Projet ICare

Archivage électronique (1) :

Les principes de la conservation juridique

Référence : ICARE/CAB/TPC/DOC_4/v1
Type : Note de travail
Diffusion : Générale

Date : 22/03/2002
Titre : **ICare – Archivage électronique (1) : Les principes de la conservation juridique**

Auteur(s) : Thierry Piette-Coudol, avocat

Résumé :
Ce document expose les exigences de la conservation juridique à partir des textes légaux.

Table des matières

1 Préambule

Les deux années écoulées depuis la réforme de la Loi n°2000-230 du 13 mars 2000[1] instaurant dans le Code Civil l'écrit sous forme électronique sont encore insuffisantes pour mesurer l'ampleur des changements à intervenir sur le fond du droit. Parmi les conséquences à envisager figurera naturellement la question de la conservation, d'autant que l'article 1316-1 issu de la loi vient à propos rappeler que l'écrit sous forme électronique doit être conservé. Cette nouvelle variété d'écrit devra se couler dans le moule général des actes sous-seing privés traditionnels dont on doit préciser aujourd'hui qu'ils sont rédigés sur un "*support papier"*. Mais le monde de l'électronique et qui plus est, celui de l'écrit électronique, est trop récent pour que le législateur ne s'aventure à donner des indications sur l'esprit qui doit présider à la conservation légale et sur les pratiques à déployer lors de l'archivage. Pourtant l'article 1316-4, qui procède de la même loi mais ne vise que la signature, donne à penser au juriste en réclamant un procédé technique fiable.

Conservation et archivage - Une précision lexicographique débutera utilement ce texte sur les termes de *conservation* et d'*archivage*, employés quelquefois indifféremment. Ces termes visent des opérations proches et semblables dans l'esprit du public, les juristes privilégiant le terme de conservation et les techniciens préférant celui d'archivage. Toute réflexion dans ce domaine tourne autour d'un élément matériel sur lequel les mesures de conservation et d'archivage portent, l'*archive*, objet de prédilection d'une profession spécifique, les archivistes. La loi n°79-18 sur les archives[2] définit de la façon suivante cet élément central :

> *"Les archives sont l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale, et par tout service public ou privé dans l'exercice de leur activité. La conservation de ces documents est organisée dans l'intérêt public tant pour les besoins de la gestion et de la justification des droits des personnes physiques ou morales, publiques ou privées, que pour la documentation historique de la recherche".*

Cette riche définition corrobore le sentiment dans l'aspect juridique de la conservation d'une part, et dans l'aspect technique de l'archivage, d'autre part. Un autre terme, le *stockage*, sera rencontré plus rarement. Ainsi la Directive 2001/115[3] propose indirectement une définition du stockage en précisant comment il est effectué (article 2 point e) : "*au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et en utilisant le fil, la radio, les moyens optiques ou d'autres moyens électromagnétiques*". Cependant le terme d'archivage renvoie l'image d'un procédé dynamique qui permet de mettre en œuvre la conservation d'éléments matériels, alors que le stockage suggère l'idée d'un état statique pour les éléments conservés.

Les normes techniques n'ignorent pas les significations respectives des deux termes. Par exemple, la norme technique internationale ISO 15489[4] qui définit la conservation comme l'ensemble des "*actions et tâches concourant à la pérennité technique et intellectuelle des documents authentiques"*[5]. Quant à l'archivage pris dans son ensemble, le système d'archivage : *système d'information qui intègre les documents, les organise, les gère et les rend accessibles à terme"*[6].

Lorsque sera identifié ce qui doit être conservé et que seront connus les principes de la conservation, le procédé technique d'archivage pourra prendre le relais, en respectant étape par étape lesdits principes.

---

[1] Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique (JO du 14 mars 2000 p. 3968)

[2] Loi n°79-18 sur les archives, JO du 5 janvier 1978, p. 43.

[3] Directive n°2001/115/CE du Conseil du 20 décembre 2001 modifiant la directive 77/388/CEE en vue de simplifier, moderniser et harmoniser les conditions imposées à la facturation en matière de taxe sur la valeur ajoutée (Journal officiel des Communautés européennes du 17.1.2002 n°L 15/24).

[4] Norme ISO/DIS 15489 (SOURCE : ISO TC 46/SC 11), en date du 29 mai 2000 dites " Records Management". Traduction française par l'AFNOR du document officiel en langue anglaise.

[5] Norme ISO 15489, chapitre 3 Termes et Définition, 3.4.

[6] Norme ISO 15489, chapitre 3 Termes et Définition, 3.17.

2 La recherche d'un procédé de conservation fiable

La conservation, obligation générale posé par le droit, est en quelque sorte le résultat final à atteindre, sans que la loi indique les moyens à employer. Aussi peut-on procéder par analogie pour se doter d'une doctrine. La référence à quelques textes juridiques, sans négliger les compléments apportés par les normes techniques, montre quels sont les principes à respecter en mettant en application la doctrine élaborée. Enfin les moyens devront être mise en pratique et formalisés au niveau instrumentaire.

La loi n°2000-230 du 13 mars 2000 a créé dans le Code Civil une double modalité pour les actes sous-seing privés : les écrits sur support papier et les écrits sous forme électronique. La loi a encore reconnu une seconde modalité pour les signatures : à la traditionnelle signature manuscrite, vient s'adjoindre la signature électronique. Après avoir formulé pour la première fois en droit français une définition de la signature, qui s'applique aussi bien à la signature traditionnelle qu'à la signature électronique, l'article 1316-4 donne quelques précisions sur cette dernière. La signature électronique est un "*procédé fiable d'identification*". Dans le monde de l'écrit, le procédé "manuel" de signature est sans doute bien réel, quoique peu visible. Il en va différemment dans le monde de l'électronique où une action aussi simple que le tracé d'une signature ne peut survenir qu'au terme du déroulement d'un véritable procédé technique. Un autre point, plus juridique celui-ci, est dans la fiabilité du procédé. Le procédé doit être fiable c'est-à-dire susceptible d'aboutir à la fin pour lequel il a été mis en œuvre. La sanction, juridique, est la suivante : si la fiabilité du procédé est établie, le procédé bénéficiera d'une présomption légale.

