Projet ICare

Typologie juridique des signatures électroniques

Référence : ICARE/CAB/TPC/DOC_13/v1
Type : Note d'information
Diffusion : Publique

Date : 16/10/2002
Titre : **ICare – Typologie et emploi des signatures électroniques.**

Auteur(s) : Thierry Piette-Coudol, avocat

Résumé :
Aux yeux des juristes, il existe plusieurs types de signature électronique possédant un impact juridique plus ou moins fort. Le but de ce papier est de lister les différentes signatures identifiables par un juriste et de les classer. Puis il sera question de choisir une signature pour chaque étape du cycle de vie du message électronique.

TABLES DES MATIERES

1. Introduction

Procédant à la transposition de la Directive signature électronique dans des délais honorables, la France a intégré ce puissant instrument qu'est la signature électronique dans son Code Civil. Quoiqu'une année ait été nécessaire pour la sortie d'un premier texte d'application et que le dispositif législatif n'est pas encore complet, signatures et certificats électroniques sont disponibles chez plusieurs fournisseurs du marché.

Quelle signature électronique utiliser ? La question est moins paradoxale qu'il n'y paraît, car la simple lecture des textes juridiques et européens montre à l'évidence qu'il y a plusieurs signatures électroniques. Le besoin est alors manifeste de bâtir une classification (Première Partie), et certains s'y sont déjà lancés, première étape d'une recherche afin de répondre à l'issue de l'analyse aux attentes légitimes des utilisateurs en matière de typologie des emplois (Deuxième Partie).

Afin de procéder à une tentative de classification juridique, il importe tout d'abord de rassembler les éléments et caractéristiques intéressant les questions juridiques et susceptibles de fournir au juriste des points d'entrée dans un tableau d'ensemble.

1.1. La recherche de caractéristiques pour une classification des signatures électroniques

Il est bien précisé que cette approche est propre au juriste français ; le génie et la logique propres à d'autres systèmes juridiques pouvant porter les juristes nationaux vers un autre type d'approche. Ces éléments proviennent de différentes origines :

- le consentement à l'acte et l'identification du signataire, du régime juridique de la signature,
- l'admissibilité et la portée, du droit de la preuve
- l'authentification et l'intégrité, du régime technique de la signature électronique.

Tout d'abord pour une signature électronique intégrée dans le Code civil français au titre de la preuve des obligations, nous retiendrons les classiques notions d'*admissibilité* et de *portée*[1]. Il s'agit d'éviter la répudiation générale et globale d'une signature au motif qu'elle est électronique. La signature étant admise, sa *portée* correspond à la force qu'elle possède pour emporter la conviction du juge, face à des éléments de preuve contraires. Dans le dispositif légal français, le juge pourra mesurer sa portée à l'aune de son degré de fiabilité. D'un autre côté, la signature en soi (manuscrite ou électronique) identifie le signataire et *manifeste son consentement* quant au contenu de l'acte. Enfin en ce qui concerne la modalité électronique de la signature, le législateur a insisté sur une identification déjà connue dans le monde papier et a introduit dans le droit la notion d'intégrité. L'*intégrité* est la qualité d'un message électronique parvenu entre les mains d'un destinataire sans modification et sans altération après une *transmission* électronique telle qu'envisagée par l'article 1316 du Code Civil. Restent les caractéristiques proprement juridiques de la signature en droit interne : l'identification du signataire et le consentement à l'acte. La garantie d'authentification apportée par la signature électronique devrait satisfaire le besoin d'identification de la signature juridique. Par contre, la question du consentement à l'acte conduit à quelques réflexions liminaires.

1.2. Un caractère fondamental de la signature : le consentement à l'acte

Classiquement la doctrine[2] et la jurisprudence affirmaient que la signature est une marque personnelle de l'auteur du texte. Cela est vrai au point que la forme la plus élémentaire de la signature s'appuie sur la transcription du nom. Il en va tout autrement de la signature électronique dont la base est le message lui-même, un message dont le condensé calculé par un logiciel spécialisé est personnalisé (chiffré) par un élément propre au signataire, sa clé

[1] L'admissibilité est la qualité d'un fait ou d'un acte qui peut être reçu devant un tribunal comme élément de preuve sans être repoussé a priori.

[2] L'Observatoire Juridique des Technologies de l'Information (OJTI), aujourd'hui disparu, a possédé un groupe de travail sur "les aspects juridiques de la signature numérique dans l'E.D.I." dont le rapport publié en 1993 est encore disponible à la Documentation Française.

privée. Ce rappel est nécessaire pour corriger une affirmation fréquente selon laquelle le consentement sur le contenu est assuré par la garantie d'intégrité. Le consentement doit être manifeste selon la loi, ce qui s'analyse sur les deux éléments suivants :

- Le consentement porte sur le contenu d'un acte juridique[3]. Pour s'assurer de la concordance d'un contenu juridique avec sa volonté, le (futur) signataire doit préalablement lire le document avant de procéder à sa signature.
- Pour que le consentement soit manifeste, il faut le... manifester de façon volontaire. Ce qui exclut tout traitement automatique. Il est bon de rappeler que certains serveurs d'entreprise sont susceptibles de signer à la volée tous les messages électroniques qui en sortent sans intervention humaine.

Le consentement sur le contenu reste une caractéristique purement juridique qui ne peut être gérée et calculée par la machine. Le consentement d'un être humain doit être manifeste, notamment par sa signature. L'acte volontaire consiste à dessiner la signature par la main prolongée d'un stylo ou dans le monde électronique par le lancement d'un dispositif technique de signature.

A titre d'illustration, voici un premier type de signature électronique qui ne sera pas directement intégré dans notre tentative de classification : la signature de la Commission des Nations Unies sur le Droit Commercial International (CNUDCI). La signature de la CNUDCI n'est définie que dans un instrument dit *Loi-type*. Les lois-types sont préparées pour inciter les Etats à intégrer dans leur droit interne de nouvelles législations compatibles avec une certaine internationalisation du droit. Aussi le juriste praticien français ne peut la rencontrer dans les échanges électroniques, ce qui explique qu'elle ne figure pas dans la classification. Penchons-nous cependant sur l'article 2 de la loi type de la CNUDCI sur les signatures électroniques[4] et particulièrement sur un instrument que nous nommerons SE-CNU par convention. On y lit la définition suivante :

"a) Le terme "signature électronique" désigne des données sous forme électronique contenues dans un message de données ou jointes ou logiquement associées audit message, pouvant être utilisées pour identifier le signataire dans le cadre du message de données et indiquer qu'il approuve l'information qui y est contenue".

