Section 10 - intégrité, authenticité et preuve

FRANÇOISE BANAT-BERGER
CLAUDE HUC

version 1

22 novembre 2011

Table des matières

Section 10 - intégrité, authenticité et preuve

A. Chapitre 1- Objectifs de cette section

Dans cette partie, sera présenté le nouveau cadre juridique de la preuve qui, au-delà du cas de la France, a affecté l'ensemble des pays. Ce nouveau cadre vise à donner une même valeur de preuve aux documents sur support numérique qu'aux documents sur support papier, sous certaines conditions, dans un contexte d'utilisation croissante des réseaux de l'Internet et du commerce électronique. Les procédés de signature électronique (cryptographie à clé publique) seront explicités dans cette section.

Une seconde section concerne, dans ce cadre, le développement de l'administration électronique : programmes gouvernementaux, référentiels généraux structurant ce développement, enjeux particuliers de l'interopérabilité, présentation d'un exemple détaillé de la dématérialisation d'un processus administratif, interventions des Etats dans les différents pays de l'Union européenne.

Enfin seront étudiés les impacts de cette e-administration sur l'archivage : l'exemple des actes authentiques électroniques, la recommandation française du forum des droits sur internet, les travaux menés par le groupe InterPARES sur l'authenticité dans un environnement numérique, l'archivage dans les plans gouvernementaux, la norme AFNOR 42-013 et ses enjeux en termes d'intégrité, pérennité et sécurité.

B. Chapitre 2 - Le nouveau cadre juridique de la preuve en France

L'ensemble des pays évoluent de la même manière dans la mise en place d'un nouveau cadre juridique qui accorde, sous certaines conditions, la même valeur de preuve aux documents sur support numérique qu'aux documents sur support papier.

En **France**, le nouveau cadre juridique est mis en place depuis 2000 et il est illustratif de l'évolution générale des pays. C'est pourquoi, le connaissant bien, nous avons choisi de développer ici à titre d'exemple ce nouveau cadre français en faisant ressortir ce qui est essentiel et se retrouve dans les pays qui ont adopté la même démarche.

2.1- La loi du 13 mars 2000

Jusqu'à cette date c'était le principe de l'indissociabilité entre un support matériel durable et

l'information qu'il porte, qui faisait la qualité d'une preuve et notamment de la preuve préconstituée d'un acte juridique.

La loi n° 2000-230 du 13 mars 2000 portant **adaptation du droit de la preuve aux technologies de l'information et relatives à la signature électronique**, a été qualifiée de « Révolution numérique ».

1. L'écrit devient indépendant de son support

• En effet, **pour la première fois, est donnée une définition fonctionnelle de l'écrit qui le rend indépendant de son support** :

« 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****. (article 1316 du Code civil). »*

• L'article 1316-1 est **primordial** dans la mesure où il énonce les conditions nécessaires pour que l'écrit sous forme électronique soit admis en preuve au même titre que l'écrit sur support papier : *« « sous réserve que puisse être* **dûment identifié** *la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en* **garantir l'intégrité** *» ».* **Ces notions d'authentification d'une part et d'intégrité d'autre part, vont ensuite être centrales**.

• Enfin, non seulement la loi du 13 mars 2000 n'établit **pas de hiérarchie de la preuve entre le papier et l'électronique**, mais encore elle étend le régime concernant les actes sous seing privé (c'est-à-dire pris entre particuliers) aux actes dont la valeur de preuve est la plus forte dans le droit français, à savoir les actes authentiques (c'est-à-dire établis selon des formalités juridiques et des conditions de forme très précises), et donne alors à la signature une force plus importante que celle que conférait la signature manuscrite des officiers publics, puisque **désormais c'est la signature qui confère l'authenticité à l'acte**.

2. Une définition fonctionnelle de la signature électronique est donnée

Parallèlement, la loi aborde le thème de la signature électronique :

• Elle en donne une définition fonctionnelle

«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 du Code civil).

• Elle précise

«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 […] ».

Là encore, la question du lien entre la signature et l'acte est un point central dans un environnement électronique si facilement falsifiable.

• Elle introduit un mécanisme qui permet de spécifier les conditions selon lesquelles un tel procédé sera non seulement considéré mais de plus, présumé, fiable

«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 » (deuxième partie du second alinéa de l'article 1316-4).

Ces conditions renvoient en fait à une technologie très particulière, à savoir la signature électronique cryptographique à clé publique.

2.2- La signature cryptographique à clé publique

Cette technologie prend sa source dans le domaine de la cryptographie (procédé consistant à chiffrer/masquer un langage clair).

Durant des années, pour pouvoir se communiquer des informations chiffrées, les personnes devaient s'entendre sur une clé privée (secrète).

À partir de la découverte de deux chercheurs de l'Université de Stanford, Whitfield Diffie et Martin Hellman, le mécanisme est désormais fondé sur la séparation de la clé unique en deux clés distinctes :

• une clé privée

• et une clé publique.

La clé privée est utilisée pour le chiffrement et la clé publique pour le déchiffrement.

Ce mécanisme est désigné sous le nom de cryptographie à clé publique, ou encore cryptographie asymétrique :

• avec la clé privée qui sert à la signature

• et la clé publique qui sert à la vérification.

En fait, le mécanisme repose sur trois éléments :

• **la génération d'une empreinte,**

• **la signature de l'empreinte avec une clé privée (secrète)**

• **et l'établissement du lien entre la clé privée et son propriétaire.**

2.2.1. Génération d'une empreinte

L'empreinte (appelé également « condensat »), de taille généralement fixe, est générée à partir du document grâce à une fonction mathématique dite fonction de hachage :

• cette fonction restitue une empreinte indissociable du document dont elle est extraite et qui est d'une longueur fixe ;

• l'empreinte est transmise avec le document

• et à l'arrivée, avec la même fonction, le système calcule une empreinte du document reçu et compare les deux empreintes : si le résultat est identique, cela signifie qu'une probabilité très élevée existe qu'il n'y a pas eu d'altération du document durant la transmission.

Exemple : La moindre modification du fichier entraîne la génération d'une empreinte totalement différente

Soit le texte suivant : « Algorithme MD5 ("Wikipedia, l'encyclopédie libre et gratuite") »

L'empreinte d'un fichier texte ne contenant que ce texte, calculée avec l'algorihtme MD5 est la suivante : « d6aa97d33d459ea3670056e737c99a3d »

En modifiant un seul caractère de ce texte : « MD5("Wikipedia, l'encyclopédie libre et gratuitE") »

Cette empreinte change radicalement et devient : « 5da8aa7126701c9840f99f8e9fa54976 »

2.2.2 - Signature de l'empreinte avec une clé privée (secrète)

Toutefois, durant la transmission, le document et son empreinte auraient pu être subtilisés et remplacés par un autre document avec sa propre empreinte.

C'est la raison pour laquelle

• l'empreinte de départ est signée avec la clé privée (secrète) de son auteur

• et l'empreinte générée à l'arrivée est vérifiée avec la clé publique correspondant à la clé privée et qui, elle, est destinée à être communiquée à quiconque veut vérifier la signature.