Pourquoi ne pas s'inspirer de cette démarche pour l'a conservation de l'écrit électronique ? La valeur probante de l'acte sous seing privé sous forme électronique ne peut être issue que d'un procédé fiable de conservation. Le procédé de conservation ne sera fiable que si dans un premier temps, il prend en considération les exigences contenues dans l'article 1316-1, mais la recherche juridique doit porter plus loin en intégrant d'autres exigences issues de textes épars. Le résultat des recherches permettra de revenir sur une question qui semblait triviale au premier abord : que veut-on conserver ? L'acte sous-seing privé, naturellement, mais d'autres éléments seront à archiver, tant il est vrai que la signature a mené les plus éminents auteurs à revenir sur le droit de la preuve.

2.1 La notion de procédé fiable de conservation

Par analogie avec le dispositif de l'article 1316-4 du Code Civil, on peut estimer que la plus grande efficacité juridique sera atteinte par un "procédé fiable de conservation". Déjà en septembre 1998, le Conseil d'Etat avait publié un important rapport, *Internet et les réseaux numériques*, disponible sur le Web et à la Documentation Française. Dans le chapitre 2 consacré à "*la reconnaissance de la valeur juridique du document et de la signature électronique*", le Conseil parlait de la fiabilité des techniques et apportait les précisions suivantes sur les effets juridiques :

> *La fiabilité est conditionnée par le respect des exigences suivantes :*
>
> *intégrité : elle est liée aux données qu'elle authentifie et, elle est créée dans des conditions qui permettent la conservation des données et le respect de leur intégrité ;*
>
> *imputabilité : elle est imputable au signataire qu'elle identifie."*

En ce qui concerne la preuve, le rapport indiquait quelle pourrait être la démarche du juge face à des écrits électroniques :

> *"Il reviendra au juge, si la fiabilité de la signature ou la conservation du message sur support durable sont contestés, de procéder aux vérifications nécessaires par l'intermédiaire d'un expert ... Si le message est signé et conservé de façon durable il sera admis en preuve dans des conditions identiques à un écrit original."*

Le rapport brosse en quelques phrases l'ensemble des contraintes à suivre.

Dans le domaine électronique, les normes techniques qui dirigent les processus concourant à la formation et à l'échange des écrits électroniques interviennent également dans l'archivage, modalité technique de la conservation juridique. A cet égard, on peut se référer en toute confiance à un document de spécifications

techniques tel que la norme ISO 15489 qui déclare dans le même ordre d'idée : "*Un document fiable est un document dont le contenu peut être considéré comme la représentation complète et exacte des opérations, des activités ou des faits qu'elles attestent, et sur lequel on peut s'appuyer lors d'opérations, d'activités ou de faits ultérieurs*" (point "8.22 Fiabilité" de la norme). La finalité juridique de l'archivage respectant des spécifications techniques préétablies est parfaitement claire dans le texte de la norme ISO/DIS 15489 :

> *La normalisation des principes et des procédures de « Records management » garantit que tous les documents d'archives bénéficient de l'attention et de la protection appropriées et que leurs valeurs de preuve et d'information sont susceptibles d'être mises en évidence plus efficacement et plus facilement en ayant recours à des pratiques et des procédures normalisées. Les documents d'archives permettent de fournir une protection et un soutien en cas de litige, ceci incluant la gestion des risques du fait de l'existence ou de la non-disponibilité d'une preuve" ("Introduction" de la norme).*

2.2 Les sources légales de la fiabilité

Comment assurer pratiquement la fiabilité ? Ce résultat sera atteint en mettant en œuvre des moyens techniques présentant certaines garanties de sécurité recherchées par les lois. Ainsi l'article 1316-1 du Code Civil indique quelles sont les garanties de sécurité technique dont l'écrit sous forme électronique a besoin pendant son cycle de vie :

> *"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."*

Les garanties techniques demandées sont l'identification de l'auteur de l'acte et intégrité de l'écrit.

Ce texte moderne ne doit pas faire oublier un des textes précurseurs en matière de transport électronique, la loi numéro 1994–126 du 11 février 1994, dite loi Madelin. L'article 1 de la loi vise le domaine d'application, les déclarations d'une entreprise destinée à une administration ou organisme assimilé. Selon les termes de l'article 4 :

> *"toute déclaration (...) peut-être faite par voie électronique dans des conditions fixées par voie contractuelle.*
>
> *Ce contrat précise notamment, pour chaque formalité, les règles relatives à l'identification de l'auteur de l'acte, à l'intégrité, à la lisibilité et à la fiabilité de la transmission, à sa date et à son heure, à l'assurance de sa réception ainsi qu'à sa conservation".*

On y retrouve l'identification et l'intégrité exigées désormais par le Code Civil ainsi que la conservation qui est le thème de la présente analyse.

La technique se fait l'écho des mêmes besoins dans une formulation plus générale. La norme ISO 15489 parle d'*authenticité* avec un contenu qui reprend la plupart des attentes de l'article 4 :

> *"Un document authentique est un document dont on peut prouver :*
> - *qu'il est bien ce qu'il prétend être,*
> - *qu'il a été effectivement produit ou reçu par la personne qui prétend l'avoir produit ou reçu,*
> - *et, qu'il a été produit ou reçu au moment où il prétend l'avoir été.*

On retrouve ici l'identification de l'auteur. Quant à la préoccupation que le document soit bien celui qu'il doit être, le fait sera avéré à destination si le document est bien resté intègre.

Il importe de faire le point dans l'état actuel du droit sur les garanties de sécurité techniques qui, si elles sont assurées, permettent d'attester de la fiabilité du procédé de conservation.