Cette définition indique comme caractéristique de la signature électronique l'identification et le consentement à l'information. On ne voit pas trace de prime abord de la question de l'intégrité. La notion n'est toutefois pas totalement absente : on la retrouve sous le couvert de la notion de fiabilité dans l'article 6 "Satisfaction de l'exigence de signature" :

1.Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données s'il est fait usage d'une signature électronique dont la fiabilité est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris toute convention en la matière.

L'article 6-3 indique ce qu'on peut entendre par fiabilité :

"Une signature électronique est considérée fiable en ce qu'elle satisfait à l'exigence indiquée au paragraphe 1 si : ... d) Dans le cas où l'exigence légale de signature a pour but de garantir l'intégrité de l'information à laquelle elle se rapporte, toute modification apportée à cette information après le moment de la signature est décelable.

Ceci nous conduit à une interrogation sur le droit français : dans quels cas la signature garantit-elle l'intégrité dans le monde du papier ? Est-ce le cas du *paraphe* en marge du contrat ou de façon plus générale, du "*scellement*"[5] opéré sur un acte selon des modalités ou des fins qui restent à établir ?

On verra comment le droit français intègre dans la signature les notions de fiabilité et surtout de consentement à l'acte, alors que pour cette dernière les textes européens restent muets.

---

[3] Il s'agit d'un consentement sur un contenu juridique c'est-à-dire d'un contenu qui ne se présente habituellement que sous deux modalités, le plus souvent des obligations quelquefois des droits.

[4] Rapport de la Commission des Nations Unies sur le droit commercial international sur les travaux de sa trente-quatrième session, tenue à Vienne du 25 juin au 13 juillet 2001, adopté le 5 juillet 2001. Disponible au service des publications de la CNUDCI ou sur son site Web : www.uncitral.org .

[5] Selon le *Guide de l'archivage sécurisé* de EDIFICAS / IALTA, le sceau ou l'empreinte d'un texte est une réduction de celui-ci obtenu à partir d'un algorithme de hachage. Lorsque ce sceau est chiffré par une clé cryptographique privée, il devient une signature électronique.

2. Essai de classification des signatures electroniques

En première approche, nous disposons de quatre signatures juridiques, deux issues de la Directive (signature électronique et signature électronique avancée) et deux issues du droit français (signature électronique et signature électronique sécurisée). Sur cette base et en observant les caractéristiques techniques et juridiques des diverses signatures électroniques existantes, un essai de classification peut être tenté par et pour le juriste français.

2.1. La signature numérique des techniciens

La première des signatures électroniques est celle développée par les techniciens. 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)".* C'est à partir de cet instrument que les juristes de l'American Bar Association ont émis les premières réflexions tendant à l'implémentation de la signature technique dans un environnement juridique[6]. Par convention, nous désignerons dans ce papier cette signature par SE-ISO.

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[7]. Cette distinction n'empêchera pas certains produits ou certains textes de préférer le terme de signature numérique.

La SE-ISO est générée par un logiciel (ou un matériel) susceptible de comporter un second module pour la vérification de la signature. Cette dernière nécessite l'intervention d'une Autorité de Certification qui émet le certificat comportant la clé publique. A son actif, cette signature est susceptible d'assurer l'identification et l'intégrité, ce qui n'est pas obligatoirement le cas de la signature ordinaire de la Directive comme on le verra ci-après. Par contre, la SE-ISO n'apporte aucun élément sur la question du consentement du signataire. Certes on peut constater que le *destinataire c*ité est un être humain. Mais le signataire ? Existe-t-il en tant qu'être humain ou bien le destinataire a-t-il simplement affaire à une entité technique qui signe automatiquement ? Soulignons qu'il n'y a pas de signature au sens du droit s'il n'y a pas un être humain signataire. Cette question se reposera avec la signature ordinaire de la Directive.

Pour en terminer, la SE-ISO qui est la vraie signature électronique des techniciens est-elle libre de toute interférence avec le domaine juridique ? Il semble que non selon l'interprétation qui sera donnée à l'article 5.2. de la Directive (cf. INFRA).

2.2. La Signature Electronique "ordinaire" de la Directive

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.

[6] Voir le rapport "Digital Signature Guidelines" qui incorpore également l'US Model Digital Signature Law publié en 1995 par l'ABA. Les Guidelines sont téléchargeables sur le site de l'ABA : www.abanet.org/scitech

[7] 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.

2.2.1. La définition de la SE-DIR

L'article 2 de la Directive précise :

"on entend par «signature électronique», une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification".

Nous désignerons dans ce papier cette *signature électronique ordinaire*[8] comme la SE-DIR. 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 dont la signification et l'intérêt échappent de prime abord au juriste[9].

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 semble présenter aucune des caractéristiques que le droit accorde à la signature. Elle ne donne aucun gage du consentement du signataire. On peut d'ailleurs douter que la SE-DIR ne soit créée par un être humain signataire, tandis que la Directive envisage une signature avancée qui, elle, est rattachée à un signataire.

2.2.2. Les différentes espèces de SE-DIR

La SE-DIR ne prétend pas assurer l'intégrité. Elle ne fera pas appel à un algorithme de hachage permettant d'obtenir un condensat du texte, parade sécuritaire habituelle pour vérifier l'intégrité d'un texte signé arrivé à destination. La définition générale est susceptible de s'appliquer à de nombreux types de signatures technologiques :

- ainsi les mesures biométriques, les signatures graphiques, les signatures électroniques avancées "dégradées",
- et dans un deuxième temps, les certificats et les signatures numériques.