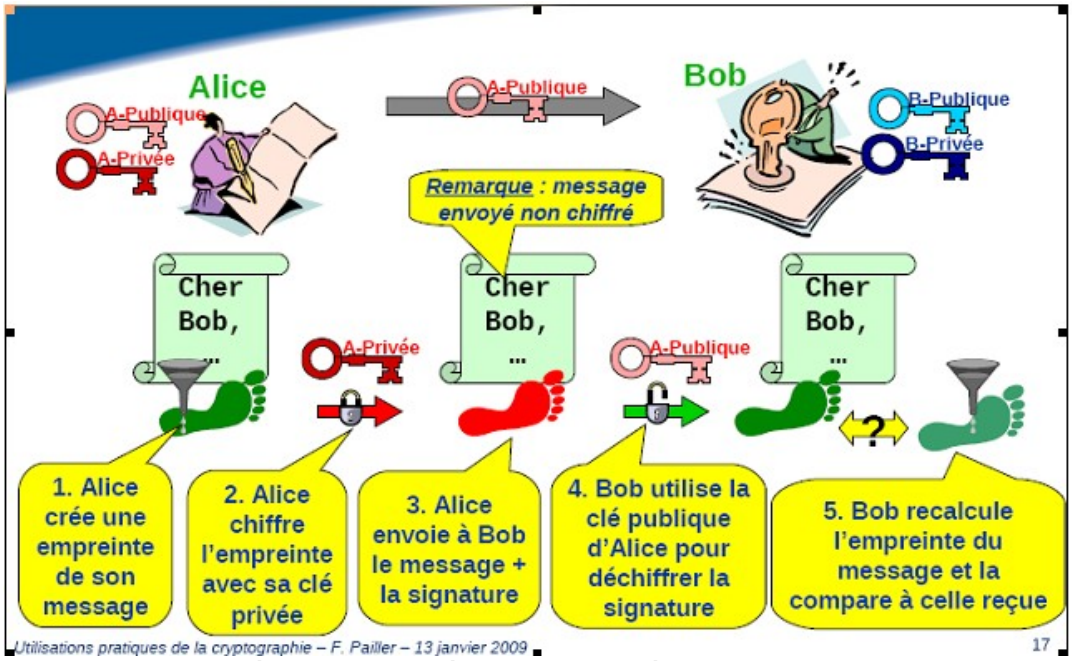
Ainsi

• si l'empreinte permet de s'assurer qu'un document n'a pas été altéré,

• la signature permet en plus de certifier la provenance du document : on parle alors de «

non-répudiation » car l'auteur ne peut pas ne pas reconnaître être l'auteur de l'acte dans la mesure où la clé publique ne peut vérifier positivement que ce qui a été signé par la clé privée correspondante.

Les deux algorithmes les plus connus dans ce domaine sont d'une part MD5 (128 bits) et d'autre part SHA-1 (160 bits).



Représentation schématique du mécanisme de signature.

2.2.3. Etablissement du lien entre la clé privée et son propriétaire

Enfin, il reste à s'assurer du lien entre la clé privée et son propriétaire.

C'est là qu'interviennent alors les prestataires de certification auprès desquels on va faire enregistrer sa clé publique.

Ainsi un tiers (le prestataire) se porte garant que la clé publique est bien la vôtre et, de la sorte, crée un lien :

- entre la clé publique
- et votre identité.

L'enregistrement se fait sur un certificat qui contient un certain nombre d'informations, variables suivant le niveau de sécurité du certificat et du prestataire :

- identité de son propriétaire,
- qualité,
- clé publique,
- etc.

Deux éléments très importants sont

- d'une part la durée de validité du certificat (généralement entre un et trois ans),
- d'autre part les transactions qui sont permises pour ce certificat.

Bien évidemment, le certificat est à son tour signé avec la clé privée du prestataire. Ceci implique, dès lors qu'un système vérifie une clé publique, qu'il commence par vérifier la signature du certificat, avant de vérifier la signature du document envoyé.

Nous pouvons ajouter que le processus de signature électronique tel que nous venons de le décrire vise à garantir l'intégrité du document au cours de son transfert et à donner au

destinataire, la certitude de l'identité de l'expéditeur.

Attention

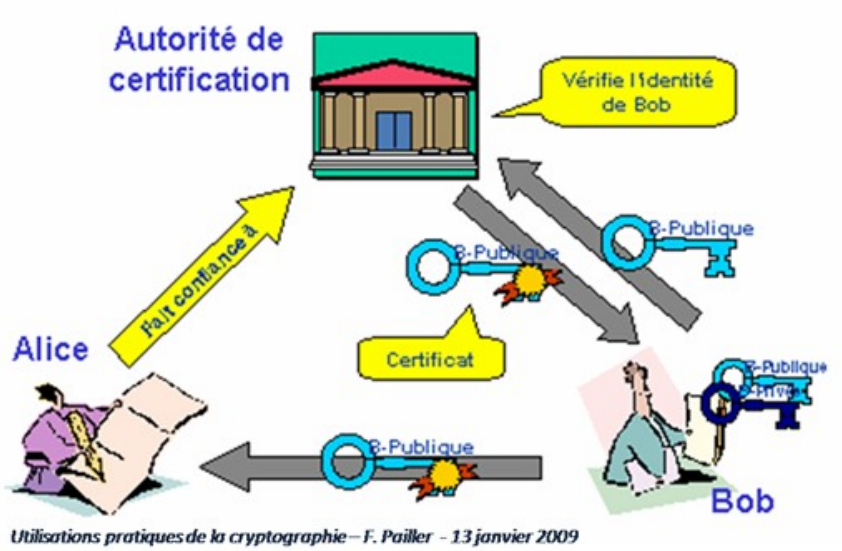
Ce processus ne vise pas à assurer la confidentialité du document.

Cette confidentialité ne pourra être obtenue que si le document lui-même est chiffré.

Des technologies connexes de celles de la signature électronique sont utilisées à cet effet, notamment pour les transactions bancaires.

Exemple

Principe de création d'un certificat



Principe de création d'un certificat

Ce système relativement complexe induit la mise en place d'une infrastructure dite infrastructure à clé publique (ou IGC) et on voit que la vérification d'une signature induit, parallèlement au document proprement dit, la conservation

• notamment des algorithmes de signature utilisés au moment où le document a été signé,

• ainsi que celle des certificats (on doit s'appuyer sur celui qui était valide au moment où le document a été signé).

Complément : Le fonctionnement des certificats

Il existe 4 types de certificats en fonction du niveau de sécurité:

- classe 1 : adresse électronique du demandeur requise;
- classe 2 : preuve de l'identité requise (photocopie de carte d'identité par exemple);
- classe 3 : présentation physique du demandeur obligatoire.
- classe 3+ : identique à la classe 3, mais le certificat est stocké sur un support physique (clé USB à puce, ou carte à puce; exclut donc les certificats logiciels).

