

Introduction

L'émergence du document numérique sur fond de dématérialisation des processus métier et de généralisation du Web semble refermer ce que Thomas Pettitt (cité par Jean Michel Salaün) appelle la « parenthèse Gutenberg ».

La fixité et la stabilité de l'écrit obtenu dans un cadre bien particulier laissent aujourd'hui leur place à de nouveaux modèles qui, par certains aspects, renouent avec d'anciens modes de connaissance et de pensée (instabilité, variantes)

Ces transformations en cours ont de profonds impacts sur les métiers de l'information et notamment sur les disciplines de l'archivistique et de la diplomatique pour lesquelles la **consignation d'un écrit certifié** était le cœur des missions.

Introduction

Dans l'environnement numérique, un document n'existe plus en tant que tel

Dissociation entre support et contenu de l'information

Risques dès lors que transmission

- Dans l'espace (intégrité et sécurisation)
- Dans le temps (préservation sur le long terme).
Notions de fossés d'intelligibilité et technologiques

Enjeu essentiel : le document et son contexte doivent pouvoir être représentés dans un nouvel environnement culturel, social et technologique

L 'écrit numérique

La mise en place du cadre juridique

L'arrivée de l'électronique

Conséquences de la loi du 13 mars 2000
Élargissement du support documentaire

*« La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles **dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission** »*

(Code Civil, article 1316)

L'arrivée de l'électronique

Conséquences de la loi du 13 mars 2000

Les documents numériques ont la même valeur probante que le papier

« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. »

(Code Civil, article 1316-1)

« L'écrit sur support électronique a la même force probante que l'écrit sur support papier. »

(Code Civil, article 1316-3)

L'arrivée de l'électronique

Conséquences de la loi du 13 mars 2000

Définition de la signature électronique

« La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère **l'authenticité** à l'acte »

« La fiabilité de ce procédé est présumée, jusqu'à preuve du contraire, lorsque la signature est créée, l'identité du signataire assurée et **l'intégrité** de l'acte garantie, dans des conditions fixées par décret en Conseil d'État »

(Code Civil, article 1316-4, premier alinéa).

Un décret d'application relatif à la signature électronique

Décret du 30 mars 2001 : article 2

La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié

Transposition très fidèle de l'annexe de la directive européenne de 1999 sur la signature électronique

Décrit les conditions nécessaires pour que la fiabilité soit avérée : fiabilité qui entraîne le renversement de la charge de la preuve

La mise en place de la législation et réglementation sur l'écrit numérique

Toute une série de textes visant à préciser les formalités à remplir dans un environnement numérique :

Articles 1369-1 à 1369-11 du code civil relatifs aux contrats passés sous forme électronique

Article 1325 (CC) : concepts d'originaux et de pluralité d'originaux

La mise en place de la législation et réglementation sur l'écrit numérique

Pour le secteur public :

Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives : mise en place d'un **référentiel général d'interopérabilité et d'un référentiel général de sécurité**

Décret n° 2010-112 du 2 février 2010 : porte sur le **référentiel général de sécurité**

Deux notions essentielles : l'identité et l'intégrité

- Mais deux limites essentielles à ces textes relevées par notamment par les archivistes
 - Comment concilier l'intégrité au sens technique du terme (les 0 et les 1) et le maintien de la lisibilité sur le long terme ?
 - Comment assurer la conservation et la vérification sur le long terme des signatures électroniques ?

Une première approche basée sur la sécurité informatique : le Référentiel général de sécurité (RGS)

Comment garantir en effet ?