3 La fiabilité du procédé et les garanties de sécurité

La loi n°2000-230 du 13 mars 2000 privilégie l'importance de certaines garanties de sécurité. Mais si certaines ont été retenues, d'autres posées par des textes juridiques plus anciens ont été écartées. Enfin d'autres garanties de sécurité à ce jour encore ignorées par le droit peuvent renforcer la fiabilité des procédés.

3.1 Les garanties écartées : la durabilité et la fidélité

La première qualité d'une bonne archive est la durabilité. Dans son rapport précité, le Conseil d'Etat avançait qu'un message électronique pouvait tenir lieu d'acte sous seing privé "*dès lors qu'il est assorti d'une signature fiable et qu'il est conservé avec celle-ci de façon durable"*. Pour solutionner la question de la preuve de l'acte sous seing privé électronique, on pouvait tenter de procéder à une extension du système de la "*copie fidèle et durable"* de l'article 1348 du Code Civil. L'article 1348 définit le concept de durabilité :

> *"Est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support".*

Cependant une solution technique se positionne dans le cadre de cette durabilité, celle des disques WORM. Le support WORM "est un support optique pour lequel l'écriture des bits codant les données se fait par transformation irréversible d'un ou de plusieurs constituants de ce support", comme l'énonce la définition (point 3.7) d'une norme française basé sur ce moyen technique, la norme NF Z 42-013. La norme NF Z 42 - 013 Archivage électronique est une liste de spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes. C'est une norme française homologuée par décision du directeur général d'AFNOR le 20 novembre 2001 pour prendre effet le 20 décembre 2000. La norme selon son préambule "*fournit un ensemble de spécifications concernant les mesures techniques et organisations d'aide à mettre en œuvre pour l'enregistrement, le stockage et la restitution de documents électroniques afin d'assurer la conservation et l'intégrité de ceux-ci*".

Cependant la durabilité de l'article 1348 ne semble pas pouvoir être appliquée au cas des échanges électroniques ou des supports magnétiques. De plus, les changements de supports lors de la conservation d'un même écrit posent problème. La solution ne sera pas reprise dans la loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve. Pourtant le dictionnaire apporte une nuance intéressante. Pour le Petit Robert, la durabilité est le "*temps d'utilisation d'un bien*". L'élément supplémentaire est le délai, la période pendant lequel le bien est censé perdurer. L'article 1348 qui vise un état *irréversible* du support faisait plutôt référence à la pérennité[7]. Certaines contraintes d'exploitation technique font que les messages électroniques, comme tout fichier de données, sont archivés un temps plus ou moins long pour des raisons de sécurité (sauvegarde) ou de contrôle. Lorsque les messages électroniques sont des actes sous seing privés sous forme électronique, la durée de la conservation est dictée par les exigences légales et non plus par les contraintes techniques. La norme ISO 15489 ne s'y trompe pas en indiquant d'emblée que :

> *"les décisions relatives à la durée de conservation des documents dans un système d'archivage sont basées sur une évaluation des exigences issues de l'environnement réglementaire, des obligations légales et économiques et des risques encourus. "*

Cette norme technique internationale qui intègre d'emblée la dimension juridique fait un bon tour d'horizon des raisons et des enjeux de la conservation et de l'archivage, aussi bien sur le plan technique que sur le plan juridique. La norme ISO 15489 considère de façon très extensive *l'environnement réglementaire* qui comprend selon une énumération du chapitre 5 :

- la législation dans les domaines administratif et judiciaire et la réglementation spécifique du secteur d'activité concerné, ainsi que les lois et règlements relatifs aux documents d'archives, à l'accès à l'information, au respect de la vie privée, à la notion de preuve, au commerce électronique et à la protection des données ;
- les normes obligatoires ;
- les codes de bonnes pratiques adoptés volontairement ;

[7] Selon le Petit Robert, la pérennité est le "*caractère de ce qui dure toujours*".

- les codes de conduite ou d'éthique adoptés volontairement ;
- les attentes identifiées de la collectivité en matière de comportement des organismes ou entreprises dans le secteur d'activité concerné.

Autre garantie de sécurité demandée par l'article 1348 du Code Civil sans définir le concept, la *fidélité*. La définition est apportée par la norme Z 42-013 de la façon suivante :

> *Fidélité d'un document par rapport à document d'origine, un document est considéré comme fidèle au document d'origine s'il permet de reconstituer toute l'information nécessaire aux usages auxquels le document d'origine est destiné.*

Une des finalités de la norme est bien la fidélité comme elle l'indique dans son introduction :

> *"L'ensemble des prescriptions contenues dans la présente norme vise à permettre que des documents électroniques soient produits et, stockés et restitués de telle façon que l'on puisse être sûr de leur intégrité et de leur fidélité par rapport au document original".*

Sans qu'il soit utile de gloser sur le concept de fidélité, on conviendra que si l'intégrité d'un écrit électronique a été maintenue pendant l'échange électronique, il reste fidèle à son contenu d'origine.

3.2 Les garanties secondaires : la lisibilité et l'intelligibilité

La *lisibilité* est le fait de pouvoir être lu par l'œil humain. Cette garantie ou cette qualité de lisibilité doit être présente pendant la transmission de l'écrit ainsi qu'à l'arrivée. C'est surtout par les effets juridiques attachés que la lisibilité est importante : elle garantit que l'écrit électronique pourra recevoir le traitement juridique approprié. Dans les services à valeur ajoutée du marché positionnés en intermédiaire entre émetteur et destinataire des messages, la lisibilité est attestée par le service par l'envoi à l'émetteur d'une sorte d'accusé de réception plus ou moins spécifique. La demande de lisibilité va plus loin dans le monde des déclarations administratives sous forme électronique, appelées *téléprocédures* ou *téléservices*[8]. Ces déclarations lorsqu'elles ont sur support papier doivent être produits par les administrés sur des formulaires ad hoc, au design et au contenu prédéfinis par le CERFA[9]. La structuration et le rubriquage des déclarations lorsqu'elles sont sous forme électronique garantissent bien mieux que la lisibilité. Elles garantissent l'*exploitabilité*. Parmi les services à valeur ajoutée, on peut citer les portails sur le WEB permettant la transmission des téléprocédures. Le portail de l'Ordre des experts-comptables, www.jedeclare.com , prévient l'utilisateur "*dans le cas où le message serait illisible*". Lorsque le message est lisible, un contrôle sémantique est réalisé. Le portail envoie ensuite au déclarant un Avis de Conformité Signé (ACS) (art. 2 et 4 des conditions générales d'adhésion au service téléchargeable sur le site). Le message sera alors exploitable par l'administration, destinataire final du message.