Tel qu'on l'utilise en cryptographie et en sécurité informatique, un certificat électronique est un bloc de données contenant, dans un format spécifié, les parties suivantes :

- un numéro de série;

- l'identification de l'algorithme de signature;
- la désignation de l'autorité de certification émettrice du certificat;
- la période de validité au-delà de laquelle il sera suspendu ou révoqué;
- le nom du titulaire de la clé publique;
- l'identification de l'algorithme de chiffrement et la valeur de la clé publique constitués d'une paire de clés asymétriques (comme par exemple RSA);
- des informations complémentaires optionnelles;
- l'identification de l'algorithme de signature et la valeur de la signature numérique

Interface de gestion d'un certificat

Prestataires de Service de Certification électronique qualifiés[1] conformément aux exigences de l'arrêté du 26/07/2004, qui délivrent des certificats qualifiés (Site du ministère de l'Économie, de l'industrie et de l'emploi)
Il n'y a que deux prestataires qualifiés. Chacun de ces prestataires a défini une Politique de Certification :
Banque de France : Politique de certification - Autorité de certification - Signature Gamme "signature qualifiée" version 1.1 du 28 décembre 2006
Notaires de France : Politique de Certification Pour les Certificats Qualifiés Support au Service de Signature. Version : 01.02 du 30/05/2007

Tableau 1 **Les Prestataires de Service de Certification qualifiés en France**

2.3 - Le décret d'application de la loi du 13 mars 2000

C'est cette technologie de signature qui a été ensuite reprise, dans le contexte de l'explosion de l'internet.

Son encadrement juridique va se faire avec :

• d'une part, **la directive européenne du 13 décembre 1999**, dont l'objectif était de faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique,

• d'autre part, le décret d'application de la loi du 13 mars 2000, à savoir le décret n°2001-

1 - http://www.telecom.gouv.fr/rubriques-menu/entreprises-economie-numerique/certificats-qualifies/liste-psce-qualifies-delivrant-certificats-qualifies-1587.html

272 du 30 mars 2001 (**transposition de l'annexe de la directive**).

Que dit ce décret français?

Le décret définit une signature électronique simple et une signature électronique sécurisée, qui reprend en fait la signature électronique avancée qui figure dans la directive. Cette signature sécurisée est fondée sur les technologies de cryptographie à clé publique, soit une signature qui satisfait aux exigences suivantes: « *« être propre au signataire ; être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ; et garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable »* » (art. 1.2).

Par ailleurs, le décret introduit une présomption de fiabilité : «*« La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve du 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. »* » (art. 2).

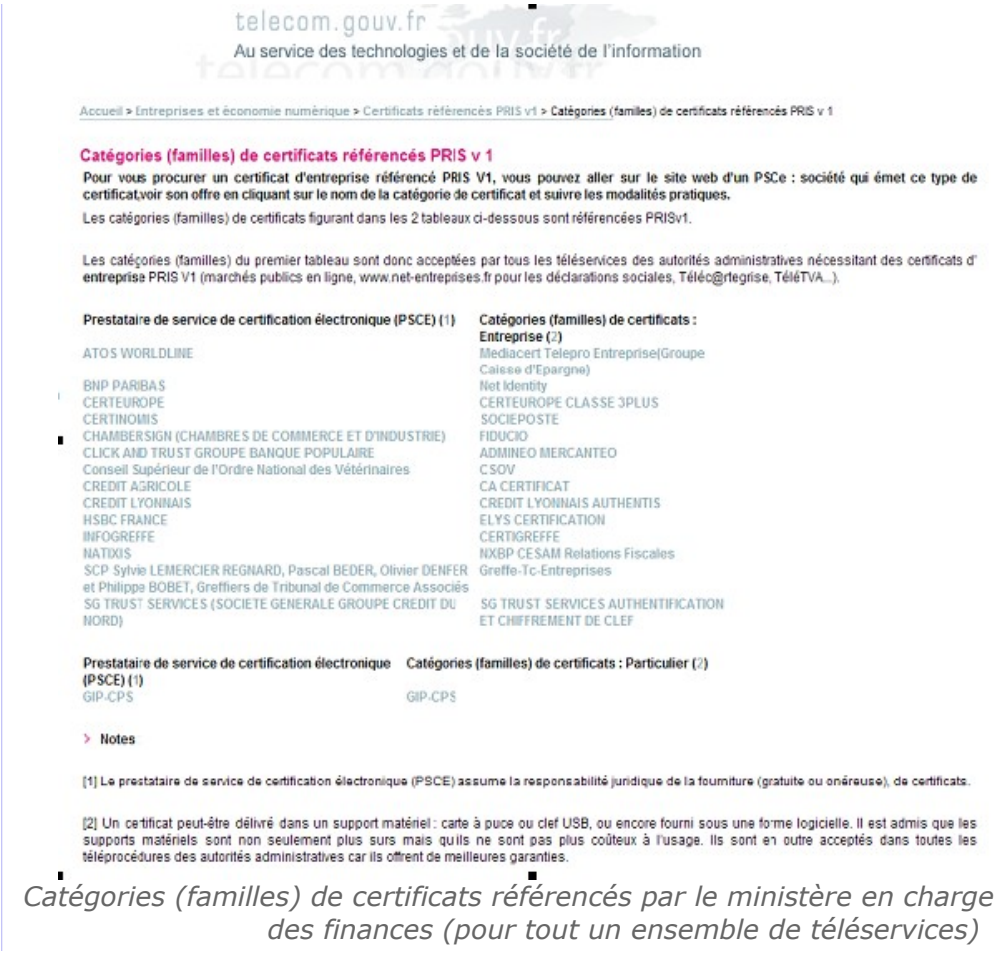
Le décret énonce par conséquent les conditions nécessaires pour qu'il y ait **présomption de fiabilité** que ce soit au niveau

- des systèmes,
- des prestataires de certification
- ou des certificats.

D'autres textes viennent compléter ce décret et fixent notamment les modalités d'évaluation, de certification et de qualification des différents acteurs en présence : comité français d'accréditation et organismes d'accréditation signataires d'un accord européen, centres d'évaluation, prestataires de certification.

Exemple

Catégories (familles) de certificats référencés par le ministère en charge de l'Economie et des finances (pour tout un ensemble de téléservices)



telecom.gouv.fr
Au service des technologies et de la société de l'information

Accueil > Entreprises et économie numérique > Certificats référencés PRIS v1 > Catégories (familles) de certificats référencés PRIS v 1

Catégories (familles) de certificats référencés PRIS v 1

Pour vous procurer un certificat d'entreprise référencé PRIS V1, vous pouvez aller sur le site web d'un PSCe : société qui émet ce type de certificat,voir son offre en cliquant sur le nom de la catégorie de certificat et suivre les modalités pratiques.

Les catégories (familles) de certificats figurant dans les 2 tableaux ci-dessous sont référencées PRISv1.

Les catégories (familles) du premier tableau sont donc acceptées par tous les téléservices des autorités administratives nécessitant des certificats d' entreprise PRIS V1 (marchés publics en ligne, www.net-entreprises.fr pour les déclarations sociales, Télé@rtegrise, TéléTVA...).

