Projet ICare

Le cycle de vie de l'écrit électronique

Référence : ICARE/CAB/TPC/DOC_22/v2
Type : Document
Diffusion : Membres du consortium seulement

Date : 17/02/2003
Titre : **ICare – Mode d'emploi des travaux juridiques**

Sous-Projet :
Auteur(s) : Thierry Piette-Coudol, avocat

Résumé :
Cette note expose les différentes étapes du cycle de vie de l'écrit électronique (notion juridique) en signalant l'apport de la signature électronique à chaque étape.

TABLE DES MATIERES

1 INTRODUCTION 3

1.1 NOTION D'ÉCRIT ÉLECTRONIQUE 3
1.2 UN ÉCRIT ÉLECTRONIQUE SÉCURISÉ PAR L'IDENTIFICATION ET L'INTÉGRITÉ 3
1) Deux garanties... 3
2) ... intimement liées 4

2 LA FORMATION DE L'ÉCRIT ÉLECTRONIQUE 6

2.1 FORMALISME JURIDIQUE ET DÉMATÉRIALISATION 6
2.2 DÉMATÉRIALISATION ET SIGNATURE ÉLECTRONIQUE 7
1) Support papier et/ou signature 7
2) Notion de signature ISO 7
2.3 CONCLUSION PARTIELLE 8

3 LA SIGNATURE DE L'ECRIT ÉLECTRONIQUE 10

3.1 UNE MISE AU POINT NÉCESSAIRE 10
1) Une seule signature, deux définitions 10
2) La sécurisation de l'acte ou de la transmission électronique 11
3.2 AVEC QUOI SIGNER L'ACTE ÉLECTRONIQUE 12
3.3 LES MOYENS TECHNIQUES DE SIGNATURE DE L'ÉCRIT ÉLECTRONIQUE 12

4 LA TRANSMISSION DE L'ECRIT ÉLECTRONIQUE 14

4.1 LES EXIGENCES JURIDIQUES DE LA TRANSMISSION 14
4.2 LA MISE EN ŒUVRE DE LA SÉCURISATION 14
1) La signature électronique et le recommandé électronique 14
2) Avec quoi sécuriser l'échange électronique ? 15
3) Les moyens techniques de sécurisation de l'échange 17

5 LA CONSERVATION DE L'ACTE SOUS FORME ELECTRONIQUE 18

5.1 LES ÉLÉMENTS À ARCHIVER 18
1) L'archivage de l'écrit électronique et de sa signature 18
2) L'archivage du certificat électronique 18
5.2 L'ÉVENTUELLE TRANSMISSION À UN ARCHIVEUR DISTANT 19
1) Les modalités : archivage interne ou externe 19
2) La transmission à un Tiers Archiveur 20
3) La nécessité de maintenir l'intégrité pendant le transfert de l'archive 20
5.3 LE DÉSARCHIVAGE 21
1) La restitution d'archives 21
2) Le désarchivage en interne 21

6 LA PRODUCTION DE L'ÉCRIT AUX FINS DE PREUVE 22

6.1 LES DEUX SIGNATURES DU DÉCRET N°2000-230 ET LA PREUVE 22
1) Une signature électronique sans rôle défini 22
2) La primauté de la Signature Electronique Sécurisée 22
6.2 LE RETOUR DE LA SIGNATURE SIMPLE DU DÉCRET ET LA PRÉSOMPTION DE PREUVE 23

OBSERVATION :
Cette note en version 2 décrit le cycle de vie d'un écrit électronique sous l'angle juridique. A chaque étape, il sera montré quel rôle peut jouer la signature électronique.
Le texte intègre et réutilise certains développements de nos notes de travail sur l'Archivage (DOC_4 et DOC_10), la Typologie des signatures (DOC_13) et la transmission de l'écrit électronique (DOC_22 v1).
On peut se débarrasser de la version 1 de cette note.

1 Introduction

1.1 Notion d'écrit électronique

La Loi n°2000-230 du 13 mars 2000 traite du droit de la preuve et intègre dans le Code civil la signature électronique[1]. Son appellation cible clairement ses objectifs puisqu'il s'agit d'adapter le droit de la preuve aux technologies de l'information et de la communication. A cette occasion, la loi a révolutionné la notion d'écrit en lui reconnaissant deux modalités : le support papier et la forme électronique. La loi expose comment apporter la preuve de l'écrit électronique et ce faisant, décrit ce qu'on pourra qualifier de "cycle de vie de l'écrit électronique. Le cycle de vie de l'écrit électronique ou plus précisément de l'*acte sous-seing privé sous forme électronique* comprend les trois étapes principales suivantes :

- la création de l'acte, car l'article 1316-1 indique qu'il est "établi" ;
- la transmission de l'acte, car l'article 1316 envisage toutes les modalités de transmission[2] ;
- et la conservation de l'acte, visée par l'article 1316-1.

1.2 Un écrit électronique sécurisé par 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.

1) Deux garanties...

Comment la signature assure-t-elle l'identification de la personne ? Sans qu'il soit besoin ici d'exposer les caractéristiques et le mode opératoire de la signature électronique[3], 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[4]. 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.

Quant à l'intégrité, le terme est peu usité en droit, voir par exemple l'intégrité du territoire national dans la Constitution. Ainsi la plupart du temps, "*intègre*" a son sens habituel d'honnête, par exemple un homme intègre. En technique, intègre qualifie l'état d'un objet qui n'a pas été modifié, intentionnellement ou non, par rapport à un état antérieur. La transmission présente des risques de pollution des messages ou des fichiers transmis, ce qui

---

1 Cf. *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 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.*"

3 Sur la certification et la signature électronique, cf. notamment les ouvrages : PARISIEN Serge et TRUDEL Pierre, *"L'identification et la certification dans le commerce électronique"* Editions Yvon Blais, Montréal 1996, PIETTE-COUDOL Thierry "*La signature électronique*" à Droit@Litec aux Ed. LITEC, Paris 2001. Et notamment, les articles : LINANT DE BELLEFONDS Xavier, "*Signature électronique et tiers certificateur*", Expertises Février 2000 p.18 et suiv., CAPRIOLI Eric, "*Sécurité et confiance dans le commerce électronique*", JCP 1998, ed. G, I, 123.

4 Il s'agit du Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code Civil et relatif à la signature électronique, modifié par le Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information (voir notre note de présentation dans le fascicule n°147, mai 2002, du LAMY Droit de l'Informatique et des Réseaux, ainsi que "*la signature électronique : mythes et réalités*" (3ème partie, le décret du 18 avril 2002) par NEVEUX Nathalie, EXPERTISES des Systèmes d'Information, juin 2002, p. 213 et suiv.).

explique le contrôle de "bon état" à l'arrivée. L'introduction de la notion d'intégrité dans le Code civil à propos de la signature et de l'écrit électronique est une innovation[5] notable. Cependant l'arrêté du 4 janvier 2002 relatif à la déclaration d'échanges de biens (DEB)[6] 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"*. Diverses normes techniques apportent des précisions :

- Selon la norme NF Z42-013 l'intégrité est "*la caractéristique d'un document électronique qui n'a subi aucune destruction, altération ou modification.*
- Pour la norme ISO 15489, 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, n'est-il pas un procédé de contrôle d'intégrité juridique[7] ?

Au total, 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. Cet instrument apporte en standard l'identification et l'intégrité, garanties 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 qui révélera sa fiabilité à condition que l'identité du signataire soit assurée et l'intégrité de l'acte garantie dans des conditions fixées par le Décret n°2001-272 précité. 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.

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*[8] 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.

2) ... intimement liées

Comme on le voit les garanties d'identification et d'intégrité président à la création de l'écrit électronique. Considérant que l'écrit dans son étape de conservation doit rester intègre et doit maintenir un lien avec son auteur, nous prenons le pari –sans risques- que la transmission de l'écrit électronique doit maintenir les deux garanties. Mais conclusion plus délicate, 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 un article consacré à l'archivage électronique[9], nous parlions de la nécessité d'établir une *chaîne*. A chaque étape

5 On trouve pourtant dans le droit des contrats, sans que le terme soit employé, une application particulière de l'intégrité mettant en œuvre une forme "dégradée" de la signature : les *paraphes* sur les pages dans les contrats. Dans les contrats complexes ou longs, les parties ont coutume de porter leur signature ou leur paraphe en marge de chaque page. Le paraphe est seul si les parties sont d'accord sur le contenu de la page. Dans le cas contraire, le paraphe est accompagné d'une mention indiquant le nombre de mots ou de phrases supprimés ou ajoutés. C'est bien un contrôle d'intégrité du document qui ne retire rien à la signature finale du contrat par les parties en dernière page.

6 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).

7 Cf. *"La signature électronique"*, chapitre 6 sur la signature dégradée, ouvrage précité.

8 La loi 2000-230 a entendu créer deux modalités d'écrit par l'article 1316-1 : l'écrit est sur support papier ou sous forme électronique. Le support électronique de l'article 1317 est une maladresse due à la mauvaise gestation d'un amendement de dernière heure au Sénat. Il ne s'agit pas d'une troisième modalité d'écrit.

9 Cf. "*Conservation et archivage de l'écrit sous forme électronique*", Jurisclasseur Communication et Commerce Electronique – mai-juin 2002, chr. 12 et 14.

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. De cette nécessité, peut être naître une nouvelle garantie qui a connu son heure de gloire dans les nouvelles technologies et même en dehors, 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.

2 La formation de l'écrit électronique

L'étape de la naissance de l'acte sous-seing privé est nommée avec juste raison dans la langue juridique "*formation de l'acte*". Cette appellation jusqu'ici anodine prend tout son sens avec la loi n°2000-230 du 13 mars 2000 qui instaure une *forme électronique* à côté de l'ancienne forme papier[10]. Ce qui dépoussière une ancienne notion juridique qui avait une portée pratique limitée, le *formalisme juridique*, qui connaît dans le contexte électronique une nouvelle jeunesse. Dans la majorité des cas pour former un acte sous-seing privé, il était suffisant de s'asseoir à la table et d'écrire. La création de certains documents nécessitent néanmoins qu'on y mette les formes, puisque le formalisme juridique réunit les règles et formalités propres à la création d'un acte déterminé. Malgré l'émergence des formes électroniques, aucun acte n'échappe au formalisme juridique et si l'article 1316-1 cite deux catégories d'écrits, la liberté n'est pas totale de créer tel acte déterminé sur support papier ou sous forme électronique indifféremment.