Proche de la lisibilité de l'article 4 du 11 février 1994, l'article 1316 parle d'*intelligibilité*. L'article 1316 définit la notion d'écrit, sur papier ou sous électronique :

> *[l']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."*

Si l'écrit électronique est intelligible à sa création et pendant sa transmission, il le reste pendant sa conservation. Le sens de "intelligible" n'est pas précisé. Est-ce un synonyme à "lisible" ? La nécessaire intelligibilité sert-elle à exclure les assemblages de caractères sans signification compréhensible ? La notion d'intelligibilité permet d'éviter le rejet de certains écrits électroniques provisoirement illisibles : les messages chiffrés par des mesures

[8] Sur la notion de téléprocédures et de téléservices comme sur les premières expérimentations mises en place, voir le site WEB www.service-public.fr

[9] CERFA et l'abréviation de Centre d'Enregistrement et de Révision des Formulaires Administratifs. Actuellement régi par un Décret n°90-1125 du 18décembre 1990, le CERFA reçoit les projets de questionnaires et de formulaires qui lui sont adressés par toutes les administrations d'Etat quel qu'en soit le support pour les examiner dans un souci d'harmonisation, de normalisation et de simplification.

cryptologiques. Pour peu qu'on possède la clé cryptographique nécessaire au déchiffrement, l'intelligibilité se transforme en lisibilité !

Comment la lisibilité –ou l'intelligibilité- doit-elle être satisfaite pour qu'en fin de processus de conservation c'est-à-dire au moment du désarchivage, le texte soit intelligible. Les messages ont été créés, éventuellement transmis, puis présentés à l'archivage sous un certain format, celui de leur logiciel de traitement ou de présentation, par exemple un traitement de texte. Au moment du désarchivage, ce logiciel n'existera peut-être plus. Sauf à archiver par la même occasion, les logiciels applicatifs et les fichiers en procédant, la prudence consiste à archiver le message dans un format indépendant du logiciel de traitement. Il existe quelques formats qui permettre de décrire complètement la structure et le contenu des messages électroniques indépendamment des applications et des environnements informatiques, notamment :

- les documents balisés EDIFACT (ISO 9735)
- les documents balisés SGML (NFEN 28879)[10],
- le mode texte ISO/CEI 8859 parties 1 et 15 et ISO/CEI 10646-1),

Lorsque les documents proviennent de logiciels qui ont leurs propres formats d'encodage, ces documents doivent être convertis dans un des formats ci-dessus avant leur stockage. La norme Z42-013 décrit cette problématique. Elle précise quelles sont les caractéristiques des formats de représentation ou de description susceptible d'offrir une possibilité de conversion[11] dans les formats cités. Cette méthode permet d'éliminer certains formats "exotiques" d'une part et de laisser la porte ouverte à d'autres formats qui apparaîtraient dans l'avenir. Pour être retenus, la norme prévoit que les nouveaux formats doivent bénéficier au minimum des caractéristiques suivantes: "*compatibilité ascendante des différentes versions des spécifications, spécifications publiées et accessible librement, possibilité de représenter des documents monopages aux multipages dont le contenu peut-être une combinaison de textes, d'images ou de graphiques*".

La norme technique ISO 15489 va plus loin. La lisibilité et l'intelligibilité doivent permettre d'établir la pertinence de la syntaxe et la sémantique. Il s'agit alors bien d'assurer l'*exploitabilité* des messages électroniques archivés :

> *"un document exploitable est un document qui est localisé, repéré, décrit et analysé. Il est susceptible d'être décrit plus largement dès lors qu'il est relié à l'activité ou à l'opération qu'il l'a produit. Il convient que les liens contextuels des documents portent les informations nécessaires à la compréhension des opérations qui les ont crées et utilisés. Il devrait être possible d'identifier un document dans le contexte d'activités ou de fonctions élargies. Il convient de maintenir les liens entre les archives qui documentent une succession logique d'actions".*

Quoiqu'il en soit, un texte prévoit une garantie de lisibilité à intégrer prochainement dans le droit interne. Il s'agit de la *Directive 2001/115/CE du Conseil du 20 décembre 2001 modifiant la directive 77/388/CEE en vue de simplifier, moderniser et harmoniser les conditions imposées à la facturation en matière de taxe sur la valeur ajoutée*. Ce texte incite les Etats Membres à accepter les factures électroniques "*à condition que l'authenticité de leur origine et l'intégrité de leur contenu soient garanties*" soit par des messages EDI soit en validant les factures électroniques par une signature électronique avancée. L'article 2.2.3.d) de la Directive indique que les mesures de sécurité doivent rester les mêmes pendant les opérations techniques :

> *"l'authenticité de l'origine et l'intégrité du contenu de ces factures, ainsi que leur lisibilité, doivent être assurées durant toute la période de stockage".*

L'article poursuit en posant que les Etats peuvent imposer l'archivage de la pièce sous sa forme originale (écrit ou électronique) et que dans le cas d'un archivage électronique, "*les données garantissant l'authenticité de l'origine et l'intégrité du contenu de chaque facture soient également stockées*". Le texte montre in fine la prééminence d'autres garanties de sécurité déjà connues du droit français : identification et intégrité.

10 Dans le cas des documents à balises SGML, s'il existe une DTD (définition type de document), celle-ci doit être incluse dans le dossier de description technique du système.

11 Conversion selon la norme ISO 15489 : "*action de transférer des documents d'un support à un autre, ou d'un format à un autre*".