Prestataire de service de certification électronique (PSCE) (1)	Catégories (familles) de certificats : Entreprise (2)
ATOS WORLDLINE	Mediacert Telepro Entreprise(Groupe Caisse d'Epargne)
BNP PARIBAS	Net Identity
CERTEUROPE	CERTEUROPE CLASSE 3PLUS
CERTINOMIS	SOCIEPOSTE
CHAMBERSIGN (CHAMBRES DE COMMERCE ET D'INDUSTRIE)	FIDUCIO
CLICK AND TRUST GROUPE BANQUE POPULAIRE	ADMINEO MERCANTEO
Conseil Supérieur de l'Ordre National des Vétérinaires	CSOV
CREDIT AGRICOLE	CA CERTIFICAT
CREDIT LYONNAIS	CREDIT LYONNAIS AUTHENTIS
HSBC FRANCE	ELYS CERTIFICATION
INFOGREFFE	CERTIGREFFE
NATIXIS	NXBP CESAM Relations Fiscales
SCP Sylvie LEMERCIER REGNARD, Pascal BEDER, Olivier DENFER et Philippe BOBET, Greffiers de Tribunal de Commerce Associés	Greffe-Tc-Entreprises
SG TRUST SERVICES (SOCIETE GENERALE GROUPE CREDIT DU NORD)	SG TRUST SERVICES AUTHENTIFICATION ET CHIFFREMENT DE CLEF

Prestataire de service de certification électronique (PSCE) (1)	Catégories (familles) de certificats : Particulier (2)
GIP-CPS	GIP-CPS

Notes

[1] Le prestataire de service de certification électronique (PSCE) assume la responsabilité juridique de la fourniture (gratuite ou onéreuse), de certificats.

[2] Un certificat peut-être délivré dans un support matériel : carte à puce ou clef USB, ou encore fourni sous une forme logicielle. Il est admis que les supports matériels sont non seulement plus surs mais qu'ils ne sont pas plus coûteux à l'usage. Ils sont en outre acceptés dans toutes les téléprocédures des autorités administratives car ils offrent de meilleures garanties.

Catégories (familles) de certificats référencés par le ministère en charge de l'Economie et des finances (pour tout un ensemble de téléservices)

2.4 - Conclusions relatives au nouveau cadre juridique

Le dispositif juridique en place permet par conséquent de dématérialiser des processus métier progressivement sur l'ensemble de la chaîne. **Les notions d'authentification et d'intégrité, à la mesure des dangers du numérique dès lors qu'on utilise les réseaux, sont centrales et ce sont les technologies de cryptographie à clé publique qui sont utilisées pour répondre à ces exigences.**

Des infrastructures sont mises en place qui permettent de sécuriser les échanges, les transactions, les flux de données échangées : **des plates-formes font appel à des services de signature et d'horodatage, qu'on appelle tiers certificateurs, tiers horodateurs. Ces derniers sont appelés les « tiers de confiance », l'idée étant qu'on ne peut pas être à la fois juge et partie et qu'en faisant appel à un tiers pour certifier une signature, une date, on sécurise sa transaction.**

Dans le secteur privé, des « tiers-archiveurs » sont également apparus : on confie à un tiers le soin d'archiver ses données. Ce marché existait déjà pour les archives sur support papier mais, dans la foulée de la nouvelle réglementation en matière de données et de documents nativement numériques, un nouveau marché de tiers archiveurs s'est développé, visant ce qui est alors improprement appelé l' « archivage légal ». Le souci est avant tout de maintenir l'intégrité des données et documents archivés, afin de leur conserver leur valeur légale au sens des articles 1316 et suivants du Code civil français. De même sont apparus de nouveaux types de logiciels visant à assurer des fonctions de sécurisation et traçabilité des données et documents (solutions dites de « coffres-forts électroniques »). La Fédération nationale des tiers de confiance (FNTC) rassemble un grand nombre de ces acteurs.

De même, **deviendra également centrale la notion d'interopérabilité de manière à ce que les systèmes d'informations des partenaires puissent dialoguer par le biais**

de formats de données standardisés, comme par exemple le langage XML, devenu incontournable dans cet environnement. Ce langage permet

- de modéliser les processus, les échanges
- et de faire en sorte qu'un langage commun soit mis en place entre différents acteurs.

Attention

Toutefois, n'ont pas été prises en compte dans l'élaboration de ces différents textes, les questions afférentes

- aux durées de conservation des données et documents ainsi produits,
- aux processus à mettre en œuvre afférents à leur cycle de vie,
- ou encore à leur pérennisation à moyen et long terme.

C. Chapitre 3 - La mise en place de l'administration électronique

L'évolution de la législation en matière de droit de la preuve , on l'a vu, reconnaît une valeur de preuve aux documents sur support numérique.

Nous allons retrouver cette évolution dans l'ensemble des pays car elle vise à donner une confiance juridique indispensable au développement du commerce électronique.

En corollaire, cette évolution va entraîner le développement de ce qu'on appelle l'administration électronique avec la dématérialisation des processus métier qui généralement débute avec la mise en place des télétransmissions et téléservices, et se poursuit avec l'introduction de la signature électronique, ce qui entraîne la production d'originaux numériques qu'il s'agit de conserver, comme on devait conserver les originaux papier.

3.1 - Le développement de l'administration électronique en France et les plans gouvernementaux

Le Gouvernement français souhaite depuis la fin des années 1990, utiliser les nouvelles technologies de l'information et de la communication. Après une première période commençant en 1997 et centrée notamment sur le développement des sites internet gouvernementaux et des premières mises en place de téléprocédures, une accélération a été initiée en 2004 avec le programme stratégique pour l'administration électronique (PSAE) qui, sur une durée de trois ans, prévoit un plan d'action (ADELE) visant à dématérialiser des pans entiers de processus administratifs, dans tous les domaines. Cette accélération s'inscrit dans le nouveau cadre législatif et réglementaire qui vient d'être esquissé et s'appuie sur une agence interministérielle, devenue aujourd'hui une direction interministérielle placée auprès du ministère en charge du budget de l'Etat : la direction générale pour la modernisation de l'État (DGME) autour actuellement de quatre axes : adapter les missions de l'Etat, simplifier la relation avec les usagers, améliorer la qualité des services, optimiser la gestion des administrations.

Parallèlement le secrétariat d 'Etat à l 'Economie numérique a publié en 2008 : « France numérique 2012 : plan de développement de l'économie numérique » qui vise à permettre à tous les Français d'accéder aux réseaux numériques, à développer la production et l'offre de contenus numériques, à diversifier les usages et les services numériques (dont une partie concerne l'administration électronique) ainsi qu'à rénover la gouvernance et l'écosystème de l'économie numérique. Y figure la publication d'un nouveau plan stratégique pour l'administration électronique qui n'a pas encore vu le jour.