- la **sécurité des informations** échangées, et notamment leur **confidentialité et leur intégrité**,
- la **disponibilité et l'intégrité de ces systèmes** et l'**identification** de leurs utilisateurs

En mettant en œuvre des fonctions de sécurité :

- **identification**
- **signature électronique**
- **confidentialité**
- **horodatage.**

En mettant en place des mécanismes de **conformité** d'un produit de sécurité et d'un service de confiance

Une première approche basée sur la sécurité informatique : le RGS

Rejoint les tentatives de mettre en place un nouvel formalisme dans l'environnement numérique

- **envoi d'une lettre recommandée par courrier électronique** (décret n° 2011-144 du 2 février 2011)
- horodatage des **courriers expédiés ou reçus par voie électronique pour la conclusion ou l'exécution d'un contrat** (décret n° 2011-434 du 20 avril 2011)
- notion de procédé **d'horodatage fiable** avec la certification du module d'horodatage et la qualification des prestataires de service d'horodatage

Une première approche basée sur la sécurité informatique : le RGS

Problématique des accusés de réception suite à l'envoi de courriers électroniques (principe posé par l'ordonnance de 2005) actuellement revisité

De fait, jusqu'alors très peu de précisions données par les textes sur la forme et la certification de ces accusés de réception

En train d'évoluer avec les futures dispositions législatives sur le renversement du principe suivant lequel le silence de l'administration vaut rejet de la demande

Une première approche basée sur la sécurité informatique : la politique d'archivage

LA P2A : la politique d'archivage sécurisé dans le secteur public (2006)

Des compétences croisées (pour la première fois) : juristes, informaticiens (sécurité informatique), archivistes

Une définition de l'archivage électronique sécurisé est ainsi défini comme l'ensemble des modalités de conservation et de gestion des archives électroniques **ayant une valeur juridique lors de leur établissement**, cet archivage garantissant la valeur juridique jusqu'au terme du délai durant lequel des droits y afférents peuvent exister

Une première approche basée sur la sécurité informatique : la PA

Des conditions nécessaires définies :

Il est **OBLIGATOIRE**, pour que l'archivage électronique remplisse sa finalité juridique, que les modalités mises en place **permettent de garantir que le document archivé peut être**

lu et intelligible

imputable à un auteur identifié et

fiable et intègre jusqu'au terme du délai durant lequel des droits y afférents peuvent exister

Une seconde approche : basée sur la signature électronique

Depuis la loi française n°2000-230 sur l'adaptation du droit de la preuve et relative à la signature électronique

Code civil, Article 1317 : « **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 ».

« Il peut être dressé sur support électronique, s'il est établi et conservé dans des conditions fixées par décret en Conseil d'État »

« **La signature** nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. **Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte** » (Article 1316-4, premier alinéa)

Code général des impôts, annexe 3, article 96-F :

« Les factures émises dans les conditions visées au premier alinéa du V de l'article 289 du code général des impôts tiennent lieu de factures d'origine lorsque **l'authenticité de leur origine et l'intégrité de leur contenu** sont garanties au moyen d'une signature électronique ».

Durant les premières années suivant la loi de 2000, **lien évident entre la notion d'authenticité et celle de signature électronique**

Authenticité dans les textes législatifs et réglementaires

- Décret n° 2011-167 du 10 février 2011 instituant une procédure de vérification sécurisée des données à caractère personnel contenues dans les actes de l'état civil (et arrêté du 23 décembre 2011)
- Lorsqu'elles [demandes de vérifications] sont échangées par voie électronique, elles doivent être réalisées dans des conditions qui garantissent **l'intégrité des informations échangées, la sécurité et la confidentialité de la transmission, l'identité et la fonction de l'expéditeur et celles du destinataire** (article 13-5 du décret n° 62-921 du 3 août 1962)
- COMEDEC utilise des procédés techniques garantissant l'authentification, la signature électronique, l'horodatage, l'intégrité, la confidentialité et la traçabilité des échanges électroniques (certificats 3 étoiles, signature de niveau 3 étoiles)

Une seconde approche : basée sur la signature électronique

Exemple des procédures pénales :