3.3 Les garanties principales : le balancement entre l'identification et l'intégrité

L'article 1316-1 du Code Civil indique quelles sont les garanties de sécurité technique dont l'écrit sous forme électronique a besoin pendant son cycle de vie :

> *"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."*

L'identification permet d'attribuer un écrit à son auteur ; l'intégrité est la garantie que l'écrit n'a pas été altéré au cours des traitements.

Le cycle de vie de l'acte sous-seing privé sous forme électronique comprend trois étapes principales :
- la *création* puisque l'article 1316-1 indique qu'il est "établi",
- la *transmission* puisque l'article 1316 envisage toutes les modalités de transmission[12],
- et la *conservation* visée par l'article 1316-1.

Toute démarche de sécurisation pendant le cycle de vie d'un acte sous forme électronique se traduit par un balancement entre les deux garanties :
- Au moment de sa création comme préconstitution de preuve, l'identification est très forte; l'intégrité est surtout nécessitée par l'absence de *support* de la forme électronique.
- Pendant l'échange, l'identification ne doit pas être perdue de vue, de même que l'intégrité de l'écrit ne doit pas être remise en cause, intentionnellement ou non.
- C'est l'utilisateur qui prend l'initiative de la conservation et c'est probablement lui qui procédera au retour de l'archive. L'identification est alors acquise et constante. Par contre, il faudra conserver les archives pendant un temps plus ou moins long, tout au moins pendant la durée de conservation légale. Autant dire immédiatement qu'à l'issue de la période d'archivage, l'archive devra être dans le même état qu'elle était au début du processus : l'intégrité est prédominante dans cette phase.

Toutes combinaisons de moyens techniques garantissant l'identification et l'intégrité sont admissibles. Les moyens du marché sont nombreux. Un de ceux–ci doit être particulièrement signalé : la signature électronique[13]. Ce moyen apporte en standard l'identification et l'intégrité, ce que le droit a bien intégré. L'article 1316-4 du Code Civil exige pour une signature électronique reconnue par le droit un procédé d'identification dont la fiabilité sera avérée à condition que l'identité du signataire soit assurée et l'intégrité de l'acte garantie dans des conditions fixées par Décret en Conseil d'Etat[14]. La signature électronique se présente comme un moyen primordial de fiabiliser la conservation. Au demeurant, le moyen ne figurant pas en toutes lettres dans le corps de l'article 1316-1 n'est pas obligatoire. Toute autre combinaison de moyens garantissant identification et intégrité pourrait être retenue.

Si on se place dans l'hypothèse de base, celle d'un message électronique signé à conserver, arrêtons-nous encore quelques instants pour examiner comment la signature assure l'identification de la personne. Sans qu'il soit besoin ici d'exposer les caractéristiques et le mode opératoire de la signature électronique, l'élément d'identification personnel est le bi-clé cryptographique. La clé privée sert à créer la signature électronique par le biais du Dispositif Sécurisé de Création de Signature aux termes du Décret n°2001-272 du 30 mars 2001. Comme l'hypothèse traite de l'archivage dans la phase post-transactionnelle du cycle de vie du message, on peut ignorer ici la clé privée. Reste la clé publique qui sert également à l'identification de la personne. Au demeurant, l'identification ne peut être *assurée*, comme le demande l'article 1316-4 du Code Civil que par l'intervention d'un tiers certificateur. Naturellement pour avoir confiance dans la signature électronique, toute personne intéressée, le destinataire du message signé par exemple, devra la vérifier grâce à un dispositif de vérification de signature (termes du décret précité) à qui sera fourni le certificat contenant la clé publique. Il apparaît alors clairement que la garantie d'identification n'est pas un attribut immédiatement visible ; elle demande à être vérifiée. Au niveau de la conservation, l'acte sous seing privé ne peut être réputé satisfaire à l'identification de l'article 1316-1 du

[12] Article 1316 du Code Civil : "*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.*"

[13] Les travaux de l'ISO donne dans une norme ISO 7498-2 (1989) la définition de la signature électronique : "*données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de donnée et protégeant contre la contrefaçon (par le destinataire par exemple)*".

[14] 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 (JO du 31 mars 2001 p. 5070)

Code Civil par la seule présence d'une signature électronique. La signature doit être *vérifiée* dans la phase transactionnelle et *vérifiable* dans la phase post-transactionnelle, ce qui ne pourra pas être fait matériellement, sans clé publique et juridiquement, sans clé publique attestée par un certificat. Le certificat devra dès lors être archivé en renfort du message signé.

3.4 La priorité donnée à l'intégrité

Le concept d'intégrité est peu défini par le droit. Cependant l'arrêté du 4 janvier 2002 relatif à la déclaration d'échanges de biens (DEB)[15] énonce l'intégrité comme permettant au déclarant de *"s'assurer que les données enregistrées par le centre de collecte sont identiques aux données qu'il a transmises"*. Les normes techniques apportent des précisions. La norme NF Z42-013 définit l'intégrité ainsi qu'il suit :

> *Intégrité : caractéristique d'un document électronique qui n'a subi aucune destruction, altération ou modification.*

C'est également la position de la norme ISO 15489, pour laquelle l'intégrité d'un document renvoie au caractère complet et non altéré de son état.

Si l'intégrité n'est pas un concept totalement nouveau pour le droit français, il n'était pas jusqu'ici mentionné aussi expressément. Le paraphe, forme dégradée de la signature, est également un procédé de contrôle d'intégrité juridique. On verra plus loin comment l'intégrité est spécifiquement assurée pendant les opérations pratiques de l'archivage. L'intégrité doit être constante.