2.1 Formalisme juridique et dématérialisation

Un texte de loi peut requérir un support papier pour un acte précis (c'est-à-dire ne pas laisser le choix, tacitement ou expressément, entre le support papier ou la forme électronique). La dématérialisation d'office par l'utilisateur peut-elle être alors validée ultérieurement par l'emploi d'une signature électronique ? La réponse est négative, car le formalisme juridique s'oppose généralement à cette démarche dans les systèmes juridiques de droit civil. Lorsque la loi n'autorise la formation d'un acte que par un support papier, tout contournement de la règle, n'aboutit qu'à la nullité de l'acte ou à son inexistence. La réforme du printemps 2000 n'a pas changé cet état de chose. Elle organise bien un nouveau dispositif de preuve qui n'est utilisable que si auparavant, il a été possible de franchir la barrière de la dématérialisation documentaire dans le respect du formalisme juridique.

La doctrine a manifesté un enthousiasme mitigé devant cette réforme. Pour certains, il est remarquable que le texte sur la signature électronique soit intégré dans le chapitre du Code Civil traitant du droit de la preuve. En conséquence, la signature électronique ne s'applique pas pour les exigences d'écrit *ad validitatem*, par exemple pour les contrats de crédit à destination des particuliers. Les écrits sur papier sont en effet indispensables pour la validité du document que l'on dresse. Mais la distinction *ad validitatem / ad probationem* pourrait être remise en cause et diminuée par la Directive Commerce électronique[11] dont certaines dispositions prévoient que les contrats pourront être négociés par voie électronique. La Loi sur l'Economie Numérique qui transpose cette directive devrait permettre la dématérialisation documentaire, lorsque jusqu'ici le jeu des lois et règlements exigeait la seule modalité papier pour un écrit déterminé. Le projet de *Loi relative à la confiance dans l'économie numérique* a été adopté par le Conseil des ministres le 15 janvier 2003. Ce texte inclurait un article 1108-1 ainsi rédigé :

> *"Lorsqu'un écrit est exigé pour la validité d'un acte juridique, celui-ci peut être établi et conservé sous forme électronique dans les conditions prévues aux articles 1316-1 et 1316-4 et, lorsqu'un acte authentique est requis, au second alinéa de l'article 1317 (...)"*

On conviendra à la lecture de l'article ci-dessus que les garanties d'identification et d'intégrité demandées peuvent être apportées par une signature électronique générique comme celle définie par l'ISO 7498-2 : *"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 cette unité en la protégeant contre la contrefaçon (par le destinataire par exemple).*

[10] Le nouvel article 1317 parle de *"support électronique"*. La mention d'un *support* électronique au lieu de la *forme* électronique de l'article 1316-1 est dû à un amendement parlementaire de dernière heure qui a complété la loi du 13 mars 2000 par l'introduction de l'*acte authentique électronique*. Dans la réalité physique de l'électronique, le support électronique n'existe pas. Les informations électroniques, c'est-à-dire l'ensemble d'octets ou même de bits ou encore d'impulsions électriques, voyagent tels quels, précédés, suivis et coupés par d'autres informations de service ou de contrôle. Cependant pour le papier, il est juste de parler de support, puisque avant le 13 mars 2000 le support papier était avec l'écriture un composant de la forme écrite.

[11] Directive 2000/31/CE du Parlement Européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique dans le marché intérieur ("directive sur le commerce électronique") (JOCE du 17 juillet 2000 p. L.178/1).

S'agissant de l'objectif de passer outre au support papier pour un écrit déterminé, la série des article 1316-1 à 1316-4 nous met potentiellement en présence de 3 signatures électroniques :
- la signature électronique[12] des techniciens (ISO 7498-2) via l'article 1316-1,
- la signature électronique "ordinaire" de l'article 1-1° du Décret n°2001-272 du 30 mars 2001 modifié via l'article 1316-4,
- la signature électronique sécurisée de l'article 1-2° du Décret n°2001-272 du 30 mars 2001 modifié via l'article 1316-4.

Dans l'attente de la LEN, il n'y a que deux façons de sortir du problème :
- si la nature du document considéré ne fournit aucune information sur la nature de son support, on se réfère à l'article 1316-1 du Code civil qui stipule que l'écrit peut adopter soit le support papier soit la forme électronique. Dans cette circonstance, on procède à la dématérialisation sans coup férir.
- si la nature du document considéré indique que son support est le papier. Il n'est pas possible de passer outre, tout au moins tant que la Loi sur l'Economie Numérique (LEN) ne soit venu résoudre la question.

2.2 Dématérialisation et signature électronique

Laissons de côté, le renvoi à l'article 1317 qui fait référence aux actes authentiques électroniques[13]. Restent les articles 1316 à 1316-4 pour répondre à la question concrète : comment valider a posteriori un acte sous-seing privé électronique pour lequel les textes demandent un support papier obligatoire ? La validation dépend des deux conditions à observer qui sont citées dans l'article 1316-1 : l'identification de la personne et l'organisation d'une garantie d'intégrité. En conséquence les moyens techniques à retenir sont au choix : tous les types de moyens techniques susceptibles de fournir l'identification et l'intégrité et la signature électronique de l'article 1316-4.

1) Support papier et/ou signature

Sur le premier point, il s'agit bien de n'importe quel type de moyen technique. On aura noté que le nouvel article, du moins s'il subsiste dans la version définitive de la LSI, ne se renvoie pas uniquement à l'article 1316-4. On peut en déduire qu'une signature électronique peut être employée, mais pas obligatoirement. Il est loisible au technicien de faire son choix dans l'offre technique du marché pour retenir les produits porteurs d'identification et d'intégrité. Mais quelle signature choisir ? Celle de l'article 1316-4, obligatoirement, ou un autre type de signature ?

Au demeurant, le bon sens ne suggère-t-il pas d'éviter de choisir un instrument juridique qui présente des caractéristiques ou des attributs qui ne sont pas recherchés dans une situation donnée ? Opter pour la signature de l'article 1316-4 n'est pas une solution unique, car l'option rebondit avec les deux signatures du décret d'application 2001-272 modifié. Laquelle choisir ? Hélas, toutes deux portent une caractéristique non souhaitée : elles manifestent le consentement du signataire aux obligations qui découlent de l'acte signé. Peut-on retenir cette solution où le fond vient se mêler à la forme ? En réalité, que faudrait-il ? Une signature électronique de type ISO (signature électronique simple de la Directive, la SEDIR), mais assurant en plus, l'intégrité. Dit d'une autre façon, une *signature électronique avancée "dégradée"* de la Directive (SESAV) pour ne pas retomber au centre de la dimension juridique.

2) Notion de signature ISO

Une signature électronique de technicien, la signature ISO. Standardisée au niveau international, cette signature est définie par la norme ISO 7498-2 de la façon suivante : "*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 cette unité en la protégeant contre la contrefaçon (par le destinataire par exemple)*".

[12] C.a.d. une signature numérique de type PKI (clés cryptographiques, certificat, AC, Dispositif de création / vérification de signature...), mais qui ne respecterait pas nécessairement les exigences techniques des textes juridiques européens et nationaux.

[13] Le lecteur qui souhaiterait se pencher sur la question de la signature de l'acte authentique électronique peut se reporter à l'ouvrage "*Les actes authentiques électroniques*", rapport de la Mission de recherche "Droit et Justice", sous la direction de Isabelle de LAMBERTERIE, La Documentation Française, 2ème trimestre 2002.

La définition, si elle vise les habituelles garanties d'identification et d'intégrité, ne précise pas comme le fait la loi française une *identité assurée* du côté du signataire. Ce qui introduit dans le système légal le *prestataire de services de certification* et le certificat électronique produit par ce dernier pour valider la clé publique du signataire. Aussi les techniciens peuvent-ils parler de *signature numérique* dans le premier cas et de *signature électronique* avec l'intervention du certificateur[14]. Par contre, la signature ISO n'apporte aucun élément sur la question du consentement du signataire, Une signature électronique de type ISO, mais assurant en plus, l'intégrité. Dit d'une autre façon, une *signature électronique avancée "dégradée[15]"* de la Directive (SE-SAV) pour ne pas retomber au centre de la dimension juridique.

Mais peut-on accorder une valeur juridique quelconque à une signature de type ISO ? Sur ce point, on se rappellera que la *Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques* reconnaît deux types de signatures électroniques. La première dont le nom est parfaitement banalisé ne doit pas être pour autant minimisée. La *signature électronique* ordinaire est définie de la façon suivante par l'article 2 : *"une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification"*. Dans les définitions de la Directive, le regard du juriste est immédiatement attiré par la signature électronique avancée qui est l'instrument prévu pour rendre dans le monde électronique les mêmes services que la signature manuscrite dans le monde l'écrit-papier. Cependant la signature avancée ne doit pas venir éclipser la signature ordinaire. Cette signature n'assure qu'un niveau de sécurité incomplet : si elle prend en compte l'authentification, elle ne donne aucune garantie en ce qui concerne l'intégrité. De plus, elle ne donne aucun gage du consentement du signataire et ne prétend pas assurer l'intégrité. En mettant en application l'adage *qui peut le plus peut le moins*, si la définition de la signature électronique n'englobe pas l'intégrité, est-ce à dire que l'intégrité est pour autant exclue ? Une position aussi restrictive est-elle requise ? Dans ces conditions, la signature ISO répond *a maxima* à la définition de la Directive. Mais quel intérêt d'assimiler la signature ISO à la signature ordinaire de la directive? L'enjeu repose dans les effets juridiques.

Pour apprécier les effets juridiques de la signature ordinaire, il est nécessaire d'interpréter l'article 5.2. de la Directive qui déclare : "*Les Etats membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que :*

- *la signature se présente sous forme électronique*
- *ou , qu'elle ne repose pas sur un certificat qualifié*
- *ou qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification*
- *qu'elle n'est pas créée par un dispositif sécurisé de création de signature".*

La signature numérique qui garantit l'identification et l'intégrité pourrait rentrer dans la sphère juridique, par exemple, si le signataire était un être humain. Ce qui ne lui donnerait pas nécessairement pas un caractère juridique, si elle n'était pas apposée sur un acte juridique sous forme électronique[16]. Cependant la non-application à un acte juridique ou sa simple forme électronique ne suffit pas pour que la signature électronique soit exclue des instruments juridiques. Par application de l'article 5.2., la signature ordinaire serait admissible aux fins de preuve, quoiqu'on puisse s'interroger sur sa portée exacte.