3.2- Les référentiels généraux de l'administration et grands domaines couverts par la dématérialisation

Ce développement de l'administration électronique s'appuie sur des référentiels principaux :

- Le premier touche à l'interopérabilité des systèmes d'information : cadre commun d'interopérabilité qui fixe par exemple les protocoles admis ou bien encore les formats de données (domaine essentiel pour la pérennité des données conservées).
- Les référentiels touchent également à la sécurité : politique de référencement intersectoriel de sécurité (PRIS) qui fixe les niveaux de sécurité exigés suivant les types de téléprocédures mises en place.

Ces référentiels n'avaient pas jusqu'alors de caractère officiel. Le Gouvernement a par conséquent fait voter une loi et, en vertu de cette loi, est parue le 8 décembre 2005, une ordonnance qui permet la mise en place de téléprocédures entre les administrations d'une part et entre les administrations et les citoyens d'autre part. C'est ainsi que l'ordonnance met en place le référentiel général d'interopérabilité (RGI) et le référentiel général de sécurité (RGS). Ces deux référentiels seront nourris à partir des dispositifs existants, à savoir le cadre commun d'interopérabilité et la PRIS.

Complément

Concernant les domaines couverts (en France):

Le domaine financier a été précurseur, avec dès 2002, la mise en place de la télé-TVA, de la déclaration de revenus en ligne, ou encore de la dématérialisation de la facture électronique.

De même s'accélère la dématérialisation des échanges entre des partenaires comme les notaires, l'administration du cadastre, des hypothèques…

Depuis ont été dématérialisés le journal officiel lois et décrets ainsi que les marchés publics.

Sont actuellement mises en œuvre ou expérimentées la dématérialisation du contrôle de légalité, celle des demandes des actes de l'état civil, ou encore des premières applications dans le domaine social. Un énorme chantier concerne également la dématérialisation de la chaîne comptable et financière entre les ordonnateurs, les comptables publics ainsi que les contrôleurs, qui s'accompagne également de celle des pièces justificatives à l'appui des dépenses et des recettes (programme HELIOS).

3.3 - L'enjeu d'interopérabilité pour l'archivage

Que retenir de très important?

L'**interopérabilité** se traduit concrètement par la capacité, pour chaque entité administrative dotée d'applications informatiques d'**échanger des données et des services** avec d'autres entités ou avec des citoyens.

Il s'agit par exemple de pouvoir créer, gérer et transmettre des données à partir d'une application A, fonctionnant sur un système d'exploitation et sur un ordinateur donnés et de réutiliser ces données dans une application B locale ou distante, fonctionnant sur le même ou sur un autre système d'exploitation et généralement sur un autre ordinateur, chacun des deux contextes techniques étant susceptibles d'évoluer en fonction de contraintes diverses indépendamment l'un de l'autre.

Pour que cela soit possible dans un **cadre d'entités multiples** qui échangent des informations sous forme numérique, il est nécessaire :

- que la structure des données soit **neutre et indépendante d'une application ou d'un progiciel particulier.**
- que la **description de ces données soit une description standardisée** reconnue par

les différentes entités utilisatrices.

Ces deux orientations techniques, motivées par les besoins d'interopérabilité, facilitent énormément l'archivage de ces informations.

Il est à ce titre intéressant de voir, dans le chapitre suivant, qu'un certain nombre de pays ont fait des choix similaires.

3.4 - Les référentiels et l'intervention des Etats

Pour être interopérables, nous venons de le voir, il convient de rester neutre par rapport à une application particulière et de standardiser la description des données.

Exemple

En France, une version 1.0 du référentiel général d'interopérabilité (RGI) est actuellement publiée sur le site de référence de la DGME, qui attend une validation dans les mois à venir.

Trois niveaux sont traités dans le RGI :

- sémantique (savoir se comprendre),
- syntaxique (savoir communiquer)
- et technique (pouvoir communiquer).

Pour chacun de ces niveaux, le RGI propose un certain nombre de normes, standards et pratiques pouvant être privilégiés lors des échanges. Cette actuelle version du RGI est très peu contraignante dans la mesure où la très grande majorité des prescriptions relèvent de l'ordre de la recommandation (et non de l'obligation ou de l'interdiction).

Le RGI définit ainsi un cadre et un ensemble de règles qui devraient être à terme applicables à tous les services de l'État. Il faut donc une structure neutre et indépendante d'une application particulière

C'est pour cette raison que, dans son volet technique, le RGI définit un ensemble de règles visant à recommander l'usage de codages normalisés pour le codage des caractères, l'usage de PNG v1.2 pour l'échange, la représentation et la conservation d'images fixes non photographiques, l'usage du codage JPEG et du format JFIF (JPEG File Interchange Format) pour les images fixes photographiques de qualité ordinaire, l'usage de PNG ou TIFF/EP (norme ISO 12234) pour les images fixes photographiques de haute qualité, ou encore le format « Open Document Format » (norme ISO 26300) pour l'échange de documents bureautiques et PDF/A-1 (norme ISO 19005) pour leur conservation.

D'une manière générale, le RGI déconseille l'usage de formats propriétaires sauf dans les cas ou il n'y a pas d'alternative.

Complément

Commission européenne

Depuis 2006, la Commission Européenne préconise une interopérabilité entre toutes les administrations nationales et régionales de l'Union Européenne.

Le programme IDABC (Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Business and Citizens) vise à fournir des services administratifs pan-européens en ligne aux administrations publiques, aux entreprises et aux citoyens. L'objectif est d'améliorer l'efficacité des administrations publiques européennes et la collaboration entre elles.

Au sein de ce programme, l'EIF (European Interoperability Framework) joue, au sein de l'Europe, le rôle du RGI en France. Avant sa mise en application contraignante, le RGI sera d'ailleurs validé au niveau européen afin que sa compatibilité avec l'EIF soit assurée.

En juillet 2008, une première version complète de l'EIF a été publiée en vue de recueillir les commentaires externes des administrations nationales, des industriels et des experts du

domaine. Le planning d'élaboration et d'approbation de l'EIF prévoit une publication définitive fin 2008. L'EIF souligne que l'interopérabilité implique l'usage de formats de données ouverts, et par conséquent publiés, libres de droits et d'usage, élaborés dans le cadre d'organismes sans but lucratif, au sein desquels, le processus d'approbation doit être ouvert et accessible à toutes les parties concernées. Les standards propriétaires ont vocation à être éliminés.

De nombreux États membres ont actuellement entrepris de faire évoluer leurs administrations dans la même direction.

Par exemple :

en Allemagne : SAGA (Standards und Architekturen für E-Government-Anwendungen), normes et architectures pour les applications de e-Gouvernement ;

en Grande-Bretagne : e-GIF, cadre commun d'interopérabilité,

en Belgique : BelGIF (BELgian Governement Interoperability Framework) ;

au Danemark : OIOXML, cadre commun d'interopérabilité danois, http://digitaliser.dk/resource/7043

en Norvège : eNorway 2009.

Nous pouvons également observer qu'au sein de ces évolutions, le domaine des informations géographiques revêt une importance toute particulière.