Les mesures biométriques semblent évidement visées par cette définition. Les mesures telles que le fond de l'œil, l'empreinte digitale ou le code génétique, permettent bien d'identifier un individu avec une faible marge d'erreur. Mais elles s'intéressent à un individu et non à un message électronique. On comprend qu'il soit impossible d'appliquer une garantie d'intégrité. Les signatures graphiques sont basées sur la reproduction du tracé de la signature manuscrite. Aujourd'hui, les plus performantes ne s'arrêtent pas au seul dessin et prennent également en compte la vitesse, les accélérations et la pression exercée par la main qui signe. Ces signatures s'attachent réellement à la signature et à l'être humain qui la trace, mais pas au document signé. En général, elles ne contrôlent pas l'intégrité. Nous rangerons également dans cette catégorie, les signatures avancées que nous qualifierons de *dégradées* dans la mesure où un des composants de la signature ne possède pas tous les satisfecit juridiques prévus par la Directive. Si la SE-DIR est une signature avancée dégradée, il est possible de lister l'ensemble des composants intervenant dans le processus de signature. Ce sont les composants techniques traditionnels de la signature électronique avec Infrastructure à clés publiques (ICP) vus sous l'angle et la dénomination juridiques : dispositif de création de signature électronique, dispositif de vérification, certificat, données afférentes à la création et à la vérification de signature, prestataire de services de certification.

Dans le processus de signature électronique, l'authentification repose sur la clé publique de l'émetteur de message certifiée par le certificateur[10]. Dans ce cas, en considérant le certificat seul, celui-ci ne répond-il pas aux termes de la définition de la Directive ? Il semble que oui. Une semblable interprétation est mise en avant par

[8] Faute d'autre appellation dans la Directive, c'est nous qui la qualifions d'ordinaire. Nous avons renoncé au qualificatif de simple, car cette signature est aussi complexe que les autres !

[9] Sur les interrogations légitimes du juriste sur les deux types de signature, voir par exemple "Digital Signature Legislation in Europe" par SINISI Vicenzo, International Business Lawyer, décembre 2000 p. 487 et suiv. Questions et doute sont levés (?) par l'exposé de deux administrateurs de la Commission : la signature ordinaire est fondée sur une approche "technologiquement neutre" afin d'offrir un large éventail de technologies, par exemple le signatures numériques ou la biométrie, "La Directive européenne pour les signatures électroniques", par BARESC Denis et SION Claire, Les Petites Affiches, 21 février 2002, n°38 p.21.

[10] avec pour chaque émission de certification, le contrôle qu'une clé privée existe, d'abord et ensuite, qu'elle correspond à la clé publique incluse dans certificat.

certains produits et services du marché qui affirment travailler avec une signature électronique (ou numérique), alors que seul le certificat est visible[11].

Enfin, revenons aux signatures numériques du paragraphe précédent. Exploitons encore une fois l'adage *qui peut le plus peut le moins*. Si la définition de la SE-DIR 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 SE-ISO répond *a maxima* à la définition de la Directive. Mais quel intérêt d'assimiler la SE-ISO à une sous-catégorie de SE-DIR ? L'enjeu repose dans les effets juridiques.

2.2.3. Les effets juridiques attachés aux SE-DIR

Pour apprécier les effets juridiques des SE-DIR, 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. Cependant la non-application à un acte juridique ou sa simple forme électronique ne suffit pas pour que la signature électronique soit exclut des instruments juridiques. Par application de l'article 5.2., la SE-DIR serait admissible aux fins de preuve, quoiqu'on puise s'interroger sur sa portée exacte.

La réflexion est de même nature pour une signature qu'on aurait voulu *avancée* mais qui à l'expérience aurait été créé par un système quelconque c'est-à-dire non sécurisé ou ferait l'objet d'un certificat non qualifié ou encore d'un certificat certes qualifié mais émis par un PSC non qualifié. Bref, cette signature imparfaite aurait tout d'une signature avancée *dégradée*. Une semblable signature devrait également être admissible devant un tribunal, même si sa portée était, naturellement, diminuée.

En ce qui concerne une dernière caractéristique juridique, on devra dire que la SE-DIR n'est pas en mesure de fournir quelque assurance que ce soit en matière de consentement du signataire. La question du consentement typique du droit français est d'ailleurs à revoir par rapport à la Directive européenne qui ne l'inclut pas dans les caractéristiques de la signature par opposition à la loi type de la CNUDCI.

2.3. La Signature Electronique Avancée de la Directive

2.3.1. Description et caractéristiques de la SE-SAV

La même Directive du 13 décembre 1999 envisage dans ses définitions une seconde variété de signature que nous désignerons ici par convention comme SE-SAV. Le texte définit ainsi cette nouvelle variété :

"*on entend par «signature électronique avancée», une signature électronique qui satisfait aux exigences suivantes :*

a) être liée uniquement au signataire ;
b) permettre d'identifier le signataire ;
c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif
et d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable ;

[11] Face à un doute de ce genre, il faut rechercher s'il existe vraiment dans cette offre de service le module de signature à proprement parler que le droit nomme "dispositif de création de signature".

Par opposition avec la Signature Electronique ordinaire de la Directive, cette définition mentionne un être humain, le signataire. Comme cette signature identifie le signataire (point c), elle peut constituer une véritable signature sous forme électronique pour les juristes. Et le point d demande la mise en place d'une garantie d'intégrité. Les a, b et c peuvent être commentés sous différents points de vue juridique :

- Liée uniquement au signataire, la SE-SAV lui est personnelle[12].
- Comme la SE-SAV est propre au signataire, elle permettra de l'identifier par le biais de la clé publique certifiée par le PSC.
- Les moyens de signature devront être mis en œuvre par le signataire, ce qui rappelle que la signature juridique est un acte volontaire.
- La délégation de signature n'est pas possible[13]. La clé privée doit rester confidentielle et sous le contrôle du signataire.

Le processus de SE-SAV met en œuvre les mêmes composants que la SE-DIR mais en présentant un niveau de confiance ou de sécurité plus élevé[14] , en particulier :

- Le dispositif de création de signature électronique (DCS) est *sécurisé*. Il doit respecter une série de spécifications fonctionnelles listées dans l'annexe III de la Directive,
- Le certificat doit être *qualifié* c'est-à-dire qui satisfait aux exigences de l'annexe I et qui est fourni par un prestataire de service de certification satisfaisant aux exigences de l'annexe II,

2.3.2. Effets juridiques de SE-SAV

Ainsi définie, la SE-SAV n'est pas seulement un sur-ensemble de la signature ordinaire de la Directive. Elle est la signature pleine et entière des juristes, celle qui est susceptible de produire les effets juridiques cités dans l'article 5.1. :

"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 :

a) répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier,

et b) soient recevables comme preuves en justice".

Le point b sur la preuve de l'article est la conséquence la plus attendue de la reconnaissance de la validité juridique de la signature électronique. La formulation ampoulée du point a) permet d'élargir les objectifs juridiques potentiels dans les Etats membres :

- la preuve en justice est dans la cible pour tous les pays,
- mais également la sauvegarde du formalisme juridique principalement dans les pays de droit civil
- et enfin, les autres caractéristiques de la signature propres au droit des Etats membres de l'Union, un à un.

Au total, la SE-SAV garantit l'identification et l'intégrité. Elle est admise en justice et possède une force probante maximale. Mais elle n'apporte aucun certitude en matière de consentement. Le juriste pourra d'ailleurs se demander quels seraient les cas d'application de SE-SAV. A priori aucune ! Si l'existence d'une droit européen peut se concevoir, il n'existe pas d'acte juridique européen, au moins au sens du droit privé. En conséquence, la SE-SAV ne trouve aucun support sur lequel se poser. Les actes juridiques se rencontreront dans le droit des Etats membres où se déclinera la SE-SAV dans une variante nationale.

2.4. La Signature Electronique "ordinaire" du Décret

La 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 a intégré la signature dans le Code Civil en renvoyant à un décret d'application en Conseil d'Etat les exigences techniques. Ce Décret n°2001-272 du 30 mars 2001 modifié pris

[12] Cette caractéristique renvoie à ce qui a été rappelé plus haut : la signature est une marque personnelle propre à son auteur.

[13] En matière de délégation de signature, c'est l'acte de signer qui est délégué et non pas la signature-marque personnelle : le délégué appose sa propre marque ; il n'imite pas le tracé du délégataire.

[14] L'article 5.1. montre dans un fragment de phrase que les signatures électroniques avancées sont "*basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature*".

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*.

2.4.1. La nature juridique et le régime juridique SE-DEC

Dans le Décret d'application de l'article 1316-4 du Code Civil, on rencontre d'abord une *signature électronique "ordinaire*[15]*"*. Selon la définition de l'article 1-1°, cette signature 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"*. Par convention, nous désignerons dans ce papier cette signature par SE-DEC.

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*[16]. 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[17]. 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[18].

2.4.2. La SE-DEC et la signature électronique avancée de la Directive

Comment relier cette SE à la française au niveau européen. Le décret comme la Directive possède deux niveaux de signatures électroniques : une *S.E. ordinaire* et une *signature électronique avancée / sécurisée*. Est-ce à dire que la signature électronique ordinaire du décret correspond à celle de la Directive ? Nous ne le pensons pas parce que la SE-DIR est issue d'un texte d'application du Code Civil et que :

- elle est donc une signature juridique, ce que n'est pas la SE ordinaire de la Directive, même si on ne peut la répudier en justice ;
- la SE du décret est apposée par un être humain signataire ;
- et surtout, la SE-DEC est apposée pour formaliser le consentement du signataire sur le contenu juridique de l'écrit électronique.

A l'opposé la SE-DEC peut-elle se présenter comme une variante française de la SE-SAV ? Pour ce faire, elle devra élever le niveau de sécurité de ses composants, en particulier :

- le dispositif de création de signature électronique devra être conforme aux spécifications fonctionnelles de l'annexe III de la Directive,

---

[15] Faute d'autre appellation plus précise dans le Décret, c'est nous qui la qualifions d'*ordinaire*.

[16] 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.

[17] A moins de considérer de façon très extensive que la périphrase "*les signatures électroniques avancées (...) répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites*" permet d'inclure le consentement à l'acte dans les effets de la SE-SAV !

[18] 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. La question sera commentée dans la seconde partie de ce texte.

- tandis que le certificat pourra être conforme aux exigences de l'annexe I, tout en étant émis par un prestataire de service de certification satisfaisant aux exigences de l'annexe II.

Or on peut constater que les exigences techniques des annexes de la Directive sont reprises par les articles 3 et 6 du Décret. Même si la SE-DEC de l'article 1-1° n'est pas concernée directement par les articles 3 et 6, elle ne peut pas ne pas se conformer aux obligations issues des annexes de la Directive (c'est-à-dire pratiquement celles du décret). La différence finale entre SE-DIR et la *signature électronique avancée* qui suit dans l'article 1-2° du Décret porte sur les effets juridiques en matière de preuve : bénéfice ou non de la présomption de preuve de l'article 1316-4. La SE-DEC ne bénéficie pas de la présomption ; la *signature électronique sécurisée*, si.

En résumé, la SE-DEC pourrait se trouver dépourvue d'efficacité juridique parce que les exigences techniques à respecter ne sont pas énoncées. Et même énoncées, leur reconnaissance officielle reste facultative, comme l'indique les termes du décret. Bref, si un prestataire de SE-DEC pour étayer son offre commerciale se réclamait des annexes de la directive ou des articles du décret et pouvait le démontrer par une attestation d'un organisme habilité, il ne commercialiserait pas une SE-DEC mais bel et bien, une signature électronique sécurisée, même s'il ne pourrait pas s'en réclamer officiellement !

Ce qui nous permet de formuler une première conclusion, la SE-DEC n'est qu'une signature électronique sécurisée *dégradée*[19]. La seconde conclusion est qu'en définitive, les deux signatures du décret sont des signatures avancées au sens de la directive !

2.4.3. Les différentes espèces de SE-DEC

Comme pour la signature ordinaire de la Directive, nous pouvons nous poser la question de l'existence de différents types de signature ordinaire du Décret. L'inclusion de la SE-DEC dans l'environnement juridique ne permet pas d'y classer les mesures biométriques et les signatures strictement numériques (SE-ISO). Mais dans une analogie avec les signatures avancées dégradées, peut-on penser qu'il existerait une forme de signature sécurisée dégradée ? Il semble qu'une réponse positive doive être apportée.

Une lecture attentive de l'article 2 du Décret s'impose qui indique qu'une *signature électronique sécurisée* est *"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*". Continuons sur la qualification du certificat... Le caractère qualifié du certificat peut avoir deux origines :

- la *reconnaissance* : La reconnaissance de la qualification des PSCE est prononcée à l'issue (positive) de l'évaluation dont la procédure et les modalités ont été établies par l'arrêté du 31 mai 2002. L'article 7 du Décret mentionne à ce sujet que les contrôles portent sur le certificat (art. 6-I) et sur le fonctionnement et l'organisation du PSCE (art. 6-II). Bref, un PSCE qualifié émet nécessairement des certificats qualifiés.
- l'*autoproclamation* : Si la qualification des PSCE est facultative, par contre l'accomplissement des formalités administratives liées à la fourniture de prestations de cryptologie[20] reste obligatoire. A cette occasion, article 9 du Décret, le PSCE doit indiquer qu'"*il entend délivrer des certificats électroniques qualifiés*". Dans ce cadre précis de la réglementation de la cryptographie, la DCSSI peut éventuellement procéder d'office à un contrôle de conformité du certificat (art. 9-II 2ème alinéa)[21]. A défaut, le caractère qualifié du certificat est bien autoproclamé par son créateur, le PSCE.

Au total, un certificat peut se dire qualifié alors que d'une part, il n'aura pas été évalué à l'occasion de la procédure de qualification des PSCE et que d'autre part, il aura pu éviter la saisine d'office de la DCSSI. Dans le présent article, l'exercice ne consiste qu'à imaginer des catégories de SE. Aussi peut-on raisonnablement penser

[19] Ce qui ne l'assimile pas pour autant à la signature ordinaire de la Directive (SE-DIR) qui est aussi une forme dégradée. La SE-DEC est imparfaite au niveau du dispositif technique qui ne dispose pas de toutes les reconnaissances nécessaires, la SE-DIR est imparfaite au niveau de son régime juridique car elle ne rend pas compte du consentement d'un signataire dont on n'est pas sûr, d'autre part, qu'il soit humain ou que la signature soit volontaire.

[20] Formalités prévues par l'article 28 de la loi du 29 décembre 1990 et les textes subséquents.

[21] A remarquer que l'article 8 de l'arrêté du 31 mai 2002 sur la qualification prévoit que la DCSSI peut demander la communication des dossiers de qualification des PSCE.

qu'une semblable signature sera une Signature Electronique Sécurisée "*dégradée*". Cependant pas de régime particulier ni de régime intermédiaire pour celle-ci, elle devra se contenter d'être une SE-DEC[22].

Avec un certificat qualifié "autoproclamé", une offre de signature électronique pourra peut-être éviter la vérification de l'article 7 du Décret, c'est-à-dire sans audit par des techniciens spécialisés dans la sécurité.

2.5. La Signature Electronique Sécurisée du Décret

La Signature Electronique Sécurisée, que nous désignerons par convention SE-SES, cumule, quant à elle, les caractéristiques de la signature SE-DEC 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 SE-SES plutôt que pour une signature électronique ordinaire du Décret. L'article 1316-4 prend alors tout son sens : la SE-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.

EN CONCLUSION :

La première partie de ce texte recensait six signatures électroniques susceptibles d'intéresser les juristes. A l'issue des réflexions formulées sur celles-ci dans la première partie, il apparaît que seules trois de ces signatures sont exploitables par le juriste français dans le cadre d'échanges électroniques :
- la signature électronique (ordinaire) de la Directive européenne (SE-DIR),
- la signature électronique (ordinaire) du décret d'application de l'article 1316-4 du Code Civil (SE-DEC),
- la signature électronique sécurisée du décret d'application de l'article 1316-4 du Code Civil (SE-SES)[23].

[22] A moins naturellement de compléter sa palette de composants techniques par un dispositif de création de signature électronique. Un dispositif qu'il pourra qualifier de "sécurisé", s'il l'a fait évaluer par un organisme reconnu d'un Etat membre de l'Union (art.3-II-2° du Décret), auquel cas il n'aurait pas à présenter la même demande à la DCSSI 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) (art.3-I-1° du Décret).

[23] La signature électronique de la CNUDCI et la Signature Electronique Avancée de la Directive européenne ne sont que des instruments-type et ne peuvent être rencontrées telles qu'elles dans les échanges électroniques. Cependant cette dernière se décline dans le droit français dans les deux variantes opérationnelles du décret d'application de l'article 1316-4 du Code Civil. Enfin la signature électronique des techniciens (de type ISO) peut toujours être utilisée dans un contexte purement sécuritaire. Mais dès qu'un litige survient et que cette signature acquiert une certaine force probante, elle sera, selon nous, assimilée par la signature électronique (simple) de la Directive.

3. Typologie des emplois de signature electronique

Un acte sous-seing privé, qu'il se présente sur support papier ou sous forme électronique, ne reste pas dans un état statique. Il connaît différents sorts au cours de différentes périodes, de sorte qu'on peut parler de *cycle de vie* de l'acte. En ce basant sur les dispositions du Code Civil, on peut estimer que le cycle de vie de l'acte sous-seing privé sous forme électronique comprend au moins les trois étapes suivantes :

- la création, parce que l'article 1316-1 indique qu'il est "établi" ;
- la transmission, parce que l'article 1316 envisage des modalités de transmission[24] ;
- la conservation visée par l'article 1316-1.

A cela, on ajoutera la question de la preuve de l'acte sous-seing privé, question transversale car susceptible de se poser à n'importe quel moment du cycle de vie. A chaque moment du cycle également, une signature électronique peut intervenir pour produire des effets spécifiques. Il importe d'identifier quel type de signature est utile et efficace à chaque étape du cycle.

3.1. La formation de l'acte sous forme 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[25]. Ce qui dépoussière une ancienne notion juridique jusqu'alors sans beaucoup de portée pratique. Cette notion qui nous est chère[26], le *formalisme juridique*, 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 est l'ensemble des 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.

3.1.1. Formalisme juridique et dématérialisation

Un texte de loi peut requérir un support papier[27] pour un acte précis (c'est-à-dire ne laisse pas 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[28].

---

24 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.*"

25 Le nouvel article 1317 parle de *"support électronique"*. Pour nous, 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 avec la création 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.

26 Voir à propos de l'EDI, notre article "La véritable problématique juridique de l'EDI : le formalisme avant la preuve", Cahier du LAMY droit de l'informatique, décembre 1990 et janvier 1991.

27 Il y a d'autres éléments dans le formalisme juridique. Par exemple, l'obligation de signer l'acte ! Dans ce cas, l'emploi d'une signature électronique sécurisée semble une bonne solution. Mais peut-être une solution maximaliste, on le verra plus loin.

28 Sur l'actualité de l'ancien débat écrit-preuve et écrit-condition de validité, voir "*La reconnaissance de la preuve électronique a-t-elle épuisé la question de la dématérialisation ?*", BRAHMI Adel, Les Petites Affiches n°36, 19 février 2002, avec une réponse plutôt négative.

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[29] dont certaines dispositions prévoient que les contrats pourront être négociés par voie électronique.

Cette directive devrait être transposée en droit interne par la Loi sur la Société de l'Information (LSI). Au début du mois d'avril 2001, le projet de loi LSI a fait l'objet d'une première communication au public. Dans le projet de loi sur la société de l'information, section 3 "*Contrat par voie électronique*", l'article 3.8 prévoit d'insérer après le chapitre VI du titre III du livre troisième du Code Civil, un chapitre VII intitulé "Des contrats ou obligations sous forme électronique", comprenant des articles 1369-1 à 1369-5. L'article 1369-1 serait ainsi rédigé :

"Lorsqu'un écrit est exigé pour la validité d'un acte juridique, celui-ci peut-être établi et conservé par écrit sous forme électronique dans les conditions prévues aux articles 1316 à 1316-4 ou 1317."

3.1.2. Dématérialisation et signature électronique

Laissons de côté, le renvoi à l'article 1317 qui fait référence aux actes authentiques électroniques. Restent les articles 1316 à 1316-4 pour répondre à la question concrète : comment valider a posteriori un acte sous-seing privé électronique dont les textes précisent 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 types de moyens techniques susceptibles de fournir l'identification et l'intégrité,
- la signature électronique de l'article 1316-4.

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 branche pas directement sur 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'une garantie d'identification et d'une garantie d'intégrité. Mais quelle signature choisir ? Celle de l'article 1316-4, obligatoirement, ou un autre type de signature ?

En poursuivant la réflexion, un principe de bon sens apparaît : 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 définitive, 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 SE-DIR), mais assurant en plus, l'intégrité. Dit d'une autre façon, une *signature électronique avancée "dégradée*[30]*"* de la Directive (SE-SAV) pour ne pas retomber au centre de la dimension juridique.

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 leur 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 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.

[29] 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).

[30] 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 ?

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[31]. Bref, on retrouve l'intérêt de l'accord d'interchange de l'EDI[32].

Enfin, il subsiste une autre façon de résoudre cette problématique, c'est de la télescoper avec celle qui suit, la problématique de la transmission de l'acte sous-seing privé[33].

En conclusion de l'étude 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 (SE-DIR) et inférieure en efficacité à la signature électronique avancée (SE-SAV) c'est-à-dire "dégradée".

3.2. La transmission électronique de l'acte

Après sa création, l'acte sous-seing privé sous forme électronique est transmis par voie télématique. Cette transmission s'effectue dans les mêmes conditions de sécurité convenues : identification de l'origine et intégrité du contenu. Pour que le niveau de sécurité soit constant, on songera tout naturellement d'une part, à sécuriser la transmission par une signature électronique et d'autre part, à employer un type de signature qui serait susceptible d'autoriser en aval la dématérialisation de l'acte. On retrouvera ci-dessous la question de la signature à employer avec de nouveaux raffinements, mais aussi une incidente avec la question du recommandé électronique.

3.2.1. Sécurisation de l'acte ou de la transmission électronique

Pour éviter les questions soulevées dans le présent texte, on pourrait être tenté d'employer un moyen maximaliste, la *signature électronique sécurisée* du décret d'application. Le bon sens commanderait plutôt d'éviter d'employer un moyen dont toutes les caractéristiques juridiques ne sont pas maîtrisés. Le droit également, si on se réfère à un exemple significatif, celui de la facture électronique[34].

La *Directive 2001/115 du 20 décembre 2001*sur la facturation[35] incite les Etats Membres à accepter les factures sous forme électronique à condition que deux garanties de sécurité soient respectées : l'authentification 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[36].

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[37]. 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

---

[31] 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, le cas avec l'archivage comme on le verra plus loin.]

[32] 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.*

[33] 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).

[34] A cette occasion, une seconde remarque de bon sens : ne jamais oublier qu'une signature électronique n'est pas grand chose en soi ; il ne faut pas négliger l'acte dématérialisé qui est accompagné de cette signature.

[35] *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).

[36] 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 concernant les aspects juridiques de l'échange de données informatisé.

[37] GOBERT Didier, "*Vers une discrimination de traitement entre la facture papier et la facture électronique*". A voir également sur le caractère d'acte sous-seing privé acquis par une facture électronique accompagnée d'une signature électronique avancée (cf. INFRA).

en déduire que la facture sur papier ne sera pas signée, alors que la facture électronique le sera par une signature électronique avancée (SE-SAV). En effet, il est deux emplois de la signature correspondant aux deux pans de la problématique juridique que rencontre tout document voué à la dématérialisation : sécurisation de l'acte et sécurisation de la transmission.

La substitution d'une forme électronique à une forme écrite vise généralement 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[38],
- 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 factures sont dans les Etats membres peu soumises à la formalité de signature. Elles devront le rester. Cependant en ce qui concerne la transmission télématique, il faut sécuriser l'échange[39]. La sécurisation, en terme d'identification et d'intégrité est assurée selon le texte par une SE-SAV considérée comme un pur instrument technique.

3.2.2. Transmission d'un acte et signature avancée

L'emploi d'une signature électronique étant acquis pour la facture électronique sur le pan unique de la sécurisation de l'échange, on peut s'arrêter sur la qualification d'*avancée* que doit présenter la signature électronique employée. Cette qualification pose en effet problème. On s'étonne des intentions du rédacteur de cette directive qui, à tout le moins, sont différentes de celui de la *Directive sur un cadre communautaire pour la signature électronique*, au point de ne pas en adopter la logique. La SE-SAV selon l'article 5.1.b. de cette dernière Directive doit être recevable comme preuve en justice. De quelle preuve peut-on parler avec la facture électronique ? La preuve en question ne concerne pas les relations de droit commercial entre vendeur et client, mais un contexte relatif à la TVA, ce qui est le domaine de Directive facture. Est-ce la preuve de l'assujettissement qui est recherchée ? De l'obligation de payer la taxe ? Certes, non. Peut-on penser que si on se dispense de dresser une facture, on est exonéré de payer la TVA ?

Conseiller de recourir à une SE-SAV n'est pas cohérent avec la Directive signature électronique. Puisqu'il ne s'agit pas de se placer dans un contexte de preuve de facture, on peut écarter la SE-SAV. Mais pour recourir à quoi, à la Signature électronique ordinaire également prévue par la Directive précitée ? Cette "*donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification*[40]" aurait pu convenir, mais il lui manque certaines qualités, comme garantir l'intégrité. Ce type de signature ne semble pas convenir, force est de revenir sur la SE-SAV

La Directive comporte une disposition complémentaire qui laisse le lecteur perplexe. Après avoir préconisé la sécurisation de la transmission de la facture par voie électronique, le texte ajoute : "*Les Etats membres peuvent toutefois, demander que la signature électronique avancée, soit basée sur un certificat qualifié et créée par un dispositif sécurisé de création de signature...*" Est-ce à dire qu'il pourrait exister, a contrario, une SE-SAV basée sur un certificat non qualifié et créée par un dispositif de création de signature (DCS) non sécurisé ? Une affirmation de ce type ne semble pas correspondre à la logique de la Directive signature, ni à ce qu'en ont compris les Etats membres qui l'ont transposée dans leur droit interne. Si l'article 2 de la Directive signature définit la SE-SAV de façon générale, l'article 5.1. ne laisse aucun doute : les SE-SAV sont "*basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature"*. L'article 5.2. envisage des cas où l'efficacité juridique sera moindre, par exemple quand le certificat n'est pas qualifié, quand le DCS n'est pas sécurisé, quand le prestataire de services de certification n'est pas qualifié. Pour tous ces cas, l'article 5.2. parle de "signature électronique" simplement et non de "signature électronique avancée".

---

[38] Les exigences les plus traditionnelles du formalisme juridique appliquées à un document sont l'obligation d'un support papier, l'apposition d'une signature et la présence de mentions obligatoires.

[39] 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..."*

[40] Définition de l'article 2-1) de la Directive signature électronique.

Au total, la Directive facture semble vouloir encourager l'usage d'une signature électronique avancée, mais "dégradée" dans la mesure où le certificat ne serait pas nécessairement qualifié et où le DCS ne serait pas nécessairement sécurisé. De plus, le texte prétend encourager l'usage d'une SE-SAV dans un contexte non juridique puisque seule, la sécurisation de la transmission électronique est en cause. Une interprétation de la SE-SAV qui n'est pas celle de la majorité des auteurs. Cette interprétation semble mal s'accorder avec la logique de la Directive signature électronique.

3.2.3. Le droit français entre signature avancée et signature sécurisée

Lorsque le législateur français procédera à la transposition de la Directive du 20 décembre 2001 dans le droit national, il devra régler la question de la SE-SAV qui n'existe pas dans notre droit interne. Comme précédemment développé dans la première partie de notre article, nous estimons que les deux signatures définies dans le décret d'application de l'article 1316-4 du Code Civil, la *signature électronique* ordinaire et la *signature électronique sécurisée* (SES) sont toutes deux transposées de la SE-SAV. Il ne serait pas inconcevable que législateur se prononce pour une modalité de facture sous forme électronique dans un format non structuré[41] munie d'une signature électronique sécurisée. En transposant de cette façon, le législateur transposerait du même coup les incohérences juridiques.

En droit français, le régime actuel de la signature (sur support papier) ne comporte aucune obligation de signature, malgré l'opinion courante. Le législateur n'aura 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 imposerait l'usage d'une signature électronique. Mais opter pour la signature sécurisée ouvrirait sur les mêmes interrogations en matière de preuve que le choix d'une SE-SAV. Il est même possible en droit interne d'être plus précis dans les conséquences.

La base de la SES 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[42]. Ce qui signifie que son régime sera celui des actes sous-seing privé. 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[43] ? 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. Gageons qu'un autre acte authentique électronique pourra lui être opposé victorieusement... dès que la réglementation de l'acte authentique électronique (article 1317, second alinéa[44]) sera connue.

3.2.4. De la signature électronique au recommandé électronique

Le droit s'est approprié la signature électronique inventée par les techniciens. Dans ces conditions, il ne faut pas s'étonner de l'hétérogénéité entre les atteintes des spécialistes des deux mondes. On va le constater ici. Pour le juriste, le plus important est l'acte de (création de) signature par l'auteur intellectuel du document. Pour le technicien, le plus utile est l'acte de vérification de signature par le destinataire du message électronique. Le destinataire a besoin d'être tranquillisé sur la source du message et sur le bon état de celui-ci une fois arrivé à

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

[42] 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.

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

[44] La 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 a ajouté à l'article 1317 un alinéa ainsi rédigé : "*Il* [l'acte authentique] *peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par Décret en Conseil d'Etat."*

destination ; c'est pourquoi la signature électronique a été inventée. L'étape de transmission d'un message qui se révèle acte sous forme électronique est le moment où les deux mondes se rapprochent le plus.

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)[45]. 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.

Les relations entre le temps et la signature sous l'angle juridique[46] ne sont pas l'objet de ce texte. 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*. On peut observer cependant les enseignements d'autres législations, comme celle du Luxembourg.

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 légitimement 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[47] qui intègre *l'heure, la date, l'envoi et le cas échéant la réception* sous la certification de l'archiveur de confiance. La leçon à en tirer est que l'horodatage

45 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.

46 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).

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

de la transmission est une procédure sécurisée dont les garanties sont l'identification de l'auteur, l'intégrité du message (toutes deux fournies par la signature électronique), un horodatage certifié.

En conclusion de l'étude de cette étape, 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, avec des spécifications telles qu'elle puisse s'intégrer dans le type SE-DIR de la directive, ou encore d'un système de type recommandé électronique.

3.3. La conservation de l'acte sous forme électronique

Le cycle de vie de l'acte sous-seing privé ne serait pas complet sans conservation ou archivage. Un professionnel spécialisé peut apparaître avec dans cette étape, le tiers archiveur. Mais que l'archivage se réalise en interne ou à l'extérieur chez le tiers archiveur, il faut d'abord s'entendre sur ce qu'on doit conserver.

3.3.1. Comment conserver et quoi archiver

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 exigées par les textes. Aussi faudra-t-il archiver l'écrit électronique et sa signature. A cela, il faudra naturellement ajouter le certificat électronique qui permettra après une période de garde plus ou moins longue de vérifier ultérieurement si la signature était valide au moment de sa création.

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. Le certificateur le diffuse dès sa création tout en gardant une copie. Valable pour une durée de temps limitée, 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. Résumons, trois éléments sont conservés : le message, sa signature et le certificat de clé publique. Ces éléments sont conservés en interne ou transmis à un archiveur professionnel.

Lorsque les archives sont stockées 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 déterminé qu'il faut retenir comme archive. Ici réapparaît 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*.

Si l'utilisateur ne craint pas de transférer par voie de télécommunications un volume important de données, générateur de risques techniques et de coûts non négligeables, il peut recourir à un archiveur distant, encore appelé *tiers archiveur*. Pour la beauté de l'exercice, le tiers archiveur pourra être alimenté en archive par voie électronique. Que lui enverra-t-on et comment ? On lui enverra naturellement les 3 éléments susvisés qui formeront un *lot*. Comme l'archiveur n'est pas censé savoir ce qu'il reçoit ou en prendre connaissance, les données à archiver pourront lui être remises chiffrées ou simplement, les éléments seront répartis en plusieurs lots. Les lots comprennent alors des données de contrôle et de service qui permettront à l'utilisateur de récupérer les 3 éléments sous forme opérationnelle en cas de restitution des archives.

3.3.2. L'intervention d'un 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.* Pour étendre cette réflexion aux échanges électroniques sécurisés par des signatures électroniques, l'association IALTA France et le Conseil Supérieur ont créé un groupe de travail commun qui a publié en juillet 2000 un *Guide de l'Archivage électronique sécurisé*. Les travaux du Groupe de travail ont été grandement confortés par les membres de l'Association des Professionnels de la Gestion électronique des documents (APROGED). C'est dans cette perspective que le groupe de travail a développé les différents scénarios d'archivage, la notion de lots et de données de contrôle.

La transmission électronique des archives entre l'utilisateur et l'archiveur entraîne de nouveau l'emploi ou la poursuite des échanges électroniques sécurisés présentant les garanties d'identification et d'intégrité. C'est au client expéditeur de mettre en œuvre les moyens techniques indispensables, une signature électronique, par exemple. Cela signifie concrètement que l'expéditeur va sécuriser le lot à envoyer par une signature électronique mettant en œuvre un certificat électronique.

Cette signature électronique "globale" vise la sécurisation de l'échange électronique. Elle ne sert ni à assurer la dématérialisation du lot ni à en assurer la preuve. C'est une signature électronique sans dimension juridique immédiate car elle ne s'applique pas à un acte. Une signature technique convient, du moment qu'elle se réfère au modèle de l'Infrastructure à clés publiques.

Le tiers archiveur se comporte dans cette relation électronique particulière comme un simple destinataire. A réception des données envoyées, il effectuera plusieurs traitements pour vérifier la permanence des garanties de sécurité pendant le transport électronique entre son client et lui :
- il vérifiera que l'émetteur est un client,
- il contrôlera 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.

Par la suite, l'archiveur mettra en œuvre des normes techniques relatives à l'archivage qui garantissent une bonne intégrité des données conservées. Les travaux du groupe de travail se sont ensuite intéressés à la restitution d'archives. Ce mouvement est l'inverse du précédent. En cas de demande de toute personne ou entité autorisée, l'archiveur restituera ses archives au client à sécurité constante. Là toujours, identification et intégrité des éléments renvoyés sont prioritaires. Si les mêmes besoins sont couverts par les mêmes outils, une signature électronique technique formalisera les garanties demandées.

En conclusion de l'étude de cette étape, on peut estimer que les besoins de sécurité technique en matière d'archivage de l'écrit sous forme électronique seraient satisfaits par l'emploi d'une signature électronique de type SE-DIR ou d'un système de type recommandé électronique

3.4. la preuve de l'acte sous forme électronique

3.4.1. La primauté de la Signature Electronique Sécurisée

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*.

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.

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 ?

3.4.2. Le retour de la signature simple du décret

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. 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 renforcer 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.
- 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.

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. 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. Pourtant la qualification des PSCE reste facultative à lire l'article 7 du décret 2001-272[48]. 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 SE-SES, alors les évaluations portant sur le DCS et le certificat sont obligatoires. On peut avoir la tentation de faire l'impasse sur la SE-SES et ses procédures parce que ces audits et contrôles génèrent des charges et des coûts qui sont à la charge du demandeur[49]. 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"[50] 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 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[51].

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* (SE-SES) ou peut-être même par une signature électronique simple du Décret (SE-DEC).

---

[48] 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*".

[49] 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...*"

[50] 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.

[51] La différence entre le niveau haut et le niveau intermédiaire est la suivante : les exigences techniques sont respectées dans les deux cas, mais ont été validées par un organisme de contrôle pour le niveau haut, alors qu'elles n'ont pas été auditées et reconnue pour le niveau intermédiaire.