécessaire respect du formalisme garantissant l'intégrité des actes d'état civil, et le souci de simplifier les démarches administratives. Il a tout d'abord indiqué les règles avec lesquelles les services ne transigeaient pas, contenues dans l'instruction générale relative à l'état civil et conférant aux pièces d'état civil leur caractère authentique, à savoir la signature manuscrite de l'officier d'état civil et le support papier utilisé tant pour le registre de création des actes que pour les mentions marginales et la délivrance de copies et d'extraits.

Il a ensuite fait part des pratiques de simplification, en marge de l'instruction générale, concernant en particulier les déclarations de naissance et de décès effectuées majoritairement par les hôpitaux d'une part, les entreprises de pompes funèbres d'autre part, les demandes de communication des copies et extraits par minitel ou internet (le service d'état civil envoyant des documents sur support papier), et l'archivage sur support électronique.

M. Jean-Luc Iffrig, directeur du service population de la ville de Strasbourg, a estimé que la loi du 13 mars 2000, conférant la même force probante aux documents sur support électronique qu'aux documents sur support papier, et permettant la signature d'une partie « par elle-même » et non « de sa main », ouvrait des perspectives intéressantes pour les services d'état civil. Il s'est toutefois interrogé sur la fiabilité de l'archivage électronique et des échanges de documents par internet, ainsi que sur les difficultés liées à l'absence de compatibilité et d'interopérabilité des systèmes informatiques utilisés par les différentes mairies, préfectures et greffes des tribunaux. Après avoir évoqué l'idée de doter chaque citoyen d'une carte électronique d'état civil, il a estimé que des villes pilotes pourraient être choisies afin d'expérimenter l'électronisation des registres d'état civil.

Mme Françoise Banat-Berger, chef du service des archives du ministère de la Justice, a indiqué qu'à la différence des actes sous seing privé, dont la

conservation n'excédait pas trente ans, les actes authentiques, en fonction de leur valeur probante et de leur intérêt historique, pouvaient nécessiter un archivage pour une durée non limitée, représentant un défi tant technique que financier et d'organisation.

S'agissant des défis techniques, outre l'obsolescence rapide des formats de lecture et l'absence de toute expérience en matière d'archivage des signatures électroniques, elle a regretté que, sous la pression de l'INSEE, les états civils des grandes villes aient été informatisés sans principe directeur ni contrôle, au moyen d'applications très hétérogènes et non compatibles entre elles. Elle en a conclu que la question de la conservation des actes devait être posée dès la mise en place des systèmes informatiques et a souhaité que la normalisation s'effectue sous l'impulsion de la direction des archives de France.

Elle a ensuite mis en évidence certains problèmes financiers et d'organisation institutionnelle, liés au fait que les collectivités locales assuraient l'archivage des actes de l'état civil pour le compte de l'Etat. En l'absence de toute évaluation du coût de l'archivage électronique pour les services des archives départementales, elle s'est demandé dans quelle mesure les collectivités locales accepteraient de financer cette nouvelle charge, et si la centralisation de l'archivage électronique n'était pas préférable.

M. José Balarello s'est interrogé sur les fraudes possibles en matière d'état civil sur support électronique. Il a demandé si la Conservation des hypothèques était menacée par l'informatisation des actes authentiques. Enfin il a souhaité avoir des précisions sur les transactions immobilières avec les pays situés hors de l'Union européenne.

M. Jean-Paul Jean a répondu que les principes en vigueur n'étaient pas modifiés par le support électronique.

M. Jean-Dominique Mathias a indiqué que l'établissement des actes authentiques à distance n'était pas envisagé à l'heure actuelle, chaque partie à un contrat international étant reçue chez son notaire et signant une procuration.

Mme Isabelle de Lamberterie a ajouté que la capacité technique d'établir des actes à distance ne devait pas induire nécessairement la reconnaissance juridique de cette possibilité ; en l'occurrence, elle a souligné qu'il n'était pas question de remettre en cause la nature de l'acte authentique, en particulier la présence de l'officier public et l'encadrement très strict des possibilités de procuration. Elle a ajouté que la Conservation des hypothèques n'était pas menacée de disparition.

M. Jean-Jacques Hyest s'est inquiété du risque de perdre une partie du patrimoine écrit et de la mémoire collective lors des migrations d'archives électroniques.

Estimant que cette inquiétude était légitime, **Mme Françoise Banat-Berger** a indiqué que la réflexion sur les migrations de support et les migrations de format intégrait la conservation des métadonnées, renseignant sur l'historique des migrations successives.

M. Jacques Larché, président, s'étant demandé si tous les problèmes pouvaient être résolus par décret, et si le groupe de travail avait établi une liste exhaustive des différentes catégories d'actes authentiques, **M. Laurent Jacques, adjoint au chef de bureau du droit civil général au ministère de la Justice,** a répondu qu'aucun texte législatif ne s'opposait à l'élaboration des actes authentiques sur support électronique. Il a ajouté qu'outre les trois catégories d'actes authentiques les plus importantes en volume, à savoir les jugements, les actes d'état civil et les actes notariés, existaient d'autres types d'actes authentiques, que le groupe de travail n'avait pas recensés de façon exhaustive ; il a cité certains actes des huissiers de justice comme les significations et des commissaires priseurs comme les procès verbaux d'adjudication.

M. Jean-Paul Jean a indiqué que le groupe de travail remettrait son rapport définitif à la fin du mois de juin au ministre de la Justice.