Aux USA

Dès 1994, considérant l'impact des données géographiques sur certains domaines de l'activité économique, sur la gestion des ressources naturelles et sur la protection de l'environnement, le président américain Clinton a signé la directive 12906 faisant obligation à chaque agence relevant du gouvernement des États-Unis de décrire toute nouvelle collection de données géographiques qu'elle aura produite ou reçue, conformément au standard américain FGDC (Federal Geographic Data Committee) de métadonnées.

Quand on connaît la difficulté d'élaboration de métadonnées descriptives pour l'archivage lorsque ces métadonnées n'ont pas été produites en même temps que les données, on perçoit l'impact d'une telle directive.

En Europe

La très importante directive INSPIRE 2007/2/CE du Parlement européen et du Conseil du 14 mars 2007 vise à l'établissement d'une infrastructure d'information géographique dans l'Union européenne.

Elle définit un cadre juridique structurant pour l'accès et l'usage des données géographiques.

Elle a pour objectif de favoriser la production et l'échange des données et des services nécessaires aux différentes politiques de l'Union dans le domaine de l'environnement pris dans un sens large afin qu'il soit aisé de rechercher les données disponibles et d'évaluer leur adéquation à être utilisées, afin que les données soient mises à disposition et maintenues à jour au niveau le plus approprié, afin qu'il soit possible de combiner des données de différentes sources.

La Directive crée un ensemble d'obligations parmi lesquelles la constitution obligatoire et le maintien à jour de métadonnées conformes aux normes ISO19115 et ISO 19119 et d'un profil d'utilisation variable suivant le thème, avec une obligation de fourniture et d'accès gratuit à ces métadonnées, la fourniture des données selon des règles communes, l'application de règles d'interopérabilité des services (identifiants des objets, attributs essentiels, thesaurus multilingue) et, enfin, la mise en place de services en réseau afin de rendre les données et les services accessibles à distance.

Un très grand nombre d'institutions publiques européennes sont concernées par la directive et par voie de conséquence, toutes les entreprises privées en interaction avec ces institutions sont également conduites à prendre en compte certains éléments de la directive.

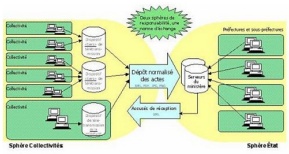
3.5 - Dématérialisation

Comment passer d'une procédure lourde de transmission d'actes papier qui doivent être conforme au droit à une transmission d'actes par voie électronique ?

C'est ce que les pays, gouvernements, administrations, institutions ou organismes divers essaient de mettre en place, ce qui simplifie, valorise le travail effectué par les agents et peut permettre de réaliser des économies substantielles.

Complément

Exemple du contrôle de légalité (France)



Un exemple est ici donné d'une des premières mises en place d'une télétransmission concernant une procédure dite du contrôle de légalité qui implique deux types de partenaires : d'une part les collectivités territoriales et d'autre part les services de l'Etat (préfectures et sous-préfectures).

Le contrôle de légalité exercé a posteriori par l'État (préfectures et sous-préfectures) depuis les lois de décentralisation (1982) sur les actes des collectivités territoriales, leurs établissements publics locaux, les sociétés d'économie mixte locales : délibérations, arrêtés, actes, conventions.

Les collectivités transmettent leurs actes en préfecture, afin que les agents du ministère de l'Intérieur puissent vérifier qu'ils sont conformes au droit. Si des actes sont incomplets, non conformes au droit, ou s'il y a doute sur la portée de l'acte, un dialogue s'organise entre le représentant de l'État et la collectivité se traduisant par exemple par des demandes de pièces complémentaires, des lettres d'observation, et se concluant éventuellement par un déféré devant le Tribunal administratif saisi par le représentant de l'État. Ces procédures s'inscrivent dans des délais précis fixés par la loi.

La transmission de ces actes papier fait l'objet de procédures lourdes, peu valorisantes pour les agents et consommatrices de ressources (frais de poste et consommation de papier, les préfectures et sous-préfectures effectuant des photocopies des actes transmis, réception par les services du courrier de la préfecture/sous-préfecture pour transmission au bureau concerné...). Il a été par conséquent décidé de mettre en œuvre une dématérialisation de cette transmission de manière à automatiser ces tâches : celle-ci a été légalisée par l'article 139 de la loi n° 2004-809 du 13 août 2004 qui autorise la transmission des actes par voie électronique.

Le ministère de l'Intérieur a alors élaboré un schéma XML que doivent respecter les fichiers XML échangés dans le cadre de la dématérialisation du contrôle de légalité. Ce schéma « Actes » est extrêmement structurant dans la mesure où il précise quels sont les messages et les documents qui doivent être échangés ainsi que leur contenu (comme par exemple les métadonnées accompagnant tout acte devant être télétransmis), les règles de nommage des fichiers, leur format, les processus métier.

Un décret d'application n° 2005-324 du 7 avril 2005 explicite les modalités de la transmission : « la commune, lorsqu'elle choisit d'effectuer par voie électronique la transmission de tout ou partie des actes mentionnés à l'article L. 2131-2 [actes qui doivent être soumis au contrôle de légalité], recourt à un dispositif de télétransmission ayant fait l'objet d'une homologation dans des conditions fixées par arrêté du ministre de l'intérieur. L'homologation est subordonnée au respect des prescriptions contenues dans un cahier des charges »…

Site du ministère de l'Intérieur, de l'outre-mer et des collectivités territoriales,

direction générale des collectivités locales (DGCL) : présentation de la

dématérialisation (programme Actes)

http://www.dgcl.interieur.gouv.fr/sections/les_collectivites_te/administration_des_c/regime_des_actes/dematerialisation/

Les dispositifs prévus assurent des fonctions de sécurisation en permettant d'attester que tel acte, tel accusé de réception a bien été télétransmis par tel expéditeur, par tel destinataire, à telle date, telle heure (technologies d'empreinte, signature électronique, horodatage). À l'heure actuelle, quinze dispositifs ont été ainsi homologués dont quatre développés en interne par des collectivités territoriales ou des agences publiques, et onze par des organismes privés.

Deux cas de figures peuvent aujourd'hui se présenter :

- soit les élus disposent d'outils de signature électronique qui leur permettent de signer leurs actes produits sous forme électronique, et dans ce cas les actes ainsi signés deviennent des originaux numériques à conserver sous cette forme, comme étaient conservés les actes sous forme papier ;
- soit l'acte est produit sous forme électronique, édité sur support papier pour recevoir une signature manuscrite. Dans ce cas, c'est la copie numérique qui est télé-transmise et l'orignal reste sous sa forme papier, à conserver telle quelle. Ce second cas de figure rend la question de la prise en charge pour archivage complexe dans la mesure où doivent également être conservées les preuves du contrôle de légalité, à savoir l'accusé de réception numérique, son fichier de signature, son jeton d'horodatage, ce qui tendrait à devoir organiser un archivage mixte (papier et numérique).

Ces dispositifs de télétransmission n'ayant pas vocation à assurer l'archivage des actes ainsi transmis et des messages qui les accompagnent, celui-ci doit être pris en charge par un service d'archives externe par export dans un format défini. Toutefois les modalités de cet archivage sont grandement facilitées par la structuration en amont imposée par le schéma Acte.