2.3 Conclusion partielle

Qu'en penser aujourd'hui ? Il semble un peu tôt pour raisonner en profondeur sur un sujet aussi neuf, alors que la législation n'est pas complète et que la doctrine ne s'est pas encore beaucoup exprimée. Aux utilisateurs qui seraient déjà face à cette problématique, on peut souhaiter d'être placés dans des relations de type B to B, car ils pourront peut-être trouver l'inspiration dans l'article 1316-2. Par analogie avec la convention de preuve, les utilisateurs professionnels peuvent se doter d'une convention de dématérialisation. Ils peuvent y indiquer

[14] Sur cette vision de la signature, voir par exemple, aux 2ème Rencontres de l'AFNOR sur la signature électronique du 14 octobre 1999, les intervention de MM. Thierry Autret et Denis Pinkas.

[15] On verra la question de la signature électronique dégradée apparaître plus loin avec une nouvelle question : une signature électronique avancée peut-être s'appuyer sur un certificat non-qualifié ?

[16] C'est-à-dire un acte sous-seing privé électronique de l'article 1316-1 du Code Civil, un acte authentique électronique de l'article 1317 du Code Civil, une téléprocédure lancée par une personne publique ou encore un contrat électronique de la Directive Commerce Electronique 2000/31/CE (Directive du Parlement Européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique dans le marché intérieur - JOCE du 17 juillet 2000 p. L.178/1) en attendant la Loi sur la Société de l'Information (LSI).

concrètement dans quel contexte juridique ils procèdent à la dématérialisation. Par exemple, ils choisiront l'une ou l'autre des signatures électroniques et diront quelles fonctions, ils lui fixent dans leurs relations électroniques. Le montage juridique pourra encore être complété : peut-être profitera-t-on de l'occasion pour faire également de cette signature électronique un moyen de preuve[17]. Bref, on retrouve l'intérêt de l'accord d'interchange de l'EDI[18].

Enfin, il subsiste une autre façon de résoudre cette problématique, c'est de la fondre dans celle qui va suivre, la problématique de la transmission de l'acte sous-seing privé[19].

En conclusion de cette étape, on peut estimer que les besoins de sécurité juridique en matière de formation de l'écrit sous forme électronique seraient plutôt satisfaits par l'emploi d'une signature électronique supérieure en efficacité juridique à la signature ordinaire de la Directive (SEDIR) et inférieure en efficacité à la signature électronique avancée (SESAV) c'est-à-dire "dégradée".

[17] A noter que le formalisme juridique pour un même document peut en plus du support papier obligatoire, réclamer l'apposition obligatoire d'une signature. Comme il est impensable d'employer deux signatures, il faut procéder de façon systématique : réfléchir sur le type de signature dans le premier cas, puis dans le second cas, enfin décider du type de l'unique signature. [note de la note : il existe cependant des hypothèses où deux signatures peuvent se trouver pour un même acte électronique. D'une part, c'est le cas avec les signatures horizontales (co-signatures) ou verticales (sur-signatures). D'autre part, dans le cas de l'archivage, comme on le verra plus loin.]

[18] Pour un accord d'interchange-type EDI, voir la *Recommandation 1994/820/CE de la Commission du 19 octobre 1994 concernant les aspects juridiques de l'échange de données informatisé.*

[19] Nous faisons ici le pari du télescopage des exigences juridiques de la transmission et de la formation. A l'appui de cette position, qu'on pense à la nature de la garantie d'intégrité. La garantie de l'origine du message (identification de l'auteur) est permanente et continue pendant la transmission. L'intégrité ne peut être jugée ni au moment de la formation de l'acte comme le réclame l'article 1316 du C.C., ni pendant la transmission électronique, mais seulement après la transmission (vérification de la signature). Il importe donc de se placer au niveau de la réception du message et non à celui de sa création.

3 La signature de l'Ecrit électronique

Si on désire rendre parfait l'écrit électronique, comme le dit l'article 1316-4 du Code civil, et lui donner la meilleure force probante, on procédera à sa signature électronique. Cependant le décret d'application de l'article 1316-4 reconnaît l'existence de deux signatures électroniques à valeur juridique : la signature électronique (art.1-1°) et la signature électronique sécurisée (art.1-2°). Laquelle employer ?

3.1 Une mise au point nécessaire

Une mise au point s'impose avant de progresser. En rendant à César ce qui est à César, on rendra la signature électronique aux techniciens. A cette occasion, on constatera la différences entre le point de vue des techniciens et des juristes sur l'instrument. Est-ce à dire que le droit a totalement absorbé l'instrument des techniciens, il ne le semble pas comme on va le voir.

1) Une seule signature, deux définitions

La signature électronique a été primitivement développée par les techniciens pour satisfaire des besoins de sécurité. Standardisée au niveau international, elle est décrite et connue sous le nom de "*digital signature*", maladroitement traduite par "signature digitale". Cette signature est définie par la norme ISO 7498-2 de la façon suivante : "*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 cette unité en la protégeant contre la contrefaçon (par le destinataire par exemple)"*. On peut retrouver dans cette définition les garanties de sécurité recherchée, l'*intégrité* mentionnée en toutes lettres et l'*identification* dans la périphrase "prouver la source". Quant à la signature électronique du Droit, l'article 1316-4 du Code civil indique d'une part, qu'elle "*identifie celui qui l'appose par un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache"* et que d'autre part, elle *"manifeste le consentement du signataire aux obligations qui découlent de cet acte"*. La Loi emprunte à la sécurité les deux garanties précitées et lui ajoute une caractéristique spécifiquement juridique, le consentement au contenu[20].

Cette petite différence est lourde de signification. C'est par abus de langage que la "signature" électronique porte cette appellation. Classiquement la signature électronique apporte deux garanties au destinataire d'un message signé : l'identification de l'origine et l'intégrité du message à destination. L'objectif est différent, il ne s'agit pas de sécuriser le message mais de sécuriser sa transmission. Un tableau comparatif des deux types de signature met en regard les éléments qui correspondent et différencient les deux types de signature.

	SE des juristes	SE des techniciens
Signataire :	auteur de l'acte	opérateur sur machine
Caractères :	Identification et intégrité Engagement sur le contenu	Identification et Intégrité
Cycle documentaire :	Formation de l'acte	Transmission de l'acte
Acteur principal :	Signataire	Destinataire

[20] La signature électronique n'est pas très éloignée de la traditionnelle signature manuscrite. Elle apporte un élément fondamental au document sur lequel elle est apposée : sa validité juridique. La signature manuscrite présente pour le destinataire du document signé deux fonctions essentielles : une fonction d'identification et une fonction d'appropriation ou d'adhésion du signataire au contenu du document, cette dernière étant réalisée d'une façon volontaire.

La CNUDCI a pris conscience de cette confusion et des conséquences que cela pouvait entraîner. Dans son rapport de février 1999, on peut notamment lire (traduction libre) : "*48. Il a été suggéré que les concepts de "signature électronique" et "signature électronique étendue" ne devraient pas être employés dans les Règles Uniformes car ils ne sont pas en fait des "signatures", mais plutôt des techniques qui permettent l'identification de l'émetteur d'un message de données ainsi que l'identification du message envoyé. En conséquence, il n'y a aucune raison d'utiliser le terme "signature" pour décrire de semblables techniques. En faisant de cette manière, on créerait une confusion sur le terme "signature" dont la signification est étroitement associée à son emploi dans un environnement papier et avec les effets juridiques de son emploi dans un tel environnement.*"

Pour les juristes et les techniciens, l'acteur principal ou le bénéficiaire de la signature n'est pas le même. Pour les juristes, l'acteur principal est le signataire qui s'identifie et qui s'engage. Pour les techniciens, c'est le destinataire du message qui peut être sûr de l'origine et de la non-altération de celui-ci.

2) La sécurisation de l'acte ou de la transmission électronique

La signature des juristes n'est plus uniquement manuelle, elle peut être électronique depuis la loi n°2000-230. Ainsi en suivant notre propos, il y aurait deux types de signatures électroniques, celle des juristes qui valide l'écrit électronique et celle des techniciens qui sécurise la transmission électronique. Cette dissociation est bien fondée ? On pourra pour s'en convaincre se reporter au cas de la *facture électronique*. La *Directive 2001/115 du 20 décembre 2001* sur la facturation[21] incite les Etats Membres à accepter les factures sous forme électronique à condition que deux garanties de sécurité soient respectées : l'authentification[22] et l'intégrité. Dans la pratique, l'article 2 de la Directive prévoit que la facture électronique sera accompagnée d'une *signature électronique avancée* au sens de la directive 1999/93/CE du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques[23].

En traitant dans le même texte des factures sur papier ou des factures sous forme électronique, la Directive n'instaure pas de régime spécifique pour chacune d'elles. Une disposition située plus haut dans le texte pourrait induire en erreur le lecteur qui lira : "*les Etats membres n'imposent pas la signature des factures*". On ne doit pas en déduire que la facture sur papier ne sera pas signée, alors que la facture électronique le sera par une signature électronique avancée. En effet, il existe deux emplois de la signature correspondant aux deux pans de la problématique juridique que rencontre tout document voué à la dématérialisation : la sécurisation de l'acte et la sécurisation de la transmission.

La substitution d'une forme électronique à une forme écrite est généralement réalisée en vue d'une transmission électronique. La faisabilité juridique de l'opération dépend des réponses apportées à la problématique qui se décompose en deux parties :

- d'une part, la dématérialisation documentaire et la substitution qui peuvent être envisagées à condition que le formalisme juridique ne soit pas violé,
- d'autre part, la transmission par voie télématique de la forme électronique qui doit pouvoir être assurée dans les meilleures conditions de sécurité.