3.5 Une garantie complémentaire : la traçabilité

Ainsi l'identification et l'intégrité doivent rester constantes pendant le cycle de vie du message électronique, de la création à la conservation en passant par la transmission électronique. Dans la problématique de preuve posée par les nouvelles technologies, certains ont parlé de la nécessité d'établir et de maintenir un "chemin de preuve". Nous parlerons plutôt dans le domaine présent de *chaîne de sécurité*. A chaque étape du cycle de vie du message, son maillon à intégrité garantie. Tous les maillons mis bout à bout doivent constituer une *chaîne d'intégrité*. Une réflexion identique sur l'autre garantie demandée conduit à préconiser une *chaîne d'identification.* Cette seconde chaîne doit rassembler et fédérer sans rupture tous les maillons à identification garantie du cycle de vie des écrits électroniques.

Pour chaque maillon de la chaîne, la sécurité recherchée doit être constante. Elle doit également se maintenir au-delà des points de rupture ou d'articulation c'est-à-dire lorsque le message électronique passe d'une étape de son cycle de vie à une autre[16]. Autant d'événements techniques qui retiendront l'attention des auditeurs dans les processus d'archivage. De cette nécessité, provient une nouvelle garantie qui a déjà connu son heure de gloire dans les nouvelles technologies et même en dehors de celles-ci, la *traçabilité*. C'est la traçabilité qui permet de vérifier la cohérence de l'ensemble des moyens employés dans une finalité précise, de montrer et démontrer la fiabilité de l'ensemble créé et ultérieurement de permettre le déroulement d'un audit des processus et des procédures ou encore de permettre le *rejeu* d'un traitement technique.

La traçabilité n'est pas une garantie demandée à l'heure actuelle par le droit. Elle est cependant visée par les normes techniques dans lesquelles elle peut servir de liant ou de fil rouge pour les différents éléments qui composent la norme. La norme ISO 15489 indique qu'il est nécessaire de se mettre en mesure de tracer les mouvements et traitements effectués sur les messages électroniques, notamment pour :

- identifier une action en cours,
- permettre le repérage d'un document,
- prévenir la perte d'un document,

[15] Arrêté du 4 janvier 2002 portant approbation du cahier des charges pour la transmission par voie informatique de la déclaration d'échanges de biens entre Etats membres de la Communauté européenne et abrogeant l'arrêté du 19 décembre 1994 (J.O. Numéro 30 du 5 Février 2002 page 2336).

[16] La sécurité doit se maintenir, se poursuivre et rester constante y compris à l'intérieur d'un même stade du cycle de vie, en cas de changement de support et de technologie de stockage, par exemple.

- contrôler la maintenance du système et la sécurité, et conserver une piste d'audit des opérations effectuées sur les documents archivés (c'est-à-dire intégration ou enregistrement, classification, indexation, stockage, accès et utilisation, migration, élimination ou transfert),
- maintenir la possibilité d'identifier la provenance fonctionnelle d'un document donné en cas de fusion ou de migration de systèmes.

4 La formalisation du procédé fiable

Une fois les procédés techniques correspondant aux garanties de sécurisation exigées réunies, la traçabilité sera formalisée par une série de mesures de services visant à enregistrer les paramètres du système et la survenance des événements de toute nature.

4.1 Les historiques et listes récapitulatives des opérations et des événements

La traçabilité nécessite qu'on documente tous les traitements et surtout tous les événements en les enregistrant dans l'informatique. Ainsi la norme NF Z 42-013 conseille dans son point 5.8. de tenir des *historiques*. Les historiques permettent de :

- savoir qui a utilisé le système (utilisateurs humains ou ressources techniques), quand et avec quels résultats,
- enregistrer les accès au système, autorisés ou non,
- vérifier le respect des procédures par le personnel

La norme fixe que :

> *"un enregistrement doit être réalisé pour chaque événement significatif survenu dans le système. Cet historique doit être créé automatiquement par le système."*

Un autre cas, celui-ci déterminé par des textes juridiques, demande l'emploi de *listes récapitulatives*. Les textes d'application de l'article 289 bis du Code Général des Impôts[17] fixent les fonctions prérequises du système de télétransmission pour les factures électroniques. En ce qui concerne les opérations d'archivage et de conservation, le système doit permettre : la constitution quotidienne et l'archivage d'une liste récapitulative séquentielle et exhaustive des messages émis et/ou reçus et des anomalies éventuelles détectées lors des contrôles, la constitution d'un fichier des partenaires, l'archivage des factures émises et reçues et la restitution de toutes les informations aux fins de contrôle par l'administration. Les obligations en matière de conservation portent sur les messages électroniques factures émis et reçus :

- Les messages doivent être conservés dans leur contenu originel et dans l'ordre chronologique de leur émission par l'entreprise émettrice et de leur réception par l'entreprise réceptrice dans les conditions et dans les délais fixés par l'article L 102 B du livre des procédures fiscales ;
- Les entreprises émettrices et réceptrices tiennent et conservent sur support papier ou sur support informatique, pendant le délai fixé au premier alinéa du I de l'article L 102 B du livre des procédures fiscales, une liste récapitulative séquentielle de tous les messages émis et reçus et de leurs anomalies éventuelles.

La liste récapitulative séquentielle et par ordre chronologique de tous les messages émis et reçus et de leurs anomalies éventuelles doit être créée dans le système d'information du fournisseur comme du client. La liste est un fichier alimenté automatiquement par le système de télétransmission par les seules données qui en sont directement issues. A la demande de l'administration, la restitution de la liste récapitulative est effectuée sur papier ou sur support informatique et non sur écran. La restitution doit pouvoir être sélective en fonction des

[17] L'article 289 bis du Code Général des Impôts ainsi que dans les articles 96 F à 96 I de l'annexe III au CGI ont été modifiés par la loi DDOEF n°98-546 du 2 juillet 1998. Il dispose désormais que : "*Les entreprises qui veulent télétransmettre leurs factures doivent recourir à un système de télétransmission répondant à des normes fixées par arrêté du ministre chargé du budget.*" Les textes d'application sont le décret n°99-337 du 3 mai 1999 relatif aux modalités de transmission des factures par voie télématique et modifiant l'annexe III au code général des impôts et l'arrêté du 3 mai 1999 pris pour l'application de l'article 289 bis du CGI relatif aux factures transmises par voie télématique. Les deux textes ont été publiés au JO du 4 mai 1999.

informations qui doivent obligatoirement être contenues. L'arrêté du 3 mai 1999 fixe le contenu obligatoire des enregistrements de la liste :
- numéro et date de facture
- date et heure de constitution du message
- montants hors taxes et toutes taxes de la transaction ainsi que le code monnaie lorsque la facture n'est pas libellée en francs français,
- les éléments d'identification de l'émetteur et du récepteur donnés par le système de télétransmission (code, nom ou dénomination sociale, numéro SIRET, adresse, qualité de fournisseur ou de client) ;
- les libellés des éventuelles anomalies intervenues lors de chaque transmission ;
- la version du logiciel utilisé.