- Code de procédure pénale, art. 801-1. - « *Tous les actes mentionnés au présent code, qu'il s'agisse d'actes d'enquête ou d'instruction ou de décisions juridictionnelles, peuvent être revêtus d'une **signature numérique ou électronique**, selon des modalités qui sont précisées par décret en Conseil d'État* »
- La signature (également trois étoiles) entraîne une vérification de la signature dont les résultats sont consignés dans les métadonnées du document
- Pour la transmission de l'expédition aux parties
 - Mention que la minute a fait l'objet d'un dispositif de signature électronique sécurisé
 - Lors de l'édition sur papier, intégration de la mention en clair du nom et de la qualité des signataires et de la date de la signature (ainsi que de la date de l'expédition)

Une seconde approche : basée sur la signature électronique

Il est intéressant de noter que, dans ces cas, la signature entraîne automatiquement le versement dans un système d'archivage (intervention des archivistes)

Le dispositif est sécurisé par l'introduction d'une **obligation d'archivage sécurisé** pour ces actes ainsi signés qui doivent alors être archivés dans un « **système d'archivage électronique sécurisé** » (arrêté du 21 juin 2011 relatif à la signature électronique ou numérique en matière pénale)

Les **fonctions de conservation, intégrité, intelligibilité, accessibilité et traçabilité** durant la durée d'utilité courante et intermédiaire des documents sont requises

Le **format pérenne** des documents est requis, de même que l'obligation de **réplication des données sur un site distant**, en conformité avec d'une part la norme ISO 14721 (norme OAIS de juin 2005) et la norme Afnor Z 42-013 (version de mars 2009) sur l'archivage électronique. (A 53-6 du CPP)

- *SAE en cours de développement au ministère de la Justice, au ministère de l'Intérieur (direction générale de la gendarmerie nationale)*

Un exemple : les actes authentiques des notaires

Décrets n° 2005-972 et 973 du 10 août 2005 relatifs aux huissiers et aux notaires (intervention des archivistes)

- L'acte doit être signé par le notaire au moyen d'un procédé de **signature électronique sécurisée** conforme aux exigences du décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.
 - « Cette signature est apposée par le notaire dès l'acte établi, si besoin après réunion des annexes à l'acte ».
 - « Pour leur signature, les parties et les témoins doivent utiliser un procédé permettant l'apposition sur l'acte notarié, visible à l'écran, de l'image de leur signature manuscrite ».

L'acte est parfait lorsque le notaire instrumentaire y appose sa signature électronique (également trois étoiles) sécurisée.

Un exemple : les actes authentiques des notaires

L'acte établi sur support électronique doit être conservé dans des conditions de nature à en préserver **l'intégrité et la lisibilité**.

Métadonnées : « L'ensemble des informations concernant l'acte dès son établissement, telles que les données permettant de l'identifier, de déterminer ses propriétés et d'en assurer la traçabilité » doit être également conservé.

Mais toujours maintien d'un registre

- Les notaires tiennent un répertoire sur support papier ou sur support électronique de tous les actes qu'ils reçoivent.

Organisation ad-hoc : une centralisation des actes

- « L'acte notarié dressé sur support électronique est enregistré pour sa conservation dans un minutier central dès son établissement par le notaire instrumentaire. Ce dernier, ou le notaire qui le détient, en conserve l'accès exclusif ».
- *Ouverture en 2008 du minutier central des notaires (MICEN) à Venelles*

Un exemple : les actes authentiques des notaires

Respect du code du patrimoine

- « Le minutier central est établi et contrôlé par le Conseil supérieur du notariat sans préjudice de l'application de l'article 2 du décret n° 79-1037 du 3 décembre 1979 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques ».

Contradiction entre signature électronique et migration de formats nécessaires à assurer la lisibilité sur le long terme résolue :

- « Les opérations successives justifiées par sa conservation, notamment les migrations dont il peut faire l'objet, ne retirent pas à l'acte sa nature d'original ».