La prohibition de la signature par la Directive correspond au premier pan de la problématique juridique, le respect du formalisme juridique. A l'exception de la Grèce, les documents factures sont dans les Etats membres peu souvent soumises à la formalité de signature. Ils devront le rester. Cependant en ce qui concerne la transmission télématique, il faut sécuriser l'échange[24]. La sécurisation, en terme d'identification et d'intégrité est assurée selon le texte par une SE avancée considérée comme un pur instrument technique.

---

[21] *Directive 2001/115 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 17.1.2002 L 15/24).

[22] Le texte communautaire parle d'*authentification*, terme que nous n'avons pas employé jusqu'ici lui préférant celui d'*identification*. L'authentification recouvre l'ensemble des moyens mis en œuvre par une entité (technique ou humaine) pour appuyer son identification, en bref le certificat électronique et le prestataire de services de certification électronique (autorité de certification). Le présent texte ne met pas en évidence un rôle particulier du certificat ou du certificateur. Aussi le lecteur considérera-t-il les termes identification et authentification comme proches voire synonymes.

[23] L'article 2 de la Directive prévoit une seconde modalité : l'*échange de données informatisé* (EDI) tel que défini dans la recommandation 1994/820/CE de la Commission du 19 octobre 1994 précité.

[24] Pour se convaincre qu'il ne s'agit pas de signer le document facture, mais de sécuriser sa transmission électronique, il suffit de se reporter à la lettre de la Directive : *"les factures transmises par voie électronique sont acceptées par les Etats membres à condition que l'authenticité de leur origine et l'intégrité de leur contenu soient garanties...*"

3.2 Avec quoi signer l'acte électronique

L'intérêt de choisir une *signature électronique sécurisée* est de faire profiter le signataire de la *présomption de preuve* instauré par l'article 1316-4 du Code Civil. Les composants de la signature électronique sécurisée doivent cependant respecter certaines conditions techniques précisées dans l'article 2 du décret précité :

- le dispositif de création de signature électronique (DCS) doit être *sécurisé*, c'est-à-dire conforme aux spécifications techniques listées dans l'article 3-I ;
- le certificat électronique sur lequel repose la vérification de cette signature doit être *qualifié*, c'est-à-dire conforme aux spécifications techniques listées dans l'article 6.

Pour établir leur compatibilité avec les exigences textuelles, les composants de la signature peuvent être évalués et faire l'objet d'une attestation de conformité, ainsi :

- le DCS sera réputé sécurisé dans les conditions du Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information[25].
- Le certificat sera réputé qualifié si le certificateur qui l'émet est réputé qualifié dans les conditions de l'Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique (PSCE) et à l'accréditation des organismes chargés de l'évaluation[26].

3.3 Les moyens techniques de signature de l'écrit électronique

Pour signer électroniquement un écrit électronique, il faut disposer des éléments techniques suivants :

- un logiciel de traitement de texte permettant de rédiger l'écrit électronique,
- un biclé cryptographique formé d'une clé privé et d'une clé publique,
- un certificat électronique de clé publique fourni par un certificateur du marché,
- un logiciel (ou une combinaison matériel et logiciel) de création de signature nommé "*dispositif sécurisé de création de signature électronique*"[27] dans le droit

L'écrit électronique est rédigé par l'utilisateur grâce au logiciel de traitement de texte. Le résultat technique est un fichier texte ou "*.doc*" pour les traitements de textes les plus courants du marché. Le fichier est déposé dans un répertoire du disque dur à la convenance de l'utilisateur. La signature de l'écrit électronique s'effectue au moyen du logiciel de signature. Ce logiciel, en se référant aux produits du marché, se présente à l'écran comme une barre d'icônes flottante qui permet de lancer l'opération de signature. Le logiciel procède suivant l'état de l'art, hachage du message et chiffrement avec la clé privée[28]. A cet instant, il faut faire une incidente avec le certificat électronique. Le certificat électronique est indispensable pour le destinataire du message. Ce dernier, que le droit appelle "*vérificateur*"[29] doit contrôler à partir du logiciel de vérification et la clé publique du signataire garantie par le certificateur grâce au certificat électronique. Une question pratique qui a son importance est celle-ci : comment récupérer le certificat du signataire ? La réponse la plus simple est que le signataire le lui envoie directement. C'est pourquoi, les logiciels de signature standards produisent à partir du fichier contenant l'écrit électronique un fichier contenant l'écrit électronique, sa signature et le certificat avec la clé publique.

Cette façon de procéder évite le mode primitif de publicité des certificats à savoir le dépôt du certificat dans un annuaire accessible aux destinataires potentiels. Il n'y a pas d'inconvénient au regard de la confidentialité de procéder de cette manière : en effet, toutes ces informations sont publiques. Un autre avantage apparaît : comme le système du destinataire stocke automatiquement le certificat du signataire, il dispose de la clé publique pour éventuellement chiffrer un message qu'il lui destinerait[30] En outre, l'agent de messagerie de votre correspondant

[25] Cf. notre présentation du texte dans le fascicule n°147 de mai 2002, du LAMY Droit de l'Informatique.
[26] Cf. notre présentation du texte dans le fascicule n°149 de juillet 2002, du LAMY Droit de l'Informatique.
[27] Cf. le Décret n°2001-272 du 30 mars 2001 modifié pris pour l'application de l'article 1316-4 du Code Civil et relatif à la signature électronique. Voir l'article 1 pour la définition et les art. 3 et 4 pour les caractéristiques.
[28] Pour les détails, voir nos ouvrages chez LITEC, collection Droit@Litec : "*Echanges Electroniques - Certification et sécurité*", mars 2000 et "*La signature électronique*", avril 2001
[29] Cf. art. 5-a. du Décret d'application de l'article 1316-4.
[30] En matière de chiffrement, la manipulation des clés est inversée : on chiffre un message avec la clé publique du destinataire. Seul ce dernier pourra le déchiffrer grâce à la clé privée correspondante.

peut stocker le certificat de l'émetteur du message reçu. Dès lors, il peut envoyer des messages chiffrés vers ce correspondant. Cette mécanique simple permet l'utilisation effective de la signature et du chiffrement même sans le déploiement d'annuaires par simple échange préalable de messages signés.

Ce fichier est remarquable par une extension de type "*.p7m*". Ce format de fichier procède de la spécification PKCS#7 (pour *Public Key Cryptography Standard n°7*). Les spécifications PKCS finalisées en juin 1911 par de grandes sociétés informatiques[31] définissent une suite de spécifications standards de modules cryptographiques. Les PCKS regroupe les composants suivants :
PKCS#1 : Cryptage RSA
PKCS#2 : *Incorporé dans PKCS#1.*
PKCS#3 : Agrément de clés Diffie-Hellman
PKCS#4 : *Incorporé dans PKCS#1.*
PKCS#5 : Cryptage basé sur un mot de passe
PKCS#6 : Format d'extension des certificats
PKCS#7 : Spécification du format de différents messages cryptographiques
PKCS#8 : Format des clés privées
PKCS#9 : Selected Attributes Types
PKCS#10 : Format des requêtes de certification
PKCS#11 : Interface de cryptographie par token.
PKCS#12 : Echange d'informations personnelles.
PKCS#13 : Techniques à clé publique utilisant la cryptographie par courbe elliptique.
PKCS#15 : Format des fichiers de cartes à puce (draft).

Les travaux ont été poursuivies par le groupe PKIX de l'IETF. L'IETF (*Internet Engineering Task Force*) qui est l'organisme de standardisation spécifique au monde Internet a mis en place le groupe PKIX a en 1995. Ce groupe travaille sur tout ce qui touche l'utilisation de certificats X509 et de leurs applications dans l'Internet. Entre autres développement, le groupe PKIX a établi des protocoles de gestion permettant aux différents acteurs (utilisateurs, certificateurs) de dialoguer et d'échanger les informations relatives à la gestion de l'ensemble : demande de création ou de révocation de certificat, certification réciproque entre autorités de certification... Des règles d'usage et des considérations pratiques : exigences en matière d'identification des sujets, sécurité physique, règles pour la révocation des certificats...

Enfin ces standards travaillent avec le protocole permettant de transmettre les messages électroniques de façon sécurisée, S/MIME. En effet, le fichier de type "*.p7m*" est transmis tel quel par la messagerie électronique sous la forme d'un *fichier attaché*. Globalement les fichiers électroniques transmis sont protégés par l'utilisation de deux fonctions : la signature et /ou le chiffrement appliqué au message original et contenu dans le fichier attaché :
- Si un message signé a un attachement de type smime.p7s, il contient la signature de l'expéditeur.
- Si un message chiffré a un attachement de type smime.p7m, il contient le message chiffré.

[31] comme Apple, DEC, Lotus, Microsoft, le MIT, RSA et Sun.

4 La transmission de l'Ecrit électronique

Parions donc que la transmission de l'écrit électronique s'effectue dans les mêmes conditions de sécurité : identification de l'origine et intégrité du contenu. Quels moyens techniques choisir ? Le marché n'est pas avare en produits techniques permettant d'atteindre ces résultats. Parmi eux, la signature électronique peut être considérée comme un moyen de premier ordre. Après tout, le Code civil ne reconnaît-il pas la validité de l'écrit signé et une présomption de fiabilité au procédé de signature si "*l'identité du signataire* [est] *assurée"* et *"l'intégrité de l'acte garantie"*.

Ainsi sans que son emploi soit une obligation expresse de l'article 1316-1, la signature électronique est une bonne solution. Mais quelle signature ?

4.1 Les exigences juridiques de la transmission

L'identification et l'intégrité s'appliquent lors de la création et de la conservation de l'écrit, l'exigence est posée clairement par l'article 1316-1. Mais la transmission mentionné ne fait pas référence aux deux garanties sécuritaires. Aussi peut-on redécouvrir avec satisfaction un des textes précurseurs en matière de transmission électronique, la *loi n°1994–126 du 11 février 1994 relative à l'initiative et à l'entreprise individuelle*, dite loi Madelin. L'article 1 de la loi vise le domaine d'application, les déclarations d'une entreprise destinée à une administration ou à un organisme assimilé. Selon les termes du premier alinéa : *"toute déclaration (...) peut-être faite par voie électronique dans des conditions fixées par voie contractuelle*. Le deuxième alinéa de l'article 4 de la loi indique ce que doit contenir le contrat : "*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 d'autres éléments sur lesquels on peut s'interroger quoique la loi n°1994-126 est caractéristique de relations de droit public plus que de droit privé.

