

Cet article vous est offert par votre magazine dematnews.com (Le magazine de la dématérialisation des échanges)

■ Archivage légal et gestion de la preuve, contre les idées fausses (JM Rietsch, Président de FedISA)

Dans l'environnement de la dématérialisation il est sans doute inutile (quoique) de préciser une nouvelle fois que la terminologie « archivage légal » n'a aucune signification réelle mais constitue un raccourci pratique correspondant à la conservation des données de telle sorte que ces dernières puissent être présentées comme éléments de preuve et finalement retenues comme preuve par le juge.



Jean Marc Rietsch

Tout ce que l'on peut lire, voir ou entendre sur le sujet du légal ou de la preuve en matière de dématérialisation et d'archivage électronique a donc pour unique objectif de pouvoir fournir un document électronique (écrit sur support électronique) qui puisse être retenu comme preuve par le juge.

OBLIGATIONS LEGALES

Il est important de rappeler que le juge est seul compétent pour juger de la conformité du système de sécurité (conservation au sens large) et dire si un document électronique est recevable en tant que preuve ou non.

Pour apprécier la conformité du système le juge dispose de plusieurs éléments :

1. les conditions légales prescrites dans les textes ;
2. les normes techniques en vigueur ;
3. les systèmes de certification, de référencement ou de labellisation existant ;
4. les experts informatiques.

Nous ne détaillerons ci-après que les deux premiers points qui nous paraissent essentiels.

1. Conditions légales

Au sens de la loi, pour conférer une valeur probante à un document électronique, sa conservation doit être fiable et sécurisée.

Elle doit ainsi répondre aux exigences suivantes :

- Intelligibilité,
- Identification, garantie de l'origine du document (voir ci-après);
- Intégrité, non modification du contenu informationnel (voir compléments ci-dessous);
- Pérennité.

A ces quatre exigences s'ajoute également la notion importante de confidentialité et d'accès contrôlé à l'information, particulièrement sensible au niveau de la CNIL.

Intelligibilité

Peu importe la forme de l'information, l'essentiel est qu'elle soit restituée de façon compréhensible par l'homme et non par la machine.

Conditions d'identification

La loi de mars 2000 précise par ailleurs que la signature électronique est un des éléments permettant de garantir l'identité de l'auteur voire l'intégrité de l'acte sous certaines conditions que nous ne rappellerons pas ici [prochain article sur la signature électronique dite « sécurisée »]. Par contre la loi ne traite pas des formes et des modalités pratiques (matériels et procédures) d'archivage essentiellement pour deux raisons, d'une part le respect du principe de neutralité technologique et d'autre part afin d'éliminer le risque d'obsolescence. Rappelons de la même façon qu'aucun texte ne précise les conditions de conservation des écrits « papier » en imposant par exemple l'utilisation de méthodes contre les insectes, les bactéries, les incendies ou autres inondations ...

Si la signature électronique est un élément permettant de fournir au juge un gage de crédibilité et de conformité vis-à-vis du document présenté, cela ne va pas sans poser d'autres problèmes. En effet le

recours à la signature électronique nécessité de vérifier la validité de la signature électronique au moment de l'établissement de l'écrit sous forme électronique mais aussi de pouvoir apporter la preuve de la vérification de la validité de la signature (et de l'écrit) sous forme électronique pendant tout le délai de conservation et/ou tout délai de prescription légale devant le juge.

Conditions de l'intégrité

Dans ses recommandations sur la « conservation électronique des documents », le Forum de Droits sur Internet propose en définitive, pour garantir l'intégrité d'un écrit, que trois critères soient cumulativement réunis par le processus de conservation :

- la lisibilité du document,
- la stabilité du contenu informationnel,
- la traçabilité des opérations sur le document.

La lisibilité désigne la possibilité d'avoir accès, au moment de la restitution du document, à l'ensemble des informations qu'il comporte. Cette démarche peut être grandement facilitée par les métadonnées à associer au document.

La stabilité du contenu informationnel désigne la nécessité de pouvoir garantir que les informations véhiculées par le document restent les mêmes depuis l'origine et qu'aucune n'est omise ou rajoutée au cours du processus de conservation. Le contenu informationnel s'entend de l'ensemble des informations, quelle que soit leur nature ou leur origine, issues du document et, le cas échéant, de sa mise en forme.

La traçabilité désigne la faculté de présenter et de vérifier l'ensemble des traitements, opérés sur le document lors du processus de conservation.

Ce qui précède démontre bien qu'en matière d'intégrité il faut absolument faire la différence entre l'intégrité « technique » et l'intégrité « juridique ». Malheureusement seule l'intégrité « technique » a tendance à être véritablement appréhendée et a priori parfaitement contrôlée grâce aux empreintes numériques. Certes ces contrôles d'empreintes sont importants, nécessaires mais largement insuffisants dans le cadre d'un processus complet de conservation.

Pérennité

Doit permettre de respecter les durées de conservation prescrites par les textes en fonction de la nature du document et des délais de prescription.