Un exemple : les actes authentiques des notaires

S'agissant des copies sur support électronique :

- « Le notaire peut procéder à la copie sur support électronique d'un acte établi sur support papier après avoir utilisé **un système de numérisation dans des conditions garantissant sa reproduction à l'identique.**
- « Le notaire qui délivre une copie sur support électronique **y mentionne la date et y appose sa signature électronique sécurisée.** La copie authentique comporte en outre **l'image de son sceau. Mention est portée sur la copie délivrée de sa conformité à l'original.[...]**
- « Les copies exécutoires et copies authentiques peuvent être transmises par voie électronique dans des conditions garantissant l'intégrité de l'acte, la confidentialité de la transmission, l'identité de l'expéditeur et celle du destinataire.

Un autre exemple : le livre foncier d'Alsace Moselle

Décret n° 2009-1193 du 7 octobre 2009 relatif au livre foncier et à son informatisation dans les départements du Bas-Rhin, du Haut-Rhin et de la Moselle

Le dépôt de la requête

Article 76 : Les procédés techniques utilisés garantissent, dans des conditions fixées par arrêté du garde des sceaux, ministre de la justice, **la fiabilité de l'identification du requérant et du bureau foncier, l'intégrité des documents adressés, la sécurité et la confidentialité des échanges, la conservation des transmissions opérées et permettent d'établir de manière certaine la date d'envoi et celle de la réception** par le destinataire

Article 77 : La date de dépôt est celle attribuée par **horodatage informatique** qui a lieu soit automatiquement en cas d'envoi électronique au sens de l'article 76, soit sur intervention du greffier en cas de dépôt par requête remise ou adressée par voie postale...

Pour chaque bureau foncier, il est tenu un registre des dépôts qui fixe la date, le rang et l'effet juridique des droits et mentions à inscrire.

Le registre des dépôts

Article 78 : Le registre des dépôts comporte les informations nécessaires à l'identification des requêtes et de leurs auteurs. Tout document déposé est enregistré avec la mention du jour, de l'heure et de la minute de son dépôt et affecté d'un numéro d'identification.

Un autre exemple : le livre foncier d'Alsace Moselle

L'ordonnance d'inscription

Article 81 : Le livre foncier, tenu sur support électronique, est signé par le juge au moyen d'un procédé de signature électronique sécurisée conforme aux exigences du décret susvisé du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.

Article 82 : **A compter du 1er janvier 2011, l'ordonnance établie sous forme électronique et signée par le juge au moyen du procédé mentionné par l'article 81 a valeur de minute.** Avant cette date, seule l'ordonnance établie sur support papier et signée par le juge a valeur de minute.

Une approche encore différente : le dossier dématérialisé de l'agent

Décret n° 2011-675 du 15 juin 2011 relatif au **dossier individuel des agents publics** et à sa gestion sur support électronique (intervention des archivistes)

Différenciation entre document numérisé et document nativement numérique

Introduction d'une structuration précise et encadrée du document

Impossibilité de conserver à la fois le support papier et le support numérique pour le même document

Une approche encore différente : le dossier dématérialisé de l'agent

Conditions d'acceptabilité du document numérisé

- *Art. 3 : Lorsque l'autorité administrative ou territoriale chargée de la gestion du dossier crée une copie sur support électronique d'un acte original établi sur support papier, elle utilise un système de numérisation dans des conditions et sous des formes garantissant sa reproduction à l'identique et la conservation pérenne du document ainsi créé. **La copie conforme** ainsi établie se substitue au document original sur support papier qui est détruit dans un délai fixé par l'arrêté ou la décision mentionné à l'article 9.*

Concepts de continuum (cycle de vie)

- *Art.4 : La gestion du dossier sur support électronique recouvre les opérations de collecte, de référencement, de gestion du cycle de vie des documents, de consultation, de modification, d'exploitation, de conservation, de transfert, de suppression ou d'effacement des documents et de versement au titre des archives*