Si on admet que la signature électronique juridique laisse encore un peu de latitude à l'instrument sécuritaire des techniciens, il y aurait deux signatures. Avant de transmettre de façon sécurisée un écrit électronique (signature des techniciens), l'écrit pourrait être signé pour des raisons de validité juridique (signature des juristes). La mise en œuvre technique va montrer la réalité de l'hypothèse avec deux modes opératoires différents.

4.2 La mise en œuvre de la sécurisation

Sécuriser une transmission n'est pas une question totalement nouvelle en droit où les questions relatives à l'acheminement postal sont connues.

1) La signature électronique et le recommandé électronique

Qu'attend le destinataire de l'acte sous forme électronique ? Des certitudes sur l'identification et l'intégrité du message. Il n'y manque que la prise en compte de la dimension temporelle pour se rapprocher du recommandé postal. Dans cette procédure d'acheminement postal "sécurisé", la poste remet au destinataire le même pli (intégrité) qu'elle a reçu de l'expéditeur (identification de la source)[32]. Par contre, la poste applique un tampon horodateur sur le pli ainsi que sur le bordereau de recommandé. La gestion du temps est encore plus fine si le recommandé est complété d'un avis de réception.

[32] Deux constatations s'ensuivent immédiatement. Premièrement, l'identification au bureau de poste pour l'envoi d'un recommandé est moins forte que celle de la certification électronique : le guichetier ne vérifie pas l'identité de celui qui se présente. Deuxièmement, comme on le voit au bureau de poste avec le recommandé, ce n'est pas obligatoirement le signataire du document qui se présente au guichetier.

Les relations entre le temps et la signature ne sont pas l'objet de ce texte[33]. Nous rappellerons simplement qu'il existe certains actes pour lesquels la date d'envoi est plus importante que la date du document : les déclarations faites par les entreprises à destination des administrations, qui sont actuellement soumis à une dématérialisation à grande échelle avec le développement des *téléprocédures*. Il faut la plupart du temps déclarer et quelquefois payer avant l'expiration d'un délai ou la survenance d'une date. Lorsque la date d'envoi s'avère critique, la pratique est d'utiliser le service de sécurisation de la poste. L'intérêt serait grand de disposer d'une procédure de même type dans le monde électronique. Malheureusement, le droit français ne possède pas actuellement de *recommandé électronique*[34]. On peut observer cependant les enseignements d'autres législations, comme celle du Luxembourg[35].

La *Loi luxembourgeoise sur le commerce électronique* du 14 août 2000 a réformé le droit interne pour favoriser le développement de cette nouvelle façon de faire des affaires en adoptant notamment, la signature électronique. Selon les motifs de la Loi, le législateur luxembourgeois a considéré que dans le contexte des échanges électroniques de données, effectués en temps réel, il est nécessaire de prévoir, en outre, une certification du temps. Le recommandé déposé électroniquement offre à l'instar de celui déposé matériellement la possibilité pour l'expéditeur d'un message signé électroniquement de se constituer une preuve de l'envoi, de la date et, le cas échéant, de la réception de ce message. Ces différents niveaux de preuve peuvent s'analyser de la façon suivante :

- Preuve de l'envoi : l'intérêt qu'offre le recommandé est celui pour l'expéditeur de se ménager une preuve de son envoi. Cette preuve pourra être réalisée, pour le recommandé électronique grâce au récépissé électronique qui lui sera remis lors du dépôt électronique.
- Preuve de la date et de l'heure de l'envoi : la loi impose, dans certains cas, un délai pour l'envoi d'une lettre ou d'un document. Tout comme pour la preuve de l'envoi, le recommandé offre à l'expéditeur la possibilité de se ménager la preuve que les délais ont été respectés.
- Preuve de la réception : grâce au recommandé avec accusé de réception, l'expéditeur peut prouver que le destinataire a reçu l'envoi et a été en mesure d'en prendre connaissance.

L'expéditeur du document est responsable des moyens techniques à mettre en œuvre pour garantir efficacement le contenu du message contre les risques d'atteinte à l'intégrité et à la confidentialité de celui-ci.

Dans la section 9 de la Loi sur le commerce électronique, l'article 36 traite ainsi du recommandé électronique : "*Le message signé électroniquement sur base d'un certificat agréé dont l'heure, la date, l'envoi et le cas échéant la réception, sont certifiés par le prestataire de service de certification accrédité conformément aux conditions fixées par règlement grand-ducal constitue un envoi recommandé.*" Si les explications juridiques semblent convaincantes, on peut s'interroger sur les moyens techniques à mettre en œuvre. L'horodatage technique à reconnaissance juridique emploie une signature électronique. Le centre du dispositif est le certificat électronique agréé[36] qui intègre *l'heure, la date, l'envoi et le cas échéant la réception* sous la certification de l'archiveur de confiance.

2) Avec quoi sécuriser l'échange électronique ?

Comme on l'a vu ci-dessus, on peut estimer que les besoins de sécurité technique en matière de transmission de l'écrit sous forme électronique seraient satisfaits par l'emploi de la signature électronique des techniciens utilement complété dans certains cas par un système de recommandé électronique. Mais faute de recommandé électronique, nous nous contenterons d'une signature électronique simplement. Oui, mais laquelle ? Les réponses

33 Pour en connaître un peu plus sur ces rapports, on pourra attendre les conclusions à intervenir avant la fin de l'année sur l'horodatage sécurisé qui est actuellement étudié par un groupe de travail ad hoc (association IALTA et Conseil Supérieur de l'Ordre des Experts-Comptables). Ce groupe de travail est similaire à celui qui a produit le *Guide de l'archivage sécurisé* (cf. INFRA, étape de l'archivage).

34 Ni recommandé électronique, ni avis de réception. Un *décret n°2001-492 du 6 juin 2001 (...) relatif à l'accusé de réception des demandes présentées aux autorités administratives* fait l'impasse sur la question. Seule rançon à la modernité, l'AR administratif peut mentionner l'adresse électronique du service chargé du dossier.

35 Le droit belge a également reconnu le recommandé électronique (depuis l'arrêté royal du 9 juin 1999 et la loi du 12 août 2000 "portant des dispositions sociales et fiscales diverses"), mais avec une certaine opacité puisque les services de tous les prestataires du marché peuvent être utilisés (art. 239 de la loi), sauf en matière de procédures judiciaires et administratives où il est obligatoire de passer par le service de La Poste (art. 21 de l'arrêté royal). CF. WERY Etienne, "*Le recommandé électronique : techniquement au point mais juridiquement à risque"*, juin 2002. URL http://www.droit-technologie.org

36 Le certificat électronique est agréé. C'est la forme luxembourgeoise du "certificat qualifié" de la directive européenne.

ne sont pas légions, puisqu'on n'a le choix qu'entre la SE et la SE Sécurisée du décret. Pourtant, nous pensons que ni l'une ni l'autre ne conviennent.

Pour tenter de le montrer, nous reviendrons sur le cas de la Directive facturation électronique mentionnée plus haut. Pour cette dernière, la signature, étant bien rappelé qu'il s'agit de sécuriser l'envoi, doit recevoir une SE Avancée. Comment procéder à une transposition directe de la Directive facture précitée, alors que la *Signature Electronique Avancée* n'existe pas dans notre droit interne ? Dans un précédent article[37], nous avons exposé que les deux signatures définies dans le décret d'application de l'article 1316-4 du Code Civil sont toutes deux transposées de la SE Avancée[38].Dans ce texte, nous ajoutions que le législateur, en se prononçant pour une modalité de facture électronique dans un format non structuré[39] munie d'une signature électronique sécurisée, transposerait du même coup certaines difficultés voire incohérences juridiques.

En effet dans le droit français, le régime actuel de la signature (sur support papier) ne comporte aucune obligation de signature, malgré la pratique courante. Le législateur n'a pas à rendre obligatoire ce que la Directive facture prohibe. Comme le veut la Directive, c'est l'obligation de sécuriser la transmission électronique qui impose l'usage d'une signature électronique. Mais opter pour la SE Sécurisée ouvre sur les mêmes interrogations en matière de preuve que le choix d'une SE Avancée. Il est même possible en droit interne d'être plus précis dans les conséquences.

La base de la SE Sécurisée est l'article 1316-4 du Code Civil qui traite de la preuve... des actes sous-seing privé. L'apposition d'une signature "juridique" sur un document qui n'en demande pas tant aboutira à la requalification de la facture. La facture qui est un document commercial, comptable et fiscal deviendra par l'effet de la signature un acte sous-seing privé de l'article 1341 du Code Civil[40]. En cas de contestation de la signature, le droit pourrait entrer en contradiction avec la technique. Lorsque le signataire d'un acte sous seing privé dénie sa signature, l'autre partie n'a d'autre choix que l'article 1324 du Code Civil : solliciter du juge une *procédure en vérification d'écriture*. Le client face à un vendeur qui dénierait sa signature sur une facture électronique ne pourra-t-il recourir qu'à une procédure de vérification de signature, alors que la signature lui garantit techniquement la non-répudiation de la signature par l'émetteur du message[41] ? Et si dans la même hypothèse l'autre partie est l'administration fiscale, ira-t-elle également devant le juge civil ? Bien plus, considérons que la "facture sous-seing privé" est reconnue par le vendeur à qui on l'oppose, aux termes de l'article 1322 du Code Civil, le document acquiert alors la même foi que l'acte authentique en matière de preuve. Dans ces conditions, contester ce type de facture ne peut pas être fait par témoignage, présomptions ou indices, mais seulement par un autre écrit.

Quoiqu'il en soit, depuis notre texte signalé ci-dessus, le législateur a transposé la Directive facturation dans l'article 17 de la Loi de finances rectificative pour 2002[42] : un nouvel article 289 du Code Général des Impôts précisera désormais dans son alinéa 5 : "*les factures peuvent, sous réserve de l'acceptation du destinataire, être transmises par voie électronique dès lors que l'authenticité de leur origine et l'intégrité de leur contenu sont garanties au moyen d'une signature électronique*". Le législateur n'a pas tranché le dilemme : quelle signature électronique utiliser ? Par contre, la question est renvoyée aux partenaires commerciaux : un client ne peut pas être obligatoirement considéré comme destinataire d'une facture électronique, s'il ne l'a pas (préalablement ?) accepté. Dans le cas de relations d'affaires constantes, les partenaires seront inspirés de régler cette affaire entre eux.