3.6 - La dématérialisation et l'archivage

A partir du moment où des originaux numériques avec signature électronique sont produits, il convient nécessairement de les conserver durant les délais requis et même, pour les documents présentant un intérêt patrimonial, à titre définitif .

Les paragraphes qui suivent concernent les actions tant de sensibilisation que d'élaboration de référentiels dans lesquels la réflexion archivistique a pu être prise en compte qui sont menées en France **mais qu'on peut retrouver, suivant les contextes et les environnements, dans beaucoup de pays qui connaissent le même type d'évolutions en matière d'administration électronique.**

3.6.1. Actes authentiques électroniques

En France, la question de la conservation à long terme des actes ainsi dématérialisés s'est posée pour la première fois lors de la discussion du projet de loi du 13 mars 2000 et d'un amendement visant à élargir la portée de la loi aux actes authentiques. Les parlementaires se sont inquiétés de la durée de conservation (à titre définitif) des actes authentiques et des problèmes liés à l'obsolescence des outils et logiciels.

Les questions liées à la conservation de ces actes se sont effectivement révélées relativement complexes et on doit notamment aux professionnels que sont les archivistes d'avoir, au cours des groupes de travail qui se sont constitués pour préparer les décrets d'application de la loi relatifs aux actes authentiques, porté à la connaissance des participants le savoir-faire de cette profession en matière d'archivage électronique.

Complément

C'est ainsi que les décrets n° 2005-972 et 2005-973 du 10 août 2005, relatifs respectivement aux actes authentiques des huissiers et des notaires, intègrent la notion de

métadonnées, à savoir l'enregistrement et la traçabilité des éléments descriptifs et de structure, mais également de gestion et techniques, permettant de retrouver, identifier et caractériser aisément les actes.

De même, la complexité de l'archivage électronique a justifié, entre autres, le choix de mettre en œuvre un minutier central électronique, par profession, les notaires et huissiers transmettant rapidement les actes élaborés et confiant leur conservation à cette structure centrale.

Enfin, pour la première fois, a été soulevée la contradiction

• visant à maintenir d'une part l'intégrité des actes au sens technique du terme (bit par bit), grâce à l'infrastructure à clé publique maintenue autant que nécessaire

• et, d'autre part, la lisibilité sur le moyen et long terme des actes, qui implique notamment de procéder à des migrations de format qui modifient l'acte et par conséquent invalident le procédé de vérification de signature.

Cette contradiction insoluble, dès lors qu'on fait reposer la sécurité juridique d'un acte sur un procédé technologique, a été écartée dans les décrets par un tour de passe-passe juridique servant de parade et visant à poser le fait que les migrations nécessaires à assurer la lisibilité de l'acte ne lui retirent pas son caractère d'original.

Ce même type de raisonnement a été mené dans un certain nombre de pays comme le Canada ou encore les Etats-Unis et a abouti aux mêmes conclusions.

3.6.2. Recommandation du forum des droits sur internet

Ces notions ont été approfondies dans la recommandation du 1er décembre 2005 sur la conservation des documents électroniques dans le secteur privé, du forum des droits sur internet.

La recommandation définit en effet ce qu'on doit entendre par « intégrité » afin d'interpréter l'article 1316-1 du Code civil : cette notion serait assurée en fait, par le respect cumulé des trois critères que sont :

• la lisibilité du document,

• la stabilité du contenu informationnel

• ainsi que la traçabilité des opérations sur le document.

De même, sont encouragées des bonnes pratiques devant se poursuivre tout au long de quatre étapes du processus de conservation que sont :

• le versement,

• l'enregistrement,

• la gestion

• et la restitution des documents.

Concernant la signature électronique des documents originaux, il est stipulé dans la recommandation que leur créateur les vérifie (ou fasse vérifier) avant que le délai du certificat utilisé soit expiré, et que le résultat de cette vérification soit porté dans les métadonnées du document qui sont transférées lors du versement vers un service d'archives.

Plus généralement, il est recommandé que, sous réserve de la possibilité de vérifier l'intégrité des documents conservés (au sens donné plus haut), les opérations successives justifiées par la conservation (et notamment les migrations de formats) ne retirent pas au document, son statut juridique.

La recommandation rappelle également la délibération n° 2005-213 du 11 octobre 2005 que la Commission nationale de l'informatique et des libertés (CNIL), toujours pour le secteur privé, a élaborée en octobre 2005, portant adoption d'une recommandation concernant les modalités d'archivage électronique des données à caractère personnel. La CNIL :

• préconise que la conservation soit divisée en trois périodes de temps, à l'instar des archives publiques (archives courantes, intermédiaires et définitives)

• et recommande que le responsable du traitement établisse des procédures aptes à gérer des durées de conservation distinctes selon les catégories de données qu'il collecte :

• s'agissant des archives intermédiaires, la CNIL recommande que l'accès en soit limité à un service spécifique

• et, pour les archives définitives, qu'elles soient conservées sur un support indépendant avec accès limité au seul service habilité.

Complément

L'archivage proprement dit est entré en 2004 dans l'action 103 d'ADELE (plan d'action visant à dématérialiser des pans entiers de processus administratifs) . Plusieurs chantiers étaient alors prévus dans cette action : sensibilisation des différents acteurs de l'administration électronique, référentiels à élaborer, renforcement des plates-formes d'archivage électronique déjà existantes et de la mise à disposition d'outils pour les collectivités territoriales.

3.6.3. Notion d'authenticité dans un environnement numérique : travaux du groupe InterPARES

Ce groupe de travail interdisciplinaire, installé à l'université de Colombie britannique et dirigée par le professeur Luciana Duranti, cherchait dans un premier temps (InterPARES 1, 1999-2002) à définir les règles et principes nécessaires pour prouver qu'un document numérique présente un caractère d'authenticité.

Complément

Les enquêtes étendues et approfondies menées pendant trois ans dans ce cadre ont abouti à la définition d'un ensemble de quatorze principes et critères.

1- Traiter les documents d'archives d'une manière spécifique au lieu de les considérer comme objets numérisés en général ; c'est-à-dire les traiter en tant que documents créés ou reçus et classés dans l'exercice des activités de travail.

2- Se concentrer sur les documents d'archives électroniques authentiques : un document d'archives électronique authentique est un document qui est ce qu'il est censé être, et qui est dépourvu d'altérations ou de modifications. Par conséquent, prouver l'authenticité d'un document d'archives électronique implique l'établissement de son identité et la démonstration de son intégrité selon les conditions de référence et les conditions minimales d'authenticité. Quand il s'agit d'un document d'archives électronique, on le considère essentiellement complet et inaltéré si le message qu'il est censé transmettre pour accomplir son but est inaltéré.

3. Reconnaître et tenir compte du fait que le risque le plus important encouru par l'authenticité des documents d'archives électroniques se présente pendant leur transmission dans l'espace (par exemple transmission entre individus, systèmes ou programmes d'application) ou dans le temps (par exemple s'ils sont stockés hors ligne ou si le matériel ou le logiciel utilisés pour leur traitement, communication ou maintenance est mis à jour ou remplacé).