Le fichier des partenaires obéit à la même logique que la liste récapitulative. Les entreprises, des clients ou des fournisseurs, doivent constituer un fichier des partenaires avec lesquels elles échangent des factures par voie télématique. Organisé par ordre chronologique, le fichier sera alimenté automatiquement par le système de télétransmission par les seules données qui en sont directement issues. Pour chaque partenaire, le fichier doit obligatoirement mentionner (arrêté du 3 mai 1999) :
- la qualité d'émetteur ou de récepteur,
- l'archivage des factures dématérialisées ou l'archivage des factures papier,
- les dates d'entrée en phase de dématérialisation avec le partenaire ou la date de sortie.

Autre variante de la garantie de lisibilité, la conservation des messages et leur archivage électronique doit permettre aux entreprises de les restituer à la Direction Générale des Impôts (DGI) en cas de contrôle. La restitution se déroulera sur support informatique ou sur papier à la demande de l'administration, et sur écran, depuis le décret du 3 mai 1999. L'administration peut demander la restitution de toutes les informations émises et reçues, obligatoires ou facultatives, mais doit pouvoir être sélective en fonction des informations qui doivent obligatoirement être contenues. Elles peuvent être demandées à l'entreprise émettrice comme à l'entreprise réceptrice. En tout état de cause, comme les messages émis sont reçus par le partenaire, les messages émis et reçus doivent être identiques, démonstration manifeste de l'intégrité du système.

Face à des formes électroniques, la norme Z 42-013 préconise une sorte de liste de récapitulative enregistrant les événements et les caractéristiques de chaque message électronique, notamment :
- le nom et prénom de l'opérateur pour la cession, ou de la personne qui a démarré le système lorsqu'il n'y a pas d'opérateur ;
- la date et l'heure de création et d'arrivée du document ;
- le format de fichiers utilisés pour le stockage ;
- la taille des documents exprimés en octets (brut, et après compression s'il y a lieu) ;
- le destinataire et l'émetteur lorsqu'il y a transmission de ce document ;
- les éventuels incidents lors de la transmission si ce document provient d'un autre système informatique.

Un concept proche qu'on verra à l'œuvre plus loin est celui de la *journalisation*. La journalisation consiste à enregistrer chaque événement technique sous forme manuelle ou sous forme électronique par saisie ou par génération automatique. Les fichiers résultants doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

4.2 La mémoire des opérations de certification

La norme X.509 de l'Union Internationale des Télécommunications préconise la description des opérations de certification électronique dans un document nommé *Politique de Certification* (PC). Selon la définition de la norme, une PC est document décrivant un ensemble de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'application avec des exigences de sécurité. La PC décrit les tâches des divers composants d'un service de certification. Parmi ceux-ci, le certificateur, qui en priorité est responsable de l'émission des certificats, doit procéder à la "journalisation" et l'archivage des événements et informations relatives au fonctionnement. D'autre part, l'Autorité d'Enregistrement (AE) qui vérifie que les demandeurs ou les porteurs de certificat sont correctement identifiés, doit archiver les dossiers de demande de certificats ou de révocation. Pour éviter d'examiner et de retenir des spécifications trop "exotiques" en matière de conservation des éléments de certification, et qui seraient issues de la PC d'un fournisseur particulier, on retiendra la Politique

de Certification-type[18] du Ministère de l'Economie et des Finances (MEFI). La Politique de Certification-type spécifie les besoins du MEFI en matière de certificats et de clés dans les échanges avec ses serveurs de télédéclarations. Le MEFI référence les certificats du marché dont les fournisseurs en font la demande et qui seront conformes à ces spécifications. Ne pourront être acceptées et traitées que les télédéclarations s'appuyant sur ces certificats référencés et sur des signatures électroniques et moyens de confidentialité conformes aux caractéristiques de la PC-Type.

4.2.1. La journalisation, archivage à court terme

La fonction de journalisation du certificateur consiste à consigner au minimum tous les événements ayant trait à la sécurité des systèmes informatiques utilisés, notamment :
- le démarrage et l'arrêt des systèmes informatiques et des applications,
- les opérations échouées ou réussies pour créer, extraire, établir des mots de passe ou modifier les privilèges système d'utilisateurs privilégiés,
- le changement des caractéristiques et (ou) des clés de ses composantes,
- la création et révocation de certificats,
- les opérations pour initialiser, extraire, valider et invalider des abonnés, et pour mettre à jour ou récupérer leurs clés,
- les opérations d'écriture dans les annuaires de certificats.

Chaque enregistrement d'événements s'organise comme une liste récapitulative en contenant des champs déterminés. Par exemple :
- type d'opération, destinataire de l'opération,
- nom du demandeur de l'opération, nom de l'exécutant, nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes),
- date et heure de l'opération,
- cause de l'événement, résultat de l'événement (échec ou réussite).

D'autres événements doivent aussi être recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits par des systèmes informatiques, notamment les accès physiques, les actions de maintenance et de changements de la configuration du système, les changements apportés au personnel, les actions de destruction : des supports contenant des clés, des données d'activation ou des renseignements personnels sur les abonnés.