Notions classiques de intégrité, accessibilité et lisibilité mais également accent sur la confidentialité

Une approche encore différente : le dossier dématérialisé de l'agent

Concept de traçabilité

Respect des référentiels interopérabilité et sécurité

Respect du code du patrimoine

Un changement par rapport aux textes du secteur judiciaire : la signature électronique n'est pas requise (pas de référence au code civil et au décret du 30 mars 2001 dans les visas)

Conclusions (1)

Depuis la loi du 13 mars 2000, de fait on constate pour le domaine de l'administration, une approche différente :

- suivant qu'il s'agit d'actes authentiques avec signature électronique dite trois étoiles et une prise en compte bénéfique du fait que la signature doit entraîner le versement dans un SAE sécurisé
- ou de simples actes administratifs pour lesquels l'exigence de ce niveau de signature, voire même la présence d'une signature n'est pas exigée, étant donné la complexité du déploiement de ce type de signature, sa diffusion en conséquence encore assez restreinte et au final, la liberté de la preuve prévalant en matière de droit administratif
- on fera alors reposer la sécurité du système sur des fonctionnalités d'authentification fortes, d'intégrité (scellements numériques), de traçabilité des opérations.

Reste à y systématiser la présence d'un SAE dès lors que les durées de conservation sont longues, adressant les fonctionnalités de pérennisation (gestion des formats et des supports, duplication de l'information sur des sites distants...)

Conclusions (2)

De fait, on constate une situation très encadrée pour les actes à la plus forte valeur probante dans le droit avec prise en compte des enjeux de la dématérialisation, en termes de droit de la preuve et de maintien de la valeur de la preuve sur le long terme (signature 3 étoiles et principe d'un SAE sécurisé)

Une situation « grise » pour d'autres autres projets de dématérialisation avec une intervention variable des problématiques archivistiques et diplomatiques suivant les cas

Conclusions (3)

En revanche une situation très médiocre pour l'ensemble de la production numérique autre : messageries numériques, productions bureautiques individuelles voire gestions électroniques de documents, bases de données « anciennes »

- pas de procédures de « records management »
- données entrées dans les bases de données douteuses, de qualité parfois médiocre, non mises à jour, erronées
- documents bureautiques produits et reçus hors de toute validation et contrôle d'aucune sorte (statut, datation, intégrité, identification de l'auteur..., lien avec d'autres documents et dossiers...)
- documents entrés dans les GED non sécurisés (numérisation hors de toute procédure et tout contrôle documenté)
- manque de temps des archivistes pour intervenir à temps et quand peuvent intervenir, se trouvent confrontés aux problématiques de données et documents « douteux »

Conclusions (4)

Mais une évolution visible au sein des services interministériels en charge du SI de l'État face aux enjeux essentiels que constituent les données numériques dans le pilotage des politiques publiques

- problématique d'urbanisation (cadre commun d'urbanisation) : archivage dans le plan d'occupation des sols des systèmes d'information de l'État, mandat « archivage numérique » mené en 2012, programme VITAM (archivistes, informaticiens) avec la nécessité d'un financement interministériel sur la problématique de l'archivage (investissements dits d'avenir)
- réflexions sur la qualité des données, leurs mises à jour et par conséquent leur conservation raisonnée (apparaît explicitement) avec une décision spécifique du comité interministériel pour la modernisation de l'État
- lancement de chantiers au delà des référentiels généraux, sur les référentiels métier (référentiels de données de référence) et les identifiants persistants et pérennes

Conclusions (5)

Autant d'éléments positifs qu'on pourra permettre aux utilisateurs (créateurs de l'information d'origine, chercheurs, citoyens, juges dans le cas d'un contentieux)

de pouvoir critiquer d'une manière satisfaisante :

- la forme
- la genèse
- la tradition

de l'information gérée, véhiculée, manipulée, transformée, représentée depuis sa création