Il n'en reste pas moins que faute de précision, la signature électronique à employer n'est pas obligatoirement celle de l'article 1316-4 du Code civil. Laquelle reste-t-il en dehors de la signature des techniciens ? La technique nous montrera, en tout état de cause, que ce n'est pas la même signature qui est employée et pas le même mode opératoire. Ce n'est peut être pas le même signataire. Dans l'entreprise, l'auteur intellectuel signe l'acte juridique ; c'est son secrétariat qui le porte à la poste et remplit le bordereau de recommandé...

---

[37] Cf. "*Classification des signatures électroniques et typologie des emplois*", LAMY Droit de l'Informatique et des Réseaux – fasc. 149 et 152, juil. et nov. 2002.

[38] Dit d'une autre façon la SE Sécurisée ne correspond pas directement à la SE Avancée. Les deux signatures du décret d'application (cf. art1-1° et 1-2°) de l'article 1316-4 sont toutes deux issues de la SE Avancée.

[39] Si la facture électronique possède un format structuré, c'est un message EDI. Si le format n'est pas structuré, c'est un mail.

[40] Cette interprétation est partagée par certains juristes hors de France mais dont le droit civil est proche du nôtre, par exemple, N. VERHEYDEN-JEANMART, *Droit de la preuve*, Bruxelles, Ed. Larcier 1991.

[41] La non-répudiation de l'émission est la 3ème caractéristique technique de la signature électronique avec l'authentification et l'intégrité.

[42] cf. Loi de finances rectificative pour 2002 n° 2002-1576 du 30 décembre 2002.

3) Les moyens techniques de sécurisation de l'échange

Voyons comment la signature électronique est traitée au niveau du message électronique (et non par le fichier attaché supporté par le message électronique). C'est la messagerie électronique qui procédera directement à la signature numérique du mail. On peut prendre comme exemple un des logiciels de gestion de messagerie les plus répandus sur la surface du globe, Outlook Express de MicroSoft qui supporte en standard dans ses versions les plus récentes le traitement de la signature électronique.

Outlook Express est compatible avec les spécifications S/MIME version 2 et 3. Outlook Express et prend en charge les algorithmes de cryptage suivants : RC2 (40 bits et 128 bits), DES (56 bits) et 3DES (168 bits). L'algorithme de cryptage RC2 40 bits et DES sont les seules disponibles pour les versions proposées en dehors des Etats-Unis et du Canada. Outlook Express ne peut utiliser que SHA-1 comme algorithme de hachage pour la signature des messages. Comme dit plus haut, l'application des techniques à base de certificats X509 à la messagerie porte le nom de S/MIME. La version initiale, S/MIME v2, a été développée par un consortium privé d'éditeurs. S/MIME v2 est techniquement lié à l'algorithme d'échange de clés cryptographiques RSA. Comme celui-ci était primitivement breveté par RSA, les RFCs (Request For Comments) de l'IETF décrivant S/MIME n'ont pas été adoptés comme des standards de l'IETF, ils ont tous un *status informational*[43].

La composition d'un message électronique se fait à partir d'une fenêtre spécialisée <nouveau message> accessible depuis la barre d'icônes ou depuis le menu principal du logiciel. A la fin de la rédaction du message, on ouvre le menu déroulant <Outils> ou on cherche dans la d'icônes. Parmi les choix possibles figurent <crypter> et <signer> que l'on recherche. Cliquer sur <signer> met le processus en route : après demande d'un code d'accès à la clé privée, la clé est appliquée au condensé du message, puis le message signé numériquement est déposé dans la corbeille de départ. On pourra contrôler de visu dans la corbeille de départ que le message est bien signé car son icône comporte un ruban rouge.

A destination, le message sera placé dans la corbeille arrivée du vérificateur-destinataire avec la même signalisation. C'est au moment de l'ouverture du message que le destinataire sera informé. Si c'est la première fois que destinataire reçoit un message signé de l'expéditeur considéré, un écran d'alerte l'informera de la présence d'une signature numérique et des possibilités de vérification, notamment par le biais du certificat électronique. Cette signature numérique garantit bien la source du message ainsi que son intégrité arrivé à destination. L'authentification est manifeste à la lecture des rubriques du certificat. Les bidouilleurs qui désireraient contrôler à fond peuvent bricoler le message : ouvrir le message avec un logiciel de type bloc-note, changer ne serait-ce qu'un seul caractère dans le corps du message, le sauvegarder en mode texte puis tenter de l'ouvrir dans Outlook. Le logiciel de messagerie détectera immédiatement l'atteinte à l'intégrité.

[43] cf. "Certificats X509 et Infrastructure de gestion de clés" par AUMONT Serge, GROSS Claude et LECA philippe.

5 La conservation de l'acte sous forme electronique

Selon le rapport du Conseil d'Etat : prétexter la forme électronique d'un acte ne permettra pas de le répudier. La preuve sera administrée à partir de la fourniture du message électronique et de sa signature électronique préalablement archivés. L'archivage devra se dérouler dans de bonnes conditions de fiabilité "certifiées" par un Tiers spécialisé : "*si le document électronique est accompagné d'un certificat répondant à certaines exigences, délivré par une autorité de certification accréditée, la fiabilité de la signature et la conservation durable du document signé (si le certificat a aussi cet objet) sont présumés*".

5.1 Les éléments à archiver

L'archivage intervient dans une phase dite *post-transactionnelle*. Le message signé passe alors concrètement à l'étape de l'archivage électronique, de telle façon qu'il devra être possible ultérieurement de le ressortir, on dira de le *désarchiver*, et de "rejouer" la signature électronique afin d'en vérifier la valeur juridique au moment où l'utilisateur l'avait en mains. A noter que l'archivage peut être le fait d'au moins deux utilisateurs, le destinataire du message ou l'émetteur signataire. Il faut encore déterminer les éléments à archiver. Le fait qu'il soit signé nécessite cependant qu'on envisage l'éventualité d'archiver de concert d'autres éléments.

1) L'archivage de l'écrit électronique et de sa signature

Le rapport du Conseil d'Etat montrait dans le rapport précité comment signature, archivage et preuve sont liés. Le Conseil envisageait le dispositif suivant : "*lorsqu'un document électronique assorti d'une signature électronique est présenté pour établir la preuve d'un acte, il ne saurait être contesté au seul motif qu'il se présente sous forme électronique ; il tient 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*". L'écrit sous forme électronique, hypothèse de travail dans lequel nous nous sommes placés, montre des garanties d'identification et d'intégrité. Dans la grande majorité des cas, l'acte sous seing privé électronique comportera une signature électronique, sécurisée ou non, qui assurera d'office l'identification et l'intégrité recherchées. Aussi faudra-t-il archiver l'écrit électronique et sa signature. Ce qui ne devrait pas poser de difficulté en pratique si on s'en remet aux protocoles techniques qui réunissent dans un même fichier le message électronique et sa signature[44].

Par contre, après une période plus ou moins longue d'archivage, lorsqu'il sera désarchivé, l'acte électronique ne pourra servir de preuve que si la signature électronique est valide[45]. Il faudra alors vérifier la signature, ce qui nécessite l'emploi du certificat électronique. Le certificat sera plus facilement disponible... s'il a été, par la même occasion, archivé !

2) L'archivage du certificat électronique

Placé au centre de la garantie d'identification, le certificat fait l'objet de mesures de conservation spécifiques pendant toutes les étapes de son cycle de vie[46]. Le certificateur[47] le diffuse dès sa création tout en gardant une copie. Créé pour une certaine durée de temps, de l'ordre de 16 à 24 mois, le certificat doit être conservé non seulement jusqu'à la fin de sa durée de validité, mais encore à l'issue de cette période, jusqu'à la fin du cycle de vie du message signé, c'est-à-dire pendant la durée de conservation légale. Sujet à conservation, le certificat est l'aboutissement d'une série de traitements électroniques de certification.

Le 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 pose dans son article 6.II une obligation pour le certificateur d'établir un système de

[44] C'est ce qui est prévu par le protocole PKCS #7 de l'IETF.

[45] Naturellement la validité de la signature électronique s'apprécie au jour de son "apposition" sur le message électronique et non au jour du désarchivage.

[46] Voir le cycle de vie du certificat décrit dans "*Certification et Sécurité dans les échanges électroniques*", Droit@Litec, ouvrage précité.

[47] L'appellation correcte est *prestataire de service de certification électronique* (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.

conservation dont l'utilité est précisée par le point l) de l'article précité. Le certificateur doit utiliser des systèmes de conservation des certificats électroniques garantissant que *:*

- *l'introduction et la modification des données sont réservées aux seules personnes autorisées à cet effet par le prestataire ;*
- *l'accès du public à un certificat électronique ne peut avoir lieu sans le consentement préalable du titulaire du certificat ;*
- *toute modification de nature à compromettre la sécurité du système peut être détectée*".

De façon plus générale, le point k) de l'article stipule qu'un prestataire de services de certification doit satisfaire à certaines exigences comme "*conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique*". Parmi les informations à conserver en priorité pour un système qui est le point central du dispositif d'identification, celles qui correspondent à l'identité des personnes ainsi que les pièces justificatives présentées. Le point m) de l'article le rappelle : *vérifier [...] la qualité dont cette personne se prévaut et conserver les caractéristiques et références des documents présentés pour justifier de cette identité et de cette qualité*".

5.2 L'éventuelle transmission à un archiveur distant

1) Les modalités : archivage interne ou externe

A l'issue d'un envoi de messages sécurisés dans la phase transactionnelle, on ne peut faire moins que de procéder à un archivage sécurisé. Archiver en interne semble la solution la plus évidente est aussi la plus discutable. En effet, en cas de problème interne ou de litige avec les partenaires aux échanges électroniques, comment s'assurer que le message sur lequel on raisonne est bien le message considéré et non une version dérivée ou rectifiée ? Comme le message est resté sous son contrôle de l'utilisateur, l'utilisateur a tout loisir de le modifier. A moins qu'on ait pris une sorte d'instantané du message qui puisse donner toutes les garanties lorsque c'est nécessaire.