Sur le même principe, l'autorité d'enregistrement doit consigner au moins les demandes de certificat, les demandes de révocations, les sollicitations et accusés de réception du certificateur et de ses composantes. Tout dossier de demande de certificat doit être archivé pendant au moins cinq ans. Durant cette durée d'opposabilité des documents, le dossier de demande de certificat doit pouvoir être présenté par le certificateur à toute réquisition des autorités habilitées. Ce dossier, complété par les mentions que l'AE sera amenée à y consigner doit permettre de retrouver l'identité réelle des personnes physiques qui ont été désignées par un pseudonyme dans le certificat émis par le certificateur.

4.2.1.1 Le processus de journalisation.

Le processus de journalisation doit être effectué en tâche de fond et permettre un enregistrement en temps réel des opérations effectuées. Il doit être conçu de façon à être incontournable. En cas de saisie manuelle, l'écriture doit se faire dans le même jour ouvré que l'événement.

L'écriture dans les journaux d'événements doit être conditionnée par des contrôles de droits d'accès. Les enregistrements ne doivent pas être modifiables a posteriori. Les journaux d'événements doivent être protégés en intégrité et le système de datation des événements doit être sûr et non modifiable. Des copies de sauvegarde des journaux d'événement doivent être réalisés. La collecte des journaux commence aux démarrages des systèmes concernés par les événements à enregistrer et se termine aux arrêts de ces systèmes.

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer dans l'un des champs du journal d'événements.

[18] C'est la version 2.0 du 20 Décembre 1999 Politique de Certification-type qui a été retenue ici. On peut obtenir le document par téléchargement sur le site du MEFI : www.minefi.gouv.fr, rubrique téléprocédures.

4.2.1.2 Anomalies et audit.

Les responsables de la fonction de journalisation chez le certificateur doivent être en mesure de détecter toute tentative de violation de l'intégrité du système de gestion des certificats, y compris les équipements physiques, l'environnement d'exploitation et le personnel. Les journaux d'événements journaliers doivent être contrôlés pour identifier des anomalies liées à des tentatives en échec. Les journaux doivent être revus avec une fréquence hebdomadaire. Cette révision donnera lieu à un résumé dans lequel les éléments importants sont analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées. Il est souhaitable qu'un rapprochement mensuel soit fait entre les journaux de l'AE et ceux des composantes du certificateur pour vérifier la concordance entre événements dépendants et contribuer ainsi à révéler toute anomalie.

4.2.2. Les archives des traitements de certification

4.2.2.1. Les principes d'archivage

Les données à archiver sont au moins les suivantes : les fichiers de configuration des équipements informatiques, les PC, les Déclarations des Pratiques de Certification (DPC), les agréments contractuels avec d'autres certificateurs, les certificats et Listes de Révocation de Certificat (LCR) tels qu'émis ou publiés, les récépissés ou notifications, les justificatifs d'identité de l'abonné.

Les certificats de clés de signature ainsi que les LCR produites doivent être archivés pendant au moins cinq ans après l'expiration des clés. Pendant tout le temps de leur conservation, les archives doivent être protégées en intégrité, être disponibles,. pouvoir être relues et exploitées. Les enregistrements des certificats et des LCR devraient être horodatés conformément à la politique de sécurité du certificateur en matière d'archivage. Une archive doit pouvoir être récupérée dans un délai inférieur à 48 heures, sachant qu'une composante du certificateur ou de l'AE ne peut récupérer et consulter que ses propres archives.

4.2.2.2. La cessation d'activité d'une composante.

Dans le cas où la composante du certificateur qui fournit des certificats interrompt ses activités ou change de fonction, le certificateur doit immédiatement en aviser ses abonnés et prendre des dispositions pour que les clés et l'information produites par cette composante continuent à être archivées. Ses archives doivent être conservées dans les mêmes conditions et pour la même période. En conséquence, cette composante du certificateur s'engage en fin de vie à remettre ses archives ainsi que l'ensemble des données dont elle dispose à une entité fiable telle que définie dans sa DPC.

4.3. L'instrumentation de la méthodologie : la charte d'archivage

Le point final des préoccupations que peut ressentir légitimement l'utilisateur au moment d'opérer la conservation consiste, si le volume et la fréquence de l'archivage le nécessitent, en la formalisation du processus d'archivage dans un document de spécifications. La norme ISO 15489 conseille de rédiger une *charte d'archivage* qui aborde les contraintes organisationnelles et techniques et sans échappatoire, les contraintes légales. La norme recommande :

- au niveau technique, d'établir clairement la responsabilité des méthodes d'archivage, telles que classification, indexation, révision et sort final des documents,
- au niveau juridique, de recenser la législation, les normes et les règles applicables afin de définir les contraintes de mise en pratique, de révision, d'audit et de test des méthodes d'archivage.
- au niveau organisationnel, d'observer les systèmes d'information ou les règles en vigueur dans l'organisme ou l'entreprise, afin de maintenir l'intégrité globale de l'environnement en matière de management de l'information et d'inclure les instructions relatives au transfert des documents vers d'autres formes de stockage (stockage hors-ligne ou hors-site).
- au niveau pratique, de documenter clairement et de conserver toutes les décisions relatives aux modalités d'archivage et aux durées de conservation.

La charte d'archivage décrira en détail chaque activité avec les documents qui en résultent, en précisant leur durée de conservation et leur finalité.

La norme NF Z 42-013 indique quelles sont les mesures à prendre et à quelles contraintes, elles doivent répondre. Les mesures comprennent :

- des procédures et les protections devant être mises en place afin de contrôler les processus et de détecter les modifications ou altérations des documents ;
- des matériels et des logiciels devant être mis en place afin d'assurer un niveau de sécurité suffisant ;
- des audits sur les systèmes et les procédures à réaliser ou faire réaliser par l'entreprise qui archive ;
- des attestations pour chaque opération impliquant un opérateur .

A la réflexion peut succéder l'action. Si on veut établir pour l'écrit sous forme électronique un système conforme aux principes de la conservation juridique, il faudra assurer intégrité et identification et à chaque étape processus d'archivage.