2. Les normes techniques en vigueur

En ce qui concerne les normes il est important de préciser qu'elles n'ont pas de caractère obligatoire et ne constituent qu'un indice de la fiabilité du système dans la mesure où elles correspondent à la reconnaissance d'un certain « état de l'art ». (prochain article sur les normes utiles en matière d'archivage électronique et autres outils de certification, de référencement ou de labellisation existants)

AVERTISSEMENTS ET PREMIERS ELEMENTS DE SOLUTION

Pour éviter les écueils, définir une politique d'archivage

Au vue de ce qui vient d'être exposé on se rend vite compte que la présentation d'un document en justice afin qu'il puisse avoir des chances sérieuses d'être retenu comme preuve par le juge n'est pas chose facile et en tout cas doit s'entourer d'un maximum de précautions. A cela s'ajoute également le fait qu'un certain nombre de professionnels ou tiers de confiance peuvent intervenir mais encore faut-il que leurs rôles soient parfaitement délimités et surtout que chacun s'y cantonne.

Précisons à ce sujet qu'une façon simple de vérifier la qualité du service de chacun consiste à analyser les responsabilités réellement prises. Ainsi une autorité de certification doit s'engager sur la validité d'un certificat au moment de son utilisation et pour ce faire doit assurer une mise à jour efficace de la liste de révocation. L'autorité d'horodatage ne peut s'engager que sur une date et une heure. Enfin un tiers archiveur doit pouvoir s'engager sur l'intégrité des documents mais au sens uniquement technique ainsi que sur la pérennité de ces derniers.

Comment faire alors pour assurer tout le reste, à savoir : l'intelligibilité, la lisibilité, l'identification, la stabilité, la tracabilité ou encore la confidentialité et les contrôles d'accès ?

Afin de compliquer encore les choses précisons également qu'il n'y a aucune obligation à faire appel à un horodateur ou à un tiers archiveur.

Ne pouvant apporter ici l'ensemble des réponses il nous paraît néanmoins important de préciser qu'en matière de méthodologie, la meilleure façon de procéder afin de ne rien oublier (quant aux objectifs à atteindre) consiste à définir une politique d'archivage qui servira ensuite de base tant pour la définition du système que pour la vérification de sa conformité aux exigences définies dans la politique. Cette dernière sera également régulièrement revue afin de tenir compte des évolutions tant légales que réglementaires.

[\(prochain article sur la politique d'archivage\)](#)

L'autorité de gestion de preuve comme moyen efficace de vérifier la signature électronique

Nous allons maintenant nous intéresser plus particulièrement à la capacité de vérifier la signature électronique. Comme vu précédemment cette vérification doit pouvoir être opérée tout au long du délai de conservation. Deux problèmes se posent alors, d'une part celui de devoir conserver l'ensemble des éléments nécessaires à la vérification dont les CRL (certification revocation list) et d'autre part celui de l'affaiblissement dans le temps des procédés cryptographiques. Sur ce dernier point il est clair que d'ici quelques années le principe utilisé aujourd'hui pour signer sera percé, dès lors il serait alors parfaitement possible de constituer un faux document signé. Une façon de se protéger contre ce phénomène serait alors de systématiquement resigner avec un nouveau procédé fiable l'ensemble des documents conservés ! De quoi faire fuir les plus courageux.

Une autre approche possible, évoquée il y a déjà plusieurs années (projet européen Openevidence IST-2001-35174), revient à faire intervenir un tiers dont le rôle est justement de vérifier la signature le plus tôt possible après son apposition et de garder la trace de cette vérification en établissant une attestation (électronique). Cette dernière est conservée à la fois avec le document et par ce tiers qualifié d'autorité de gestion de preuve. [\(prochain article sur l'autorité de gestion de preuve\)](#)

Le rôle d'une AGP n'est ni celui d'un tiers archiveur, encore moins d'une autorité de certification. Par ailleurs l'AGP pourra s'appuyer sur un tiers horodateur afin de faire figurer une date et une heure certifiées dans l'attestation. Il y a là une véritable prise de responsabilité de la part de l'AGP dont le détail doit se retrouver dans sa politique de gestion de preuve.

Une norme expérimentale (AC Z74-600-1 2 3 4) a également été publiée par l'AFNOR en août 2005 intitulée « Preuves électroniques d'antériorité, de dépôt, de retrait et de réception ».

En conclusion, en matière de « preuve électronique » attention aux termes employés, au contexte et aux belles promesses. Pensez à mettre en place une politique d'archivage dans votre organisation et quoiqu'il en soit vérifier simplement auprès des fournisseurs les engagements effectivement pris, les responsabilités assumées contractuellement et la couverture réelle en cas de sinistre. Mettez ainsi toutes les chances de votre côté afin de faire valoir vos documents électroniques en tant que preuve et surtout afin de ne pas avoir à supporter la charge de la preuve.

[La rédaction](#)

Source :

<http://www.dematnews.com>

Nous vous autorisons à imprimer cet article. Pour toute publication, veuillez nous consulter. Merci de votre compréhension. La rédaction