Pour alléger les systèmes d'information chargés de messages électroniques post-transactionnels et pour renforcer la confiance et la sécurité, on pourra envisager de faire intervenir un archiveur distant, encore appelé t*iers archiveur*. La distance entre l'utilisateur et l'archiveur entraîne de nouveau l'emploi ou la poursuite des échanges électroniques. L'idée consiste à faire appel à un tiers archiveur extérieur ou à un prestataire à valeur ajoutée offrant une fonction d'archivage en liaison avec la certification électronique. Dans ce cas, l'utilisateur réunit tous les éléments à archiver, messages électroniques, signatures électroniques, clés de chiffrement s'il y a lieu, certificats électroniques et les expédie via des moyens de télécommunications à l'archiveur. Celui-ci à réception effectue plusieurs traitements pour vérifier la permanence des garanties de sécurité pendant le transport électronique entre son client et lui :

- il vérifie que l'émetteur est un client,
- il contrôle que les éléments télétransmis sont arrivés à bon port et en bon état,
- il accuse réception au client des éléments susceptibles d'être archivés en l'état.

A noter que l'entité qu'on appelle par commodité *tiers archiveur* n'est pas réellement un "tiers" au sens de la certification électronique comme on verra ci-dessous, mais plutôt un archiveur distant. Il est à son tour un utilisateur de la certification.

La pratique précédente semble la plus évidente en théorie. Le Tiers Archiveur intervient dans un processus d'échanges électroniques qui se poursuivent vers lui après que la phase transactionnelle des messages électroniques soit terminée. L'inconvénient est qu'il équivaut à transférer par voie de télécommunications un volume important de données, générateur de risques techniques et de coûts non négligeables. D'où la tentation de revenir à un archivage en interne mais faisant appel à une certification externe. L'utilisateur se protégera en faisant appel à un témoin sur lequel il n'a pas de prise directe : le certificateur. Lorsque les archives sont chez l'utilisateur final, émetteur ou destinataire des éléments électroniques archivés, le risque existe que, volontaire ou involontairement, les éléments archivés soient modifiés, corrigés, altérés ou détruits. Au moment de l'archivage, les messages électroniques et les autres éléments ont terminé leur cycle d'utilisation normale. C'est le contenu du message à ce *moment t* qu'il faut retenir comme archive. Ici apparaît la notion de temps. Tout changement de contenu qui surviendrait après ce moment de leur cycle de vie ne serait que manipulation des archives. L'idée consiste dans ce cas à faire reconnaître l'état des messages à un moment déterminé par un tiers objectif qui dans ce cas est... un *tiers horodateur*.

Cette dernière constatation est intéressante au niveau de la théorie de la certification. Il semble nécessaire de distinguer besoin et service. Tel besoin de l'utilisateur n'est pas rempli forcément par le service de même dénomination chez un tiers de confiance. Comme on le voit:

- le besoin d'archivage de l'utilisateur peut être satisfait en externe grâce au service d'un tiers archiveur ;
- le besoin d'archivage de l'utilisateur peut être satisfait en interne grâce au service d'un tiers horodateur.

2) La transmission à un Tiers Archiveur

Les conditions et modalités de l'archivage technique ne sont pas neutres au regard des effets juridiques. Cette constatation avait déjà été faite par le Conseil Supérieur de l'Ordre des experts comptables dans un rapport publié en 1998 sur *L'Archivage Electronique*[48]. Dans la phase précédente, l'utilisateur a préparé la mise en archive. A cette fin, il a récupéré dans le système de stockage, le message à archiver et sa signature électronique. En principe, la signature électronique devrait figurer dans le message ; on se souviendra néanmoins que la signature peut avoir voyagé indépendamment du message auquel elle se rapporte. Enfin il faut nécessairement archiver le certificat électronique qui apporte simultanément la clé publique nécessaire au rejeu de la vérification et la garantie du certificateur que la clé publique appartient à un bénéficiaire, porteur par ailleurs, de la clé privée correspondante et qui a servi à chiffrer la signature. Ces éléments forment au sens du Guide un *lot* qui peut alors être envoyé à l'archiveur.

Le lot à archiver sera envoyé dans des conditions telles que le niveau de sécurité des échanges électroniques perdure. L'archiveur qui recevra les éléments devra pouvoir identifier son client, besoin d'authentification. La mission de l'archiveur est de conserver les informations dans l'état où il les a reçues pour pouvoir les restituer à l'identique ultérieurement. Ce qui suppose en amont qu'il ait bien reçu les informations que l'utilisateur a voulu lui confier, d'où un besoin renforcé d'intégrité des informations. En un mot, le lot des éléments à archiver fera l'objet d'une signature électronique. Il doit cependant être bien entendu que cette signature n'est apposé qu'à titre purement technique uniquement pour sécuriser l'envoi électronique.

3) La nécessité de maintenir l'intégrité pendant le transfert de l'archive

Comme il a été exposé plus haut, l'archivage qui se prétend *sécurisé* doit assurer en priorité un niveau optimal d'intégrité de l'écrit électronique pendant les différentes étapes de son cycle de vie sans négliger d'identification de la source du document.

Les grandes étapes du cycle de vie de l'écrit électronique, création - échange - conservation, peuvent se décliner en de nombreuses sous-étapes, en particulier pour des besoins de changement de support technique de l'écrit électronique. Dans ces points d'articulation, le maintien de l'intégrité doit être particulièrement surveillé : elle doit être garantie avant et après le changement de support. Mais le contenu du message ne reste le même que si l'intégrité perdure au moment du changement de support.

Le maintien de l'intégrité suppose qu'aucune donnée ou information nouvelle ne soit adjointe au corps de l'écrit électronique. Cependant il est nécessaire de considérer les données de services adjointes à des fins purement techniques. La question s'est posé au groupe de travail qui a produit le Guide de l'archivage. Le groupe a raisonné à partir de la notion de *lot* regroupant les éléments à archiver. En effet, l'archiveur doit rester neutre par rapport aux informations archivées. Si on considère que le message incorporant sa signature voyage d'un côté, le certificat peut voyager d'un autre. Dans ce cas, l'archiveur ne dispose d'aucun moyen de savoir que le second message est d'une part, un message électronique et d'autre part, qu'il se réfère à un message précédent. Dans le monde réel, l'archivage se réalise par stockage de boites en carton rassemblant les éléments à conserver, sans que l'archiveur sache nécessairement ce qui est dedans. Cette constatation renvoie à un niveau moyen de confidentialité facile à justifier. D'autre part, les informations à archiver ou les lots qui les contiennent peuvent être chiffrés. Le lien entre message signé et certificat doit nécessairement être géré par le client lui-même. Le client devra peut être encore gérer d'autres spécificités. Par exemple, si le lot à archiver comprend plusieurs messages signés. Le Guide de l'archivage décrit toutes les informations de service qu'il sera nécessaire d'ajouter aux lots à ces fins. Aussi les éléments à envoyer à l'archiveur seront regroupés en lot qui seront scellés par une signature électronique pour garantir la sécurité de la transmission.

[48] Rapport disponible aux éditions du Conseil Supérieur de l'Ordre des Experts-Comptables, Paris.

Au total, il faut considérer que les données techniques et autres données de service lorsqu'elles sont parfaitement documentés et traçables ne remettent pas en cause l'intégrité du de l'écrit électronique.

5.3 Le désarchivage

Les préconisations des normes techniques tendent à maintenir un niveau d'intégrité maximal pendant l'archivage. De même, lorsque les archives seront retournées. La restitution des documents électroniques conservés dans un système d'archivage électronique est définie comme étant l'opération qui vise à les présenter sous une forme exploitable pour le bénéficiaire de cette restitution. La restitution ainsi définie ne doit pas être confondue avec le retour ou la transmission d'archives, en totalité ou en partie, vers leurs propriétaires ou un tiers mandaté à cet effet.

1) La restitution d'archives

Après déstockage du lot demandé, l'archiveur le préparera pour expédition au demandeur. Dans cette phase qui poursuivra les flux électroniques, il importe que l'intégrité soit préservée sans négliger le fait que le client doive être assuré que c'est l'archiveur qui lui renvoie ses informations. Ces opérations, qui peuvent faire appel à des méthodes de sécurisation des transferts ne sont pas décrites par les normes. Le Guide de l'Archivage préconise de sécuriser l'envoi par l'utilisation d'une nouvelle signature électronique[49].

L'opération de restitution pourra être constituée soit par l'affichage sur l'écran d'un système informatique, soit par l'impression d'une copie sur papier ou sur un film. La vertu qu'on recherche dans cette phase est la fidélité de l'archive par rapport à l'écrit électronique d'origine. Cette fidélité est obtenue par l'efficacité de la chaîne d'intégrité. L'archive sera fidèle à l'écrit d'origine, si les copies successives restent intègres :

- lors de la préparation de l'archive (garanties assurées par les procédures préconisées par les normes, comme l'ISO 15489),
- lors de son acheminement électronique et surtout de sa réception par l'archiveur (garanti par la signature électronique de sécurisation),
- lors de son stockage chez l'archiveur (garanties assurées par les procédures préconisées par les normes, comme la Z 42-013),
- lors de son acheminement électronique et surtout de sa réception par son propriétaire (garanti par la signature électronique de sécurisation).

Attention qu'in fine, l'intégrité ne soit atteinte. Aussi aucun traitement sur le contenu de l'archive ne doit être autorisé lors de la restitution.

2) Le désarchivage en interne

Si au contraire, l'archivage a été réalisé en interne, le désarchivage sera plus facilement réalisé et on ne parlera pas de restitution. L'utilisateur devra alors vérifier par lui-même si les archives sont bien dans l'état originel. Cette vérification pourra procéder par degré, toujours par rapport à une référence, le certificat de l'horodatage[50] :

- d'abord, les fichiers chronologiques de son système d'information démontreront que les archives et le certificat sont de la même génération,
- puis, comme le certificat d'horodatage inclut un condensé du texte des archives, il est possible de relancer l'algorithme de hash-coding pour produire un condensé des éléments désactivés,
- enfin, on pourra se tourner vers le tiers horodateur pour comparer le certificat de l'entreprise et celui qu'il a émis.

[49] Comme précédemment, cette signature qui ne vise qu'à sécuriser l'envoi ne rentre pas dans le cadre de l'article 1316-4. Cependant ce moyen électronique ne pourrait être déclaré irrecevable en cas de litige au sens de la Directive européenne sur la signature électronique (article 5.2.)

[50] Dans le langage technique, le certificat de l'horodatage s'appelle *jeton temporel.*

6 La production de l'écrit aux fins de preuve

La loi n°2000-230 du 13 mars 2000 est relative à la signature électronique. Elle vise également un objectif ambitieux contenu dans son appellation l'*adaptation du droit de la preuve aux technologies de l'information*. Le droit français y était d'ailleurs invité par la Directive qui énonce dans son article 5.2. que *les Etats membres veillent à ce que les signatures électroniques avancées basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature (...) soient recevables comme preuves en justice*

6.1 Les deux signatures du décret n°2000-230 et la preuve

Le Décret n°2001-272 du 30 mars 2001 modifié pris pour l'application de l'article 1316-4 du Code Civil et relatif à la signature électronique mentionne deux types de signature électronique : une *signature électronique* stricto sensu et une *signature électronique sécurisée*.

1) Une signature électronique sans rôle défini

Selon la définition de l'article 1-1° du décret 2001-272 modifié, la signature "ordinaire" est "*une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil*". Rappelons que le fragment d'article en question énonce ceci : "*lorsqu'elle est électronique* [la signature], *elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache*".

Pour bien comprendre la nature de cette signature, il convient de revenir à l'article 1316-4 du Code Civil lui-même. L'article commence par une définition de l'instrument : "*La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose*". On retrouve ici un besoin constant du droit comme de la technique, celui d'identifier de façon certaine le signataire du message. Suit dans la seconde phrase cet élément fondamental du droit français, déjà rencontré dans ce papier, le consentement : *"elle manifeste le consentement des parties aux obligations qui découlent de cet acte"*. Un élément primordial dans les pays de droit civil ou le consensus social voire politique est plus difficile à obtenir que dans les pays de *common law*[51]. On peut d'ailleurs vérifier ce qu'il en est dans la directive compromis de la sensibilité d'autant de systèmes juridiques que de pays membres : le consentement sur l'acte n'est visé nulle part. Au risque de hérisser certains juristes français, des quantités de personnes signent des documents sans exprimer un quelconque acquiescement à leur contenu juridique en Europe et dans le monde. Par exemple, leur signature est un visa ; ils ont vu l'acte, ce qui ne veut pas dire qu'ils y consentent. Ils peuvent par leur signature attester que le document existe ou encore qu'ils l'ont vu dans tel état, un visa qui garantit une sorte d'intégrité. Pourtant, on s'y est arrêté plus haut, notre paraphe en marge des pages d'un contrat n'est-il pas une forme de contrôle d'intégrité ?

La question du consentement sur le contenu peut en occasionner des difficultés pratiques dans la transposition de certains textes européens. Comment expliquer à un citoyen français non juriste que la facture électronique n'a pas à être signée juridiquement parlant, mais qu'elle sera tout de même validée par une signature électronique avancée, comme le prévoit une directive récente[52].

2) La primauté de la Signature Electronique Sécurisée

Quelles sont donc les caractéristiques de la "preuve électronique" ? Les mêmes que celles de la preuve écrite-papier en termes d'admissibilité (art. 1316-1) et de portée (art.1316-3). Il y a égalité totale entre la preuve de l'écrit (sur support papier) et la preuve (de l'écrit sous forme) électronique. En cas de dualité de preuves portées devant un juge, ce dernier ne pourra donner sa préférence à l'une des modalités plutôt qu'à l'autre. Il choisira celle qui lui semblera la plus pertinente, comme le lui propose l'article 1316-2.

---

[51] Voir notre article "*Un nouveau dispositif de preuve pour l'EDI basé sur la sécurité*", EXPERTISES des Systèmes d'Information, mai 1994, p. 187 et suiv.

[52] Cf. 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, Journal officiel des Communautés européennes du 17.1.2002 n°L 15/24.

En matière d'administration de la preuve, la cause est entendue ; c'est la signature électronique sécurisée qui sera utilisée. Mais est-on aussi sûr de cette solution ? La *Signature Electronique Sécurisée* (SES) cumule, quant à elle, les caractéristiques de la signature ordinaire du Décret plus quelques exigences complémentaires listées par l'article 1-2° du décret : "[la SES] *satisfait, en outre, aux exigences suivantes :*

- *être propre au signataire ;*
- *être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;*
- *garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable".*

Pour obtenir la meilleure efficacité juridique possible c'est-à-dire pour bénéficier de la présomption de fiabilité, il est préférable d'opter pour une SES plutôt que pour une signature électronique ordinaire du Décret. L'article 1316-4 prend alors tout son sens : la SES doit obéir à des exigences techniques précises pour chacun de ses composants principaux : le dispositif de création de signature électronique et le certificat électronique. Selon les termes de l'article 2 du décret, la fiabilité est présumée "*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*".

Pour le juriste français, la signature électronique sécurisée est la signature parfaite dans son expression technique. Aussi on renverra volontiers aux travaux et recherches de la doctrine décrivant l'intégration de l'instrument technique dans le droit interne et ses effets à moyen terme et à long terme sur l'édifice juridique français, notamment sur la preuve.

6.2 Le retour de la signature simple du décret et la présomption de preuve

L'intérêt de choisir une signature électronique sécurisée (SES) est de faire profiter le signataire de la *présomption de preuve* instauré par l'article 1316-4 du Code Civil, mais il est nécessaire de passer les contrôles indiqués plus haut.

Comme on peut craindre une certaine lourdeur des évaluations et des contrôles, on peut se poser des questions légitimes sur l'intérêt de ces procédures. D'une part, peut-on se prévaloir du caractère sécurisé du DCS, si ce composant technique n'a pas été évalué favorablement ? La réponse est non à la lecture de l'article 3-II du décret 2001-272[53]. D'autre part, peut-on se prévaloir du caractère qualifié du certificat, si ce composant technique n'a pas été évalué favorablement ? Il semble que non à la lecture de l'article 6 du décret 2001-272[54]. Pourtant la qualification des PSCE reste facultative à lire l'article 7 du décret 2001-272[55]. En définitive, le choix d'une signature électronique sécurisée n'est pas obligatoire pour rester dans le cadre de l'article 1316-4 du Code Civil. Ce choix est facultatif, mais si le choix penche pour une SES, alors les évaluations portant sur le DCS et le certificat sont obligatoires. On peut avoir la tentation de faire l'impasse sur la SES et ses procédures parce que ces audits et contrôles génèrent des charges et des coûts qui sont à la charge du demandeur[56]. Naturellement outre l'inconvénient du coût, on peut craindre aussi que ces évaluations, heureusement contradictoires, durent un certain temps...

Le bilan de la signature électronique sécurisée brossé ci-dessus est celui-ci : des procédures de contrôle longues et coûteuses et une efficacité juridique. Si on choisit la *signature ordinaire* du Décret, le signataire perd le bénéfice de la présomption de l'article 1316-4. Mais est-ce si grave ? Après tout, il ne s'agit que d'une présomption de preuve c'est-à-dire jusqu'à l'administration de la preuve contraire. Le signataire "sécurisé"[57] attaqué devant le juge attendra placidement que le demandeur aligne ses experts pour tenter de renverser la présomption. Mais qu'en sera-t-il de la *signature ordinaire* ? Elle ne bénéficiera pas de la présomption. En cas d'attaque, le titulaire devra démontrer sa fiabilité. Par ses experts. Ce qui ne veut pas dire que l'attaquant

---

[53] Article 3-II du décret 2001-272"*Un dispositif sécurisé de création de signature électronique doit être certifié conforme aux exigences définies au I*".

[54] Article 6 du décret 2001-272 : "*Un certificat électronique ne peut être regardé comme qualifié que s'il comporte les éléments énumérés au I et que s'il est délivré par un prestataire de services de certification électronique satisfaisant aux exigences fixées au II."*

[55] *Article 7 du décret 2001-272 : "Les prestataires de services de certification électronique qui satisfont aux exigences fixées à l'article 6 peuvent demander à être reconnus comme qualifiés".*

[56] Voir l'arrêté sur la qualification des PSCE, article 7 : *"L'évaluation est effectuée par l'organisme aux frais du prestataire de services de certification*" et le décret n°2002-535, article 3 : "*le commanditaire de l'évaluation choisit un ou plusieurs centres d'évaluation (...) Avant le début des travaux, il détermine avec chacun de ces centres : (...) c) le coût et les modalités de paiement de l'évaluation...*"

[57] A noter que si brusquement le DCS perd sa reconnaissance de sécurisation ou si le PCSE cesse d'être qualifié et/ou que le certificat cesse d'être qualifié, la signature sécurisée perd sa qualité de sécurisée. Et la présomption, avec.

bénéficiera, lui, d'une présomption. Naturellement, il devra également aligner ses experts. D'où, une belle bataille d'experts en perspective... Si on laisse de côté la SE-SES, quelle alternative reste-t-il ? Celui de la *Signature Electronique*, sans autre précision, de l'article 1 du décret 200-272. L'emploi d'une signature ordinaire est une voie qui nous semble devoir être examinée.

Pour tout service qui ambitionne d'offrir à ses clients une *signature électronique sécurisée*, mais en fonction de ce qui est dit plus haut, le jeu en vaut-il la chandelle ? Au vu des normes réglementaires, on peut établir une sorte de typologie de signature en trois niveaux :

- niveau bas : la *signature électronique ordinaire*, une signature qui assure identification et intégrité (1ère phrase du second alinéa de l'article 1316-4), sans autre précision et sans mécanisme de contrôle,
- niveau haut : la *signature électronique sécurisée* avec DCS sécurisé et certificat reconnu qualifié par le biais de la qualification du PSC,
- niveau intermédiaire : une *signature innomée* ("ordinaire" par la force des choses) avec un DCS conforme à l'art. 3 et un certificat conforme à l'art. 6-I émis par un PSCE conforme à l'article 6-II.

En conclusion de l'étude de cette étape, on peut estimer que les besoins de sécurité technique en matière de preuve de l'écrit sous forme électronique seraient satisfaits par l'emploi d'une *signature électronique sécurisée* (SES) ou peut-être même par une signature électronique ordinaire du Décret.