4. Reconnaître que la préservation des documents d'archives électroniques authentiques est un processus continu qui commence dès leur création et dont le but est la transmission de documents d'archives électroniques authentiques dans l'espace et dans le temps.

5. Se baser sur le concept de fiabilité dans la tenue et la préservation des documents d'archives et spécifiquement sur le concept de système de gestion des documents d'archives fiable et sur le rôle du conservateur en tant que dépositaire fiable.

6. Se baser sur la reconnaissance du fait qu'il n'est pas possible de préserver un document d'archives électronique de la même manière qu'un objet physique stocké ; on peut préserver uniquement la capacité de le reproduire.

7. Reconnaître que les éléments constitutifs physiques et intellectuels d'un document d'archives électronique ne coïncident pas forcément et que le concept d'élément constitutif numérique est distinct du concept d'élément de forme documentaire.

8. Spécifier les conditions requises pour qu'une copie d'un document d'archives électronique puisse être considérée comme l'équivalent de l'original : en principe, l'original d'un document d'archives électronique est le premier document complet et effectif. Toutefois, dans l'environnement électronique, aucun document ne survit dans sa forme originale. Toute copie fidèle au contenu et à la forme documentaire de l'original doit être considérée comme la copie conforme à l'original, équivalente à l'original quant aux conséquences qui en découlent. Toute copie dont l'authenticité est certifiée par un agent à qui on a confié cette responsabilité est aussi valide que l'original.

9. Intégrer l'évaluation des documents d'archives électroniques dans le processus continu de préservation.

10. Intégrer la description archivistique dans le processus continu de préservation : la description archivistique doit fournir une attestation d'ensemble de l'authenticité des documents d'archives électroniques et de leur relation avec les autres documents dans le contexte du fonds auquel ils appartiennent, en suivant les conditions minimales requises.

11. Affirmer d'une manière explicite que le processus de préservation doit être documenté dans tous ses détails, comme moyen principal de protection et d'évaluation de l'authenticité à long terme.

12. Reconnaître d'une manière explicite que le principe traditionnel, selon lequel

les documents d'archives utilisés dans le cours normal des activités de travail sont présumés authentiques, doit être accompagné, dans le cas des documents d'archives électroniques, par la preuve qu'ils n'ont pas été altérés d'une manière inappropriée.

13. Reconnaître que le conservateur doit à la fois évaluer et maintenir l'authenticité des documents d'archives électroniques. L'évaluation de l'authenticité des documents d'archives électroniques est faite avant leur versement au conservateur et fait partie du processus d'évaluation, tandis que la maintenance de l'authenticité des copies des documents d'archives électroniques a lieu après leur versement et fait partie du processus de préservation à long terme.

14. Faire une nette distinction entre la protection de l'authenticité des documents d'archives électroniques et l'authentification des documents.

3.6.4. Archivage dans les plans gouvernementaux

Il est important que les gouvernements prévoient des actions spécifiques à l'archivage électronique.

Complément

France : plan gouvernemental

Actuellement une action spécifique à l'archivage électronique (action 124) est inscrite dans le plan « France numérique 2012 » : « Prévoir et assurer l'archivage électronique des données et documents numériques » visant à assurer la lisibilité, l'intelligibilité, la fiabilité et l'intégrité de ceux-ci autant que nécessaire.

Un double levier est prévu :

• la détermination du cycle de vie des données et documents dès la conception ou le choix d'un système d'information, en coopération avec l'administration des Archives

• et l'élaboration de politiques d'archivage avant toute mise en œuvre d'un système d'archivage sécurisé.

À ce jour, l'archivage entre dans le champ du RGI et plus précisément dans la partie consacrée à l'interopérabilité sémantique. L'archivage y est abordé :

• sur le plan des ressources à utiliser pour gérer le cycle de vie de l'information notamment pour ce qui concerne les durées de conservation des documents et des données

• sur le plan du contexte de l'archivage en prenant en compte le cadre législatif et réglementaire ainsi que nécessité, sous la forme d'une recommandation, lorsqu'on souhaite mettre en œuvre une plateforme d'archivage électronique, de se conformer au modèle OAIS, et de définir une organisation et une politique d'archivage,

• sur le plan des processus d'archivage avec une recommandation sur le fait de respecter le format d'échange pertinent (le SEDA) (voir dans la section 9 sur les métadonnées),

• sur le plan du sens et de la structuration de l'information archivés en donnant une typologie des métadonnées.

Conseil : Chapitre 3.7- La norme AFNOR NF Z42-013 et ses enjeux en termes d'intégrité, pérennité et sécurité

Voir la partie 5 du module 7 consacrée au modèle OAIS et les normes associées.

La norme AFNOR NF Z42-013 cherche à définir les spécifications techniques à mettre en œuvre pour un système d'archivage électronique visant à assurer la pérennité et l'intégrité des documents.

Ainsi trois supports d'archivage sont acceptés qui sont les WORM (Write Once Read Many) physique, logique ainsi que des supports réinscriptibles. En effet l'intégrité dans les deux premiers cas est assurée par les caractéristiques intrinsèques aux WORM tandis que pour les supports réinscriptibles, la garantie d'intégrité est assurée par des moyens cryptographiques (calcul d'une empreinte, d'une contremarque de temps ou d'une signature électronique), l'intégrité étant définie comme la « caractéristique d'une information qui n'a subi aucune destruction, altération ou modification intentionnelle ou accidentelle ».

On remarque à cet égard que cette définition laisse ouverte la possibilité d'effectuer des conversions de formats (et par conséquent de toucher à l'intégrité physique des trains de bits) pour des besoins de conservation pérenne (la section 6 est d'ailleurs consacrée au choix des formats et à la problématique de leur conversion).

La norme consacre également de nombreuses parties à la sécurité et à la traçabilité du système :

- définition d'une politique d'archivage,
- description précise du dossier technique du système,
- tenue d'un journal des évènements,
- tenue d'un journal du cycle de vie,
- duplication des objets archivés au moins sur deux sites distants.

Attention

Tous les systèmes n'exigent pas les mêmes besoins en termes d'archivage, d'où la définition d'un niveau minimal et d'un niveau supérieur (exigences complémentaires) en termes de pérennité, intégrité et sécurité.

Bibliographie

[Jean-François Blanchette]

Jean-François Blanchette, rapport cité. Voir également « Intégrité, signature et processus d'archivage » » (en collaboration avec Anne Canteaut), La sécurité aujourd'hui dans la société de l'information, L'Harmattan, 2007.

[Premier ouvrage de synthèse sur l'archivage numérique en langue française.]

• BANAT-BERGER F., HUC C., DUPLOUY L., L'Archivage numérique à long terme, les débuts de la maturité? Paris, La Documentation française, 2009.

[Norme de référence essentielle pour comprendre le problème posé par l'archivage numérique]

http://public.ccsds.org/publications/archive/650x0b1(